Number 106 July 2016

ERCIM NEWS

www.ercim.eu

Special theme: Cyber-Security

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of about 6,000 printed copies and is also available online.

ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
Tel: +33 4 9238 5010, E-mail: contact@ercim.eu
Director: Jérôme Chailloux
ISSN 0926-4981

Contributions
Contributions should be submitted to the local editor of your country

Copyright notice

Advertising
For current advertising rates and conditions, see http://ercim-news.ercim.eu/ or contact peter.kunz@ercim.eu

ERCIM News online edition
The online edition is published at http://ercim-news.ercim.eu/

Next issue
July 2016, Special theme: Cybersecurity

Subscription
Subscribe to ERCIM News by sending an email to en-subscriptions@ercim.eu or by filling out the form at the ERCIM News website: http://ercim-news.ercim.eu/

Cover photo – source: Beeldbank TNO

© FreeImages.com/Rayko Swensson

Cybersecurity: A Key Pillar of the European Digital Single Market

by Afonso Ferreira (European Commission, on leave from the French CNRS) and Paul Timmers (European Commission)

In February 2016 one of the largest heists in history was attempted against a Bangladesh bank. Gangsters tried to rob almost 1 US$ Billion and disappear in the Philippines. At the time of this writing 81 US$ Million are still unaccounted for and seemingly unrecoverable. This was a crime committed exclusively in cyberspace until electronic orders were transformed in cash. The current state of investigations points to the fact that the computer hackers only had to tamper with two bytes – twice – in the bank software in order to get away with the money.

Cybersecurity is an ever-growing challenge for companies, states and individuals, as digital technologies become more widely used in economic, social and governance matters. With the convergence of the cyber and the physical spaces, risks and threats in the cyberspace may increasingly affect physical space and individuals' livelihoods. Cyber incidents and attacks can disrupt the supply of essential services for our societies, since digital technologies are complex and underpin other systems and services, like finance, health, energy, transport.

On the positive side, with the fast continuing evolution of information and communication technologies (ICT) and their integration into almost every facet of modern society, enormous opportunities for innovation are created. Digital technologies and the Internet are the backbone of our society and economy; they are key enablers of prosperity and freedom. A high level of network and information security (NIS) across the EU is essential to ensure consumer confidence and to keep the online economy running. This will, in turn, preserve the well-functioning of the internal market and will boost growth and jobs. Cybersecurity is therefore an integral part of a much broader transformation across society, driven by the digital revolution.

Consequently, the European Union works on a number of fronts to ensure cybersecurity in Europe, supported by ENISA – the European Network and Information Security Agency.

EU Strategies and Legislation

The Cybersecurity Strategy for the European Union provided in 2013 the overall strategic framework for the EU initiatives on cybersecurity. Its goal is to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world.

Also in 2013 the European Commission put forward a proposal for the NIS Directive, with measures to ensure a high common level of network and information security across the Union. It should be adopted in summer 2016 and provides legal measures to boost the overall level of cybersecurity in the EU. Once adopted and implemented, the NIS Directive will benefit citizens, government, and businesses, who will be able to rely on more secure digital networks and infrastructure to access or provide essential services online.

Afonso Ferreira (left) and Paul Timmers (right), DG CONNECT, European Commission.

The establishment of the NIS Public-Private Platform was announced in the Cybersecurity Strategy, to foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrations in Europe. Its Working Group on secure ICT research and innovation was tasked with the preparation of the European Strategic Research Agenda in Cybersecurity (SRA), which was delivered by end 2015.

Finally, one of the 16 initiatives set in the Digital Single Market Strategy is the launch of an ambitious contractual public-private partnership (cPPP) on cybersecurity. It aims to strengthen the EU cybersecurity industry and make sure European citizens and businesses have access to more innovative, secure and user-friendly solutions that take into account European rules and values.

The Cybersecurity cPPP will deliver innovation against a roadmap for research and innovation (based on the SRA developed by the NIS Platform). It will implement:
- Bottom-up cooperation on research and innovation between Member States and industrial actors in the upstream part of the innovation life cycle.
- Better alignment of demand and supply sectors for cybersecurity.
- Synergies to develop common, sector-neutral technological building blocks.
- Engagement of big costumers of cybersecurity solutions to define common requirements for their sector.
- Parts of the DSM Priority Standardisation Plan, as announced in the Digitising European Industry strategy launched in April 2016.
- Mechanisms to ease access to finance as well as developing human capacities.

The cPPP will maximize the use of Horizon 2020 funds through better focus on a few technical priorities, leveraging funding from Leadership in Enabling and Industrial Technologies and Societal Challenge Secure Societies to deliver societal benefits for users and provide visibility to European Research and Innovation excellence in cybersecurity.

The views expressed in the article are the sole responsibility of the authors and in no way represent the view of the European Commission and its services.

KEYNOTE

RESEARCH AND SOCIETY

SPECIAL THEME

The special theme section "Cybersecurity" has been coordinated by Fabio Martinelli (IIT-CNR) and Edgar Weippl (SBA Research)

Introduction to the Special Theme

Invited contribution

Cryptography

Data

Network

Systems

Cyber-Physical Systems

Cybercrime

RESEARCH AND INNOVATION

This section features news about research activities and innovative developments from European research institutes

EVENTS, IN BRIEF

Announcements

On the Occasion of Aad van Wijngaarden's 100th Birthday

International Informatics

by Gerard Alberts

Building up informatica, as computer science came to be called in The Netherlands, has been an international affair. Aad van Wijngaarden, 1916-1987, founding father of Dutch computer science was responsible for forging international collaboration and helping to make informatics an international endeavour. His influence reached from cooperative efforts in building computers in the 1940s to Algol68, the epitome of his style of computing. CWI commemorates his 100th birthday this year.

London

It was in London, February 1946, that Aad van Wijngaarden's decision marked the beginning of computer science for The Netherlands. Sent out by Delft University of Technology on assignment to collect all available literature and reprints on the latest developments in mechanical and naval engineering that Dutch research might have missed during the war years, Van Wijngaarden wrote to his supervisor, C.B. Biezeno, that the latest developments in mathematical machines were worthy of a separate report. Up to this point computing had been an auxiliary activity for fields such as engineering, astronomy and physics, but here was a young academic in engineering with his finger on the pulse of international developments and bringing computing into the limelight.

His two Delft mentors facilitated Van Wijngaarden's trip to London: Jan Burgers, and Cornelis Biezeno. The first, professor of fluid dynamics known for the "Burgers equation", the latter, professor of Applied Mechanics and known for the big book with Richard Grammel, Technische Dynamik. Burgers created the scheme that sent out out a dozen young Delft scholars on a post-war reconnaissance tour to the United Kingdom. Biezeno chose Van Wijngaarden to be a member of that team and assigned him two study topics.

During the war years Van Wijngaarden had been calculating tedious computations in turbulence supervised by Burgers. When in early 1945 Burgers asked him to summarise the work in a dissertation, Aad rejected and threw away the results because 'it simply lacked beauty'. At this point, Biezeno, for whom he had solved several major problems raised in Technische Dynamik stepped in and saved the day by guiding him to a cum laude doctorate on those results, which he completed by December 1945. These two teachers not only taught him to do sophisticated computations, but perhaps just as importantly raised him in an atmosphere of internationally oriented scholarship. Biezeno and Burgers had earlier created the tradition of quadrennial congresses in Theoretical and Applied Mechanics starting in Delft in 1924. Now, in 1948, Burgers oversaw the formation of a committee on computing technology chaired by the Parisian professor Auger, with Van Wijngaarden as its secretary. They sent letters to academics throughout northern Europe with the hope of engaging other institutions and although the responses were sparse, the spark of international cooperation was lit.

Amsterdam

It was in Amsterdam, February 11th 1946, that mathematicians turned their ambition to put mathematics at the service of society into the founding of a research institute, the Mathematical Centre, now CWI. Van Wijngaarden was appointed head of the centre's computing department by January 1947. Most of his first year was spent in the UK and the US. It is likely that anyone in that position would have been destined to be considered as the founding father of informatica in The Netherlands, but Van Wijngaarden went well beyond the call of duty. He was capable of making the leaps of intellect, the reflections that lifted the emerging discipline to new levels of abstraction. In those early years, Van Wijngaarden contributed to the field – then known as numerical analysis – with subtle reflections on rounding off errors when using the new machine power.

Machines, however, were not readily available. Means and components were scarce in a small country like The Netherlands, and once again international cooperation was sought with both Belgium and France – to no avail. In 1949 and 1951 two very promising bids were made for a Unesco-sponsored International Computing Centre (ICC) to be established in Amsterdam with the Mathematical Centre. ,The dynamics of the Cold War placed the ICC in Rome. Although Amsterdam was on its own now to construct machines, Van Wijngaarden followed the English and American examples. The 1952 ARRA was largely an emulation of Booth's ARC in London.

At this time, building computers was one thing, but getting them properly programmed, quite another. Van Wijngaarden had the vision to appoint Edsger W. Dijkstra as an assistant 'for the programming of the ARRA', well before that machine was dedicated, midsummer 1952. Many Europeans learnt programming with Maurice Wilkes at Cambridge Summer School. Further reflections on programming were absorbed at international conferences, for example, Rutishauser's concern about readable formulation and unified notation of computer programs, in Darmstadt 1955.

IFIP

International exchange intensified and, quite naturally through his international presence, Aad van Wijngaarden was closely involved in preparing under the aegis of Unesco, the International Conference on Information Processing, to be held in Paris in the summer of 1959. Cold War circumstances dictated that the envisaged international union could only materialise as a federation of national societies – one per country. Hence, in the spring of 1958 on a terrace in Paris, it was decided to create a Dutch society for computing machinery, NRMG.

That summer, August 1958, Van Wijngaarden's work came to a cruel standstill. Being invited to give a talk on the International Congress of Mathematicians in Edinburgh was a highlight of his career. Leaving the conference with his wife for a holiday in Scotland, his car crashed. His wife died and he spent time recovering in hospital until November. Rather than pick up the pieces after this disaster, he decided

Aad van Wijngaarden at the Mathematisch Centrum in Amsterdam in 1951. Picture: CWI.

to start a new life and embark on a new career: he became a specialist in programming language.

What for him was a new career, was in fact the next step of abstraction in the emerging discipline of computer science. Stepping up from the Darmstadt concern of program notation, a committee of European and American computing specialists joined efforts towards a system of unified notation. The committee was initiated by the German founding father of computer science, Friedrich Bauer. Their next step was to call such a system a language, at first in 1958 International Algebraic Language (IAL), and later Algorithmic Language (ALGOL). The language metaphor had been suggested a few year before in debates on programming in the US, and was now adopted to become the cornerstone of computer science worldwide. It was this wagon that Van Wijngaarden, together with his Amsterdam team, joined in 1959. Computer science was now starting to look like a discipline – an international discipline. And at the Mathematical Centre, the computing department had set its internationally flavoured research agenda.

Copenhagen

From 1959 Aad van Wijngaarden joined the ALGOL committee, taking Dijkstra and others to the preparatory meetings, himself voting at the final meeting in Paris, January 1960, and performing as one of the authors of the ALGOL report. Dijkstra and Zonneveld joined him on a subsequent trip to Copenhagen to meet Peter Naur, acting editor of the ALGOL report, and left with the invitation to come see a working ALGOL compiler in half a year in Amsterdam, August 16th 1960. Van Wijngaarden, prompted by Dijkstra on his side, changed the ALGOL agenda by calling Peter Naur on the telephone and convincing him of phrasing the “call for procedures” in the defining report in such a way that it would allow recursive procedures, a sharply controversial issue for Friedrich Bauer’s German team. Writing the ALGOL compiler in time and in a novel style, Dijkstra convincingly fulfilled the promises of the amended ALGOL agenda.
IFIP, prepared at the 1959 Paris conference, and founded in 1960 created the water to swim in for the internationally oriented scholar Van Wijngaarden. IFIP adopted the ALGOL agenda by creating a working group, WG 2.1, for the development of a successor language. Here Aad van Wijngaarden effectively took the lead with abstract notions of design of language. He astonished the 1965 meeting of WG 2.1 at St. Pierre de Chartreuse with orthogonality and two level grammars –later known as Van Wijngaarden grammars. Standing in awe, the meeting decided that whatever the details of the definition of the new language, it should be formulated along these lines. The successor language came to be ALGOL 68, presented at the IFIP congress in Edinburgh and finalized in December 1968, in a report dense with motto’s, intellectual puns, and literary references. As if the personal mark needed further emphasis, Aad van Wijngaarden garned the back cover of the report with a small hidden @, his personal bookmark symbol.

As a piece of art, ALGOL 68 had, and still has, a small community of admirers. As a programming language, as a tool, it was a failure. It realised the ALGOL agenda set in 1958, in the most beautiful and least practical way. Ten years on, however, the agenda had shifted to software engineering with new pressing questions and a new generation of bright spirits.

The true influence of Van Wijngaarden internationally, apart from his avid cooperation and cooperative spirit, was that he fuelled the intellectual fire in WG 2.1 to such an extent that it spun off in all directions, one deriving from it new principles of language design – yet a level of abstraction higher, another turning orthogonality into SIMULA and object thinking, a third bringing the inspiration down to earth resulting in the development of the language Pascal that educated generations of computer scientists. To The Netherlands Van Wijngaarden left a discipline following research agendas, with a bias for theoretical directions and daring abstractions. In his footsteps, informatica was naturally an international endeavour.

Please contact:
Gerard Alberts, University of Amsterdam, The Netherlands
G.Alberts@uva.nl

Introduction to the Special Theme

Cybersecurity

by Fabio Martinelli (IIT-CNR) and Edgar Weippl (SBA Research)

Public interest in cyber security is on the rise, owing largely to the increasingly pervasive nature of cyber technologies and their ability to enhance our quality of life, affecting most of our activities (either visibly or in an invisibly). In the past, our interactions with PCs were limited to particular working activities. Now, even during our daily commutes, in our cars we are surrounded by hundreds of electronic control units (ECU), our mobile phones are next to us, and our smart watches observe and record every breath.

Indeed, the digital revolution spreads information and communication technologies anywhere, anytime. More application fields open up more opportunities for attack, and the motivations and the possible scale of attacks change, no longer being restricted to economically motivated attacks, but also to cyber terrorism (cyber crime is also mentioned in the Keynote in this special issue). As technologies evolve, the security situation thus becomes far more complex, necessitating new enhanced cyber security methods and approaches.

There is the need for increased effort, covering the new fields, and addressing the new data economy that new technology such as the Internet of Things (IoT) is creating. Unprecedented amounts of data are being collected by devices, cameras, sensors, and ICT services and can be used to analyse, predict, inform and influence digital and even physical and social behaviour (just consider the increasing relevance of social networks). The protection of data is thus a paramount objective from both technical and social perspectives. We need to empower users to define how data are collected, analysed, transferred, and aggregated and ultimately used. Privacy concerns are increasingly relevant and the relationships between surveillance and privacy should be carefully considered.

The increased networking capabilities allow the creation of systems of systems and cyber-physical systems where the digital and physical worlds meet; thus merging safety issues with security issues. Consequently, it is vital that we develop ways of addressing both safety and security in complementary ways when analysing, designing and engineering systems. While achieving zero vulnerabilities is a holy grail in our community, their reduction should be a constant aim, which is reflected in the articles featured in this issue.

In our highly interconnected world, we require new methods and approaches to risk assessment, that can exploit data in a cooperative manner, ideally whilst preserving the privacy of prosumers (producers and consumers). Collectively sharing information and benefiting from it is an increasing trend that should be fostered by means of technical and policy means (e.g., the NIS directive).

From a technical perspective, European researchers have significant expertise in cryptography that lies at the core of many security technologies, and several articles featured in this special issue cover areas ranging from cryptography implementation to crypto techniques for data control.

Cyber crime is undoubtedly a recurrent major concern in our interconnected world, and efforts to prevent cyber crime need to be ongoing. Cyber protection is one of the mechanisms – along with the creation of frameworks that facilitate forensic activities that can involve all relevant stakeholders. The new revolution of e-currencies with their technologies as block chain will create new issues as well as new opportunities for the growth of the digital civilisation we are experiencing.

Thus, not surprisingly, this ERCIM News special issue on cyber security has attracted a significant number of contributions grouped within the following areas:
- Cryptography
- Data
- Network
- Systems
- Cyber-physical systems
- Cyber crime.

Overall these articles present a variety of research results that show the richness and range of cyber security issues and their application domains. The ERCIM community and European stakeholders, including industry, are currently merging their efforts to successfully address the challenges of cyber security.

Please contact:
Fabio Martinelli, IIT CNR, Italy
Fabio.Martinelli@iit.cnr.it

Edgar Weippl, SBA Research, Austria
EWeippl@sba-research.org

Digital Witness: Digital Evidence Management Framework for the Internet of Things

by Ana Nieto, Rodrigo Roman and Javier Lopez (University of Malaga)

We define the concept of 'digital witness'; personal devices able to actively acquire, store and transmit digital evidence to an authorised entity, reliably and securely.

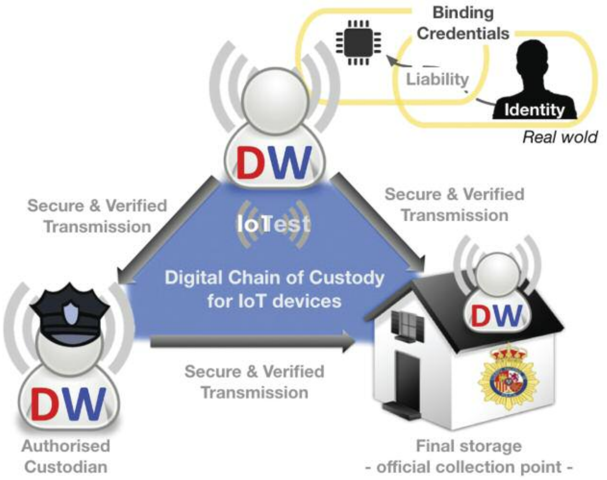


Figure 1: Digital Witness for Cybersecurity in IoT.

The growing density of networks formed by devices with heterogeneous capabilities and users with different profiles poses new challenges to cybersecurity. One clear example of this is the Internet of Things (IoT) paradigm, where cyberoffenses – not only cyberattacks – take place in very dynamic, polymorphic and even isolated scenarios [1]. There are too many devices to be controlled, and any device with minimal computing and communications capabilities can perpetrate cyber-attacks without leaving a trace. In such a scenario, and in order to clarify the facts of a cyber-crime scene, it is essential to collect and handle electronic evidence within a Chain of Custody (CoC). Yet this is a problem that is impossible to solve only with existing tools.

The IoTest project [L1] aims to help solve this problem by introducing a security solution that is drastically different from those that have been used to date. This project proposes the design and development of the 'digital witness', a trusted electronic device capable of obtaining and safeguarding electronic evidence. More specifically, a digital witness: (i) binds the user's identity to his/her personal device, (ii) has a core of trust that is able to protect the integrity of one or more electronic pieces of evidence according to the law, within a trusted execution environment, (iii) ensures that only authorised entities have access to the evidence, and (iv) is able to witness the traceability of the evidence.

Furthermore, a digital witness (v) is able to send digital evidence to other digital witnesses or any other entity with the authority to safeguard the electronic evidence. The user's identity and the capabilities of his device determine the type and role of a digital witness, which opens the door to the creation of digital witnesses with different profiles (e.g., police cars as mobile custodians). These and other properties enable the creation of a digital chain of custody in IoT (IoT-DCoC) environments (see Figure 1). IoTest defines and works with this natural evolution to digital chains of custody [2].

These five basic requirements help to define a robust digital witness, and comply with several existing challenges in the emerging IoT-forensics paradigm [3]. In order to fulfil these requirements, the project will explore various novel concepts, such as the notion of binding credentials (BC). In this context, a BC is defined as any mechanism that provides a link between a user and a device, based on the user's identity. In addition, BCs can be used in conjunction with biometric capabilities in personal devices to ensure the presence of the user at the key moments within the lifecycle of the digital evidence.

IoTest is a novel project recently funded by the Spanish Ministry of Economy and Competitiveness under the EXPLORA Programme, a complementary action that encourages frontier research. Precisely, this project also will investigate the viability of more radical ideas in the context of future network environments, such as the implementation of the concept of digital witness in local clouds of personal IoT devices, the deployment of virtual digital witnesses that are linked to the identity of a privileged digital witness device, and the implementation of binding credentials associated to these virtual witnesses.

By using digital witnesses as a foundation for the creation of a digital chain of custody within IoT scenarios, the IoTest project aims to offer a dynamic solution that will record events on heterogeneous, unpredictable and uncertain scenarios. Moreover, since existing digital evidence processes and regulations are not prepared to deal with the new cybersecurity issues created by these highly dynamic and distributed scenarios, we expect that the deployment of digital witnesses will result in a qualitative advancement in the evolution of electronic evidence management systems, improving their ability to detect attacks and identify cybercriminals.

Links:
[L1] https://www.nics.uma.es/projects/iotest

References:

[1] A. Kasper, E. Laurits: "Challenges in Collecting Digital Evidence: A Legal Perspective", The Future of Law and eTechnologies, 195–233, 2016.
[2] Y. Prayudi, S. Azhari: "Digital chain of custody: State of the art", International Journal of Computer Applications, 114 (5), 1–9, 2015.
[3] E. Oriwoh et al.: "Internet of things forensics: Challenges and approaches", 9th IEEE Collaboratecom, 608–615, 2013.

Please contact:

Ana Nieto, University of Malaga, Spain
+34 951 952914
nieto@lcc.uma.es

Security Assessment of Software Security: A Closer Look at White-Box Cryptographic Implementations

by Joppe W. Bos and Wil Michiels (NXP)

Secure software implementations in the 'white-box attack model' (where the user can be the adversary) are being used to secure smart devices. At NXP we have created a new technique for security assessment which allows one to efficiently extract the secret key from all publicly available white-box implementations. This highlights the risk of using such solutions for certain use-cases in practice.

Owing to the widespread use of 'smart' devices, which allow users to access a large variety of ubiquitous services, these platforms have become a valuable target to compromise. There are various ways to protect cryptographic secret key material, which might be used to secure your mobile payment transactions, decrypt streaming media content, or protect your fare during transit. Solutions range from using unprotected software implementations to tamper-resistant hardware implementations. In order to support as many devices as possible, there has been a trend in the last couple of years towards using secure cryptographic software implementations.

Note, however, that in many realistic scenarios the user of the device might be the adversary. In the streaming content scenario, for instance, a user might want to give a friend access to his or her subscribed content. This adversary controls the platform where the software is being executed and this allows one to perform static analysis on the software, inspect and alter the memory used, and even alter intermediate results during execution. This security model is referred to as the white-box model, and a software implementation of a cryptographic algorithm which is secure in this model is called a white-box implementation. This model was introduced in [1]. The idea is to use look-up tables rather than individual computational steps to implement the cryptographic algorithm. The usage of a fixed secret key is embedded in these tables that are filled with pseudo-random data.

A well-known attack on hardware implementations is to collect power traces: a collection of power measurements over time when executing the cryptographic implementation given known input. The statistical behaviour of a power trace might correlate to, and hence reveal information about, the secret key material used (see [2]). In order to assess the security of white-box implementations we applied this side-channel information paradigm to the software implementation setting. To collect information we have used freely available dynamic binary instrumentation tools. In such tools additional analysis code is added to the original code of the client program at run-time in order to aid memory debugging, memory leak detection, and profiling. This allows one to monitor, modify and insert instructions in a binary executable. We have developed plugins for these tools which can collect software traces: a trace which records the read and write accesses made to memory. These software traces are used to deduce information about the secret embedded in the look-up tables of a white-box implementation in the same way as this is done with power traces for hardware in differential power analysis techniques. This means that we correlate key guesses with the measurements in the software traces. We named this approach 'differential computation analysis' (DCA).

We have demonstrated in [3] that DCA can be used to efficiently extract the secret key from all publicly available white-box implementations. In contrast to the current cryptanalytic methods to attack white-box implementations, this technique does not require any knowledge about the implementation strategy used, can be mounted without much technical cryptographic knowledge in an automated way, and extract the key significantly faster. We have created a tool which can visualize the traces (accesses to memory). Figure 1 shows an example of a software execution trace of a white-box implementation of the advanced encryption standard (AES). The virtual address space is represented on the x-axis while the y-axis

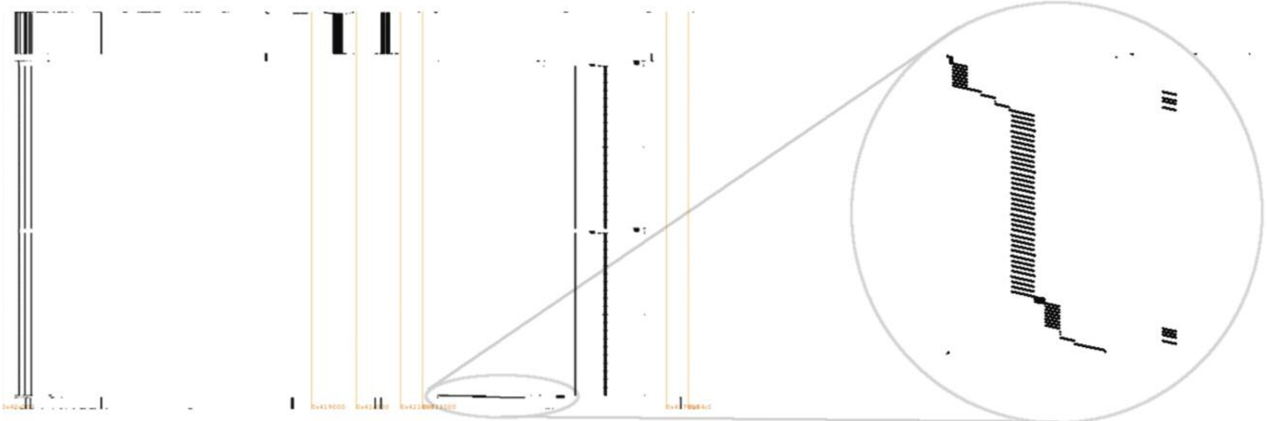


Figure 1: An example of a software trace where the enlarged part of the right shows the usage of the AES algorithm. Source: NXP.

is a temporal axis going from top to bottom. The entire execution is on the left while the enlarged part on the right shows 9 times 4 rows of instructions indicating the usage of AES: AES is a ten round block cipher where the last round differs slightly from the first nine. Once the target cryptographic cipher has been discovered with the help of this visualization tool, the embedded secret key can be extracted without any technical knowledge by collecting software traces and performing the statistical analysis in an automated fashion using our publicly available tools.

Although we could extract the secret keys from all publicly available white-box challenges we did not investigate the strength of commercially available white-box products since no company, as far as we are aware, has made a challenge publicly available. Unfortunately the well-studied countermeasures from the cryptographic hardware community do not directly apply since they rely on using randomly generated masks. In our security model an adversary can simply disable the entropy of the system rendering the random number generator mute. With this work we have highlighted the risks of relying on pure software implementation for certain use-cases and hope this security assessment will eventually increase the overall level of security for the end-users.

Link:
https://github.com/SideChannelMarvels

References:

[1] S. Chow, P. A. Eisen, H. Johnson, P. C. van Oorschot: “White-box cryptography and an AES implementation”, in SAC 2002, LNCS vol. 2595, pp. 250-270, Springer.
[2] P. C. Kocher, J. Jaffe, B. Jun: “Differential power analysis”, in CRYPTO’99, LNCS vol. 1666, pp. 388-397, Springer.
[3] J. W. Bos, C. Hubain, W. Michiels, P. Teuwen: “Differential Computation Analysis: Hiding your White-Box Designs is Not Enough”, Cryptology ePrint Archive, Report 2015/260, IACR, 2015. Source code: https://github.com/SideChannelMarvels.

Please contact:

Joppe W. Bos
NXP Semiconductors, Belgium
+32479778631,
Joppe.bos@nxp.com

CREDENTIAL: Secure Cloud Identity Wallet

by Nicolás Notario (Atos), Stephan Krenn (AIT), Bernd Zwattendorfer (Stiftung SIC) and Felix Hörandner (TU Graz)

CREDENTIAL (seCuRE clouD idENTIty wALlet) is combining technological advances to create privacy-preserving data storage, data sharing and identity management services.

With rising mobility and internet usage, the demand for digital services is increasing and has reached critical and high assurance domains such as e-Government, e-Health and e-Business. One fundamental building block that is needed for many such applications is secure data sharing functionality. The main ambition of the CREDENTIAL project [L1, L2, L3] is therefore to develop a data sharing platform that provides strong privacy, security, and authenticity guarantees to its users. As a special case, for the sharing of identity data, a privacy preserving identity management service will be implemented.

The security of the developed services will rely on the combination of three key technologies (see Figure 1): end-to-end proxy re-encryption, privacy preserving technologies such as redactable signatures, and strong hardware-based multi-factor authentication.

The first key technology is proxy re-encryption (PRE) [1], which protects the confidentiality of personal data and enables secure end-to-end encrypted data sharing. In general, PRE allows a proxy to transform a ciphertext encrypted for one recipient A to a ciphertext for another recipient B, without getting access to the underlying plaintext or involved private key material during intermediate steps. For this operation, the proxy requires a re-encryption key that was generated from B’s public key as well as A’s private key, who thereby grants delegation rights. In CREDENTIAL, users encrypt their sensitive data for themselves before uploading them to the cloud, which ensures confidentiality. PRE enables users to securely share their encrypted data by providing a re-encryption key that is used by the cloud system to transform the ciphertext for another selected participant. As a result, the confidentiality of the users’ data is protected even in a possibly insecure cloud environment, while the users are still able to securely share their data.

The second main technology included in CREDENTIAL are redactable signature schemes [2], which extend the basic functionality of standard digital signatures as follows: Upon signing, the signer can define specific parts of the message which may later be blanked out (redacted). After receiving the document and the signature, a party can now remove any subset of those predefined parts, and simultaneously modify the signature such that it is valid for the modified message. This way, the authenticity of the revealed parts of the message can be guaranteed, while no information is leaked about the redacted blocks.

Within CREDENTIAL, redactable signatures will be used for the privacy preserving identity management functionality: an authority can sign the users’ electronic identities using redactable signatures. The users can then choose, from their signed identities, which specific attributes they wish to disclose to the service provider (e.g., only the birth data to prove their age).

In order to provide a truthfully secure system, CREDENTIAL follows a ‘Defence in depth’ approach, starting by including in the CREDENTIAL Wallet our third technological pillar, multi-factor authentication protocols that will univocally biometrically link the authentication process to an identity,

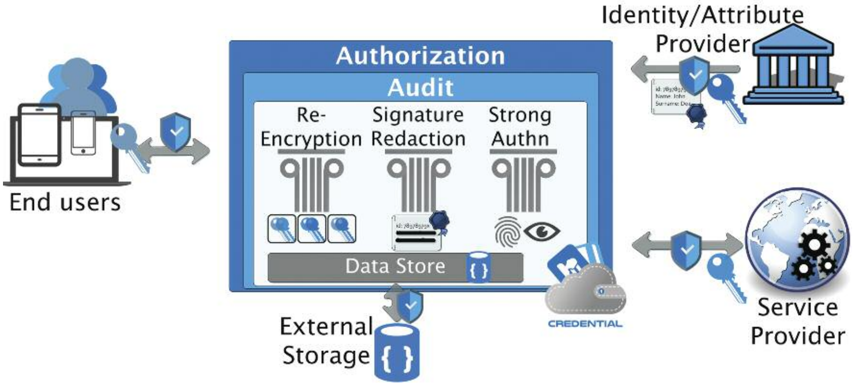


Figure 1: CREDENTIAL high level view and its main pillars.

without the need of disclosing such identity or any personal data to the Wallet or to the service providers.

Finally, one important innovative aspect of CREDENTIAL is its design process, which is carefully planned to have a multi-stakeholder point of view, taking special consideration for user-centric and privacy aspects from social, technical and legal perspectives. On the one hand, and from a functional perspective, stakeholders of three different domains are providing their own view of the system and how it can be leveraged in their own domains. These domain-specific views are consolidated into a logical view of the to-be system, representing it through a Data Flow Diagram (DFD). This DFD illustrates the system's functionality and supports the extraction of valuable insights from a security and privacy perspective. On the other hand, CREDENTIAL combines and leverages both STRIDE and LINDDUN methodologies for security and privacy threat analysis in order to provide a full security and privacy assessment, based on the consolidated view of the system already mentioned. This view is being systematically analysed, identifying, categorising (e.g., identifiability, tampering or linkability threats) and prioritising the different threats that may challenge CREDENTIAL's objectives.

The recently published EU General Data Protection Regulation [3] will be a catalyst for the adoption of CREDENTIAL. The main objectives of this regulation are to strengthen and unify the protection of personal data processing across the EU and to give the user full control of their personal data. To achieve the requirements outlined in this regulation, CREDENTIAL follows a data protection-by-design approach, will provide easier access to own personal data, and will facilitate personal data transfer between service providers.

CREDENTIAL is an EU H2020 three year research project which started in October 2015. The estimated costs of the project are € 6.6 million. The consortium consists of a well-balanced mixture from six European countries consisting of industry partners, universities, and applied research institutions.

Links:
[L1] https://credential.eu/
[L2] https://twitter.com/CredentialH2020
[L3] https://www.linkedin.com/in/credential

References:
[1] Matt Blaze, G. Bleumer, M. Strauss: "Divertible protocols and atomic proxy cryptography", in Proc. of Eurocrypt '98, volume 1403, pages 127–144, 1998.
[2] A. Kundu, E. Bertino: "Structural signatures for tree data structures", in Proc. of the VLDB Endowment 1(1), 138–150, 2008.
[3] Official Journal of the EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Please contact:
Nicolás Notario, Atos Spain (Atos Research & Innovation)
nicolas.notario@atos.net

Stephan Krenn, AIT Austrian Institute of Technology GmbH
+43 664 88256006
Stephan.Krenn@ait.ac.at

GNU Taler: Ethical Online Payments for the Internet Age

by Florian Dold and Christian Grothoff (Inria)

GNU Taler is a new digital payment system currently under development at INRIA. It aims to strike a balance between radically decentralised technologies – such as Bitcoin – and traditional payment methods, while satisfying stricter ethical requirements, for example customer privacy, taxation of merchants and environmental consciousness through efficiency. GNU Taler also addresses micropayments, which are infeasible with currently used payment systems owing to high transaction costs.

Addressing the problem of micropayments is urgent. The overwhelming majority of online journalists, bloggers and content creators currently depend on advertisement revenue for their income. The recent surge of ad-blocking technology is threatening to destroy this primary source of income for many independent online journalists and bloggers. Furthermore the existing advertisement industry is based on the Big Data business model, and users do not only pay with their attention but also with private information about their behaviour. This threatens to move our society towards post-democracy [1]. Our goal is to empower consumers and content creators by offering the choice to opt for micropayments instead of advertisements.

Unlike many recent developments in the field of privacy-preserving online payments, GNU Taler is not based on blockchain technology, but on Chaum-style digital payments [2] with additional constructions based on elliptic curve cryptography. Our work addresses practical problems that plagued previous incarnations of Chaum-style digital payments. The system is entirely composed of free software components, which facilitates adoption, standardisation and community involvement.

From the consumer's perspective, GNU Taler's payment model comes closer to the expectations one has when paying with cash than with credit cards. Customers do not need to authenticate themselves with personally identifying information to the merchant or the payment processor. Instead, individual payments are authorized locally on the customer's computing device. This rules out a number of security issues associated with identity theft. We expect that this will also lower the barrier for online transactions due to the lower risk for the customer. With current payment solutions, the risk of identity theft accumulates with every payment being made. With our payment system, the only risk involved with each individual payment is the amount being paid for that single transaction.

In GNU Taler, the paying customer is only required to disclose minimal private information (as required by local law), while the merchant's transactions are completely transparent to the state and thus taxable. Taxable merely means that the state can obtain the necessary information about the contract to levy common forms of income, sales or value-added taxes, not that the system imposes any particular tax code. When customers pay, they use anonymised digital payment tokens to sign a contract with the merchant. The digitally signed contract is proposed by the merchant and is supposed to contain all the information required for taxation – which typically excludes the identity of the customer. Later, the state can obtain the contract by following a chain of cryptographic tokens, starting from a token in the wire transfer from the GNU Taler payment system operator to the merchant. The payment system operator only learns the total value of a contract, but no further details about the contract or customer.

To pay with GNU Taler, customers need to install an electronic wallet on their computing device. Once such a wallet is present, the fact that the user does not have to authenticate to pay fundamentally improves usability. We are already seeing today that electronic wallets like GooglePay are being deployed to simplify payments online. However, the dominant players mostly simplify credit card transactions without actually improving privacy or security for citizens. GNU Taler is privacy-preserving free software and both technically and legally designed to protect the interests of its users.

Christian Grothoff

We plan to use GNU Taler as the basis for future research that investigates censorship-resistant news distribution in decentralised social networks. In addition to online payments, we eventually want to adapt GNU Taler to mobile payments with NFC-enabled devices. We hope that mobile Taler payments will further the proliferation of local currencies (such as the Abeille in France), which are currently popular in parts of Europe, but suffer from practical problems such as easy counterfeiting and the limitation to physical coupons.

GNU Taler was started at TU Munich in April 2014 and is now being coordinated by the TAMIS team[L1] at INRIA Rennes, with contributions from the free software community at large and the GNUnet project[L2] in particular. The initial research is being funded by ARED and the Renewable Freedom Foundation [L3], but we plan to launch a startup to drive the commercial adaptation of the technology. We encourage readers to try our prototype for GNU Taler at https://demo.taler.net/.

Links:

[L1] https://www.inria.fr/en/teams/tamis
[L2] https://gnunet.org/
[L3] https://renewablefreedom.org/

References:

[1] R. Stallman: "How Much Surveillance Can Democracy Withstand?", Wired, Oct. 2013, http://www.wired.com/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/

[2] Chaum et al.: "Untraceable electronic cash", in Proc. on Advances in cryptology, Springer-Verlag New York, Inc., 1990.

Please contact:

Florian Dold
Inria, France
+33 2 99 84 25 66
florian.dold@inria.fr

Christian Grothoff
Inria, France
+33 2 99 84 71 45
christian@grothoff.org

A Tool-Chain for High-Assurance Cryptographic Software

by José Almeida, Manuel Barbosa, Hugo Pacheco and Vitor Pereira (INESC TEC)

Cryptography is an inherently interdisciplinary area and the development of high-quality cryptographic software is a time-consuming task drawing on skills from mathematics, computer science and electrical engineering, only achievable by highly skilled programmers. The challenge is to map high-level cryptographic specifications phrased using mathematical abstractions into efficient implementations at the level of C or assembly that can be deployed on a target computational platform, whilst adhering to the specification both in terms of correctness and security. The High Assurance Software Laboratory at INESC-TEC maintains a domain-specific toolchain for the specification, implementation and verification of cryptographic software centred on CAO, a cryptography analyses and operations-aware language.

There is a high risk associated with poor cryptographic implementations, as is shown by frequent (and in some cases catastrophic) security breaches directly attributed to implementation errors in widely used cryptographic libraries [L1,L2]. One of the causes of these breaches in widely tested software is the semantic gap between theoretical cryptographic specifications and their concrete implementations. Effectively closing this gap is a huge challenge, especially when attackers may exploit physical vulnerabilities not covered by the specification, commonly known as side-channel attacks.

To answer this demand, research in the crossover area between cryptography and programming languages has been growing steadily in the last decade, as demonstrated by the Computer Aided Cryptography Engineering (CACE) EU/FP7 project that focused on developing tools to automate the production of high quality cryptographic software at a lower cost. The CAO cryptographic domain-specific language [L3,1,2], initially developed at the University of Bristol and subsequently re-engineered within CACE, enables the natural translation of cryptographic constructions (as found in standards and scientific articles) to high-level prototype implementations. The driving principle behind the design of CAO is to support cryptographic concepts as first-class features.

CAO adopts some features familiar to imperative programmers but has a very simple programming model by design. For instance, it does not support input/output, as it is targeted at implementing the core components of cryptographic libraries. Conversely, it offers a very rich type system tuned to the specific domain of cryptography. In recent versions of the language, CAO programs can be seen as generic specifications that, like pure theoretical cryptographic constructions, are defined abstractly for a set of parameters satisfying certain base assumptions. The CAO developer is assisted by an interpreter that enables fast prototyping and debugging, and a type-checker that enforces strong typing and performs extensive preliminary validation of the code, extracting rich crucial information for further processing down the chain. CAO specifications can also be validated in a fully automatic way for parameter consistency properties in later versions of the type checker.

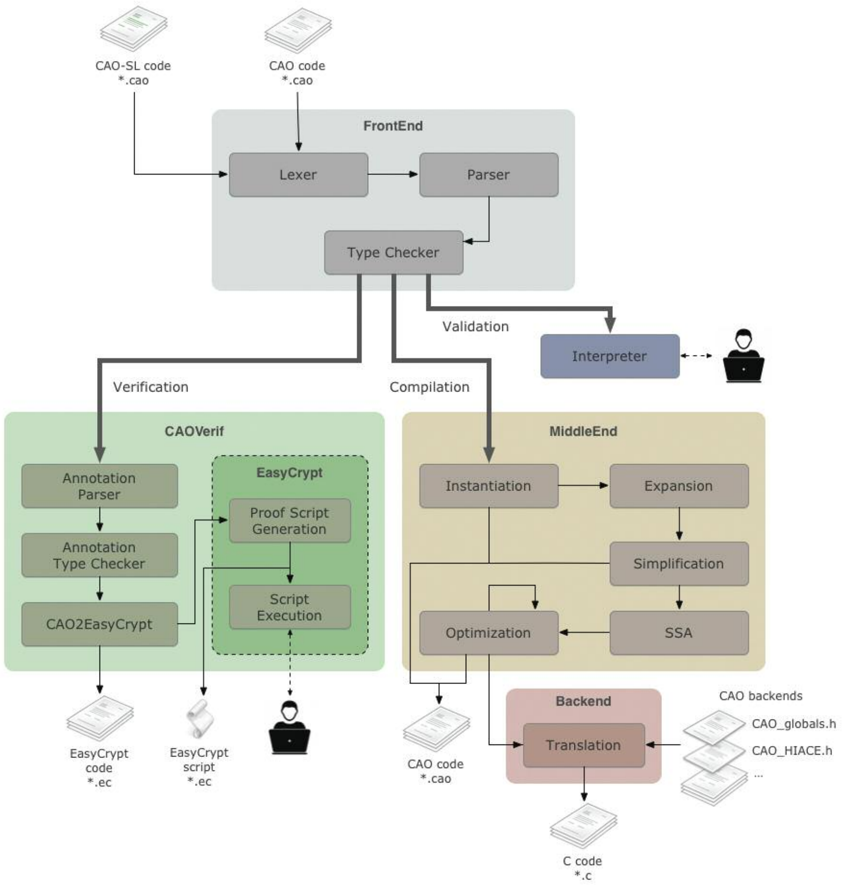


Figure 1: The CAO toolchain.

The CAO tool chain (Figure 1) also provides an optimising compiler for the automatic generation of high-security and high-speed cryptographic C implementations from high-level CAO specifications. The inner workings of the CAO compilation process mimic those performed by cryptography practitioners.

The CAO specification is first converted into a canonical CAO subset through a series of both general and domain-specific CAO-to-CAO transformation and optimisation steps.

In a second phase, the intermediate CAO code is compiled into C code in which CAO native operations are implemented as a C backend library that may be either pre-compiled or dynamically generated. This flexibility allows adapting the CAO compiler to the wide variety of computational platforms in which cryptographic code is deployed in the real world. The CAO compiler offers a generic C backend supporting the entire functionality of the CAO language and capable of targeting any computational platform with a C/C++ compiler. In the context of the SMART ENIAC/JU project, a very specific backend supporting only a limited subset of the CAO language has been developed to target a severely constrained proprietary microcontroller that resides in standalone PCM memories, while preserving the remaining high-level infrastructure.

Seeing CAO programs as specifications, it becomes natural to express the properties of CAO programs in the same abstract setting, i.e., directly in the CAO language. For this reason, the CAO toolchain also incorporates a formal verification tool that permits reasoning about arbitrarily complex properties of CAO programs (specified as in-code annotations) in a semi-automated environment, by embedding them in EasyCrypt [L4,3], a tool-assisted framework for specifying and verifying the security of cryptographic constructions. Using EasyCrypt, the developer is now able to additionally perform safety, correctness and security proofs of cryptographic algorithms written in CAO.

The joint effort across two European projects brought the CAO toolchain to life and came to fruition by demonstrating that a domain-specific high-level cryptographic language can be used to guide, validate and automate the development of low-level high-assurance cryptographic implementations for diverse computational platforms. Ongoing and future work will broaden the applications of the CAO family of tools by further exploring the integration with EasyCrypt and developing new backends. In particular, we envision the implementation of a backend for a cryptography-oriented low-level language such as qhasm, in which assembly level programs are seen as first class representations of cryptographic computations.

Links:

[L1] http://heartbleed.com/
[L2] http://resources.infosecinstitute.com/beast-vs-crime-attack/
[L3] https://hackage.haskell.org/package/cao
[L4] http://www.easycrypt.info

References:

[1] M. Barbosa, D. Castro, Paulo F. Silva: "Compiling CAO: From Cryptographic Specifications to C Implementations." POST 2014: 240-244.
[2] M. Barbosa, et al.: "Type Checking Cryptography Implementations", FSEN 2011: 316-334.
[3] G. Barthe et al.: "Computer-Aided Security Proofs for the Working Cryptographer", CRYPTO 2011: 71-90.

Please contact:

Manuel Bernardo Martins Barbosa
HASLab, INESC TEC and DCC FCUP
mbb@dcc.fc.up.pt

Code-Based Cryptography: New Security Solutions Against a Quantum Adversary

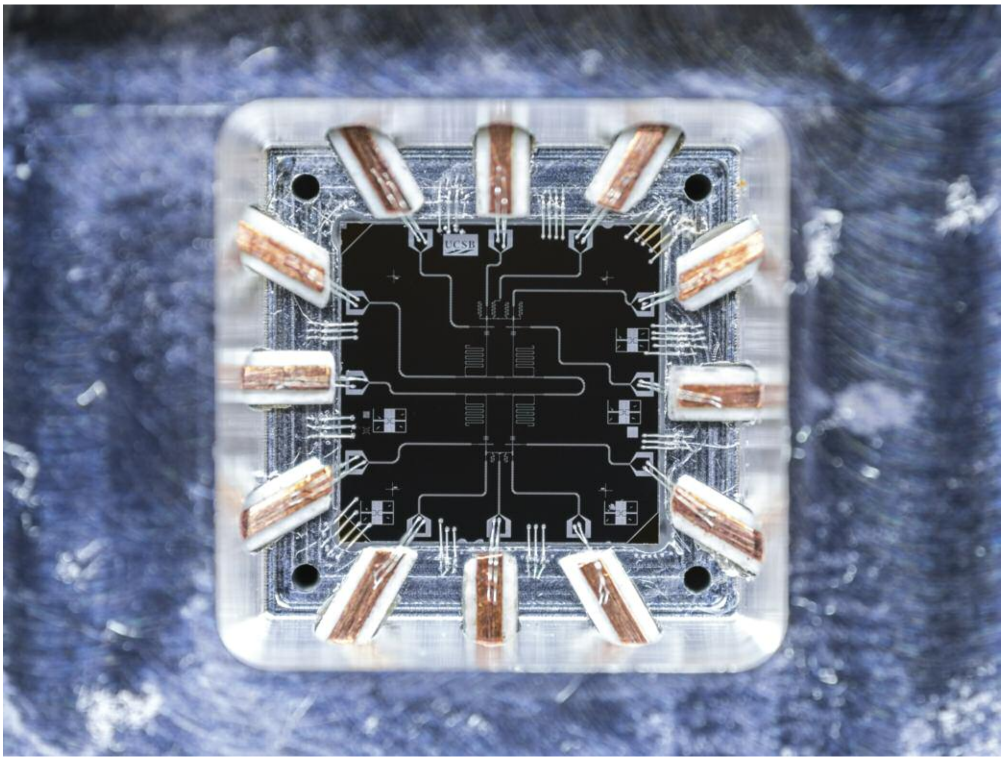
by Nicolas Sendrier and Jean-Pierre Tillich (Inria)

Cryptography is one of the key tools for providing security in our quickly evolving technological society. An adversary with the ability to use a quantum computer would defeat most of the cryptographic solutions that are deployed today to secure our communications. We do not know when quantum computing will become available, but nevertheless, the cryptographic research community must get ready for it now. Code-based cryptography is among the few cryptographic techniques known to resist a quantum adversary.

Since their appearance in the mid seventies, public key (or asymmetric) cryptographic primitives have been notoriously difficult to devise and only a handful of schemes have emerged and have survived cryptanalytic attacks. In particular, the security of nearly all public key schemes used today relies on the presumed difficulty of two problems, namely factoring of large integers and computing the discrete logarithm over various groups.

The security of all these schemes was questioned in 1994 when Shor showed that a quantum computer could efficiently solve these two problems [1]. We do not know when large enough quantum computers will be built, but this will have dramatic consequences because it will break all popular public-key cryptosystems currently in use.

Clearly, the cryptographic research community has to get ready and prepare alternatives. Those alternatives have to be ready, not only for tomorrow in case of a scientific advance (which might even be of a different nature than those that are foreseen today), but also for now, in order to provide long term security – i.e., several decades – to the data that is encrypted or digitally signed today. This effort has started already with PQCRYPTO [L1] of the European Horizon 2020 program. Furthermore, in August, 2015, NSA announced that it is planning to transition 'in the not too distant future' to a



Superconducting Quantum Circuit. Photo: Michael Fang, Martinis Lab (UCSB and Google).

new cipher suite that is resistant to quantum attacks.

The NIST has also released a report on post-quantum cryptography [L2] explaining that ‘we must begin now to prepare our information security systems to be able to resist quantum computing’. During the Seventh International Conference on Post-Quantum Cryptography, held in Fukuoka, Japan, in February 2016, NIST announced that a call for establishing new public key standards that are quantum resistant will be issued by fall 2016.

Code based public key cryptography

Code-based cryptography is one of the main post-quantum techniques currently available, together with lattice-based cryptography, multivariate cryptography, and hash-based cryptography. The first code-based cryptosystem was proposed by Robert McEliece in 1978. It belongs to a very narrow class of public-key primitives that so far have resisted all cryptanalytic attempts. McEliece’s idea was to use as cryptogram a word of a linear error correcting code (a Goppa code in this case) to which random errors were added. The legitimate user, who knows a fast decoding algorithm, can remove the error. The adversary is reduced to a generic decoding problem, which is believed to be hard on average including against a quantum adversary.

France is leader in code-based cryptography and a working group was formed at the end of 2014 to gather French groups working on this topic. It includes in particular two Inria project-teams (one in Paris, one in Saclay), the universities of Limoges and Rouen, and Telecom SudParis. Among the projected actions of this working group, one is to devise a strategy to incite and support initiatives to answer to the forthcoming NIST call, in particular by identifying topics and primitives of interest.

Code-based systems are inherently fast but suffer from a rather large public key size. There have been several recent breakthroughs which reduce the key size to a few thousand bits:

- For instance, systems based on MDPC codes [2] enjoy a strong and novel security reduction and require only very low computing resources, which make them very attractive even for embedded devices.
- Rank metric (instead of the usual Hamming metric) codes provide new code-based primitives [3] with very short keys, relying on similarly hard computational problems, also seem very promising.

Those, together with other more traditional code-based cryptographic solutions, could certainly form part of the new asymmetric cryptographic standards that will emerge in the coming decade.

Links:

[L1] http://cordis.europa.eu/project/rcn/194347_en.html

[L2] http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

References:

[1] P.W. Shor: “Algorithms for quantum computation: Discrete logarithms and factoring”, in FOCS 94, IEEE.

[2] R. Misoczki, J.-P. Tillich, N. Sendrier, P. S. L. M. Barreto: “New variants from moderate density parity-check codes”, in ISIT 2013, IEEE.

[3] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor: “New results for rank-based cryptography”, in AFRICACRYPT 2014, Springer.

Please contact:

Nicolas Sendrier, Jean-Pierre Tillich
Inria, France
nicolas.sendrier@inria.fr, jean-pierre.tillich@inria.fr

Using Cryptography to Control Your Data at a Distance

by Colin Boyd, Gareth T. Davies, Kristian Gjøsteen (NTNU), Håvard Raddum and Mohsen Toorani (University of Bergen)

Most people and companies store important information using cloud storage services that are outside their direct control. The information may be personal, such as emails, photos and videos, medical records and financial information. How can we be sure that our data is safe from the prying eyes of cloud operators, other cloud users or outside agencies? How can we be sure that our data will remain available to us when we need it?

Security of information is an essential aspect of business and government activity, whether it relates to protection of corporate knowledge, integrity of financial transactions, or reliable storage and transmission of data. The transition to cloud computing necessitates extra security measures to protect valuable data that is no longer under the direct control of its owner. This issue has been widely recognized; the industry-led Cloud Security Alliance (www.cloudsecurityalliance.org) was formed in 2008, and the NIST guidelines on cloud security and privacy were published in 2011 [2]. The Snowden revelations of 2013 and 2014 have changed the IT security priorities and it is now understood that there is an urgent need for protection of personal, business, and government data against pervasive monitoring and infiltration.

The collaborative project Cryptographic Tools for Cloud Security, funded by the Norwegian Research Council from 2016 to 2019, will study new cryptographic tools to enable cloud security against powerful attackers. The research involves experts at Norwegian University of Science and Technology and University of Bergen, in cooperation with University of Mannheim.

The new cryptographic primitives, protocol and models that we will develop will lead to theoretical advances as well as practical outcomes. We are following the current important trend in cryptographic research to connect rigorous results strongly to real-world usage. This is now both possible and timely given that a level of maturity has been reached in cloud computing which will allow us to demonstrate the practical effectiveness of our proposals, to complement the theoretical analysis.

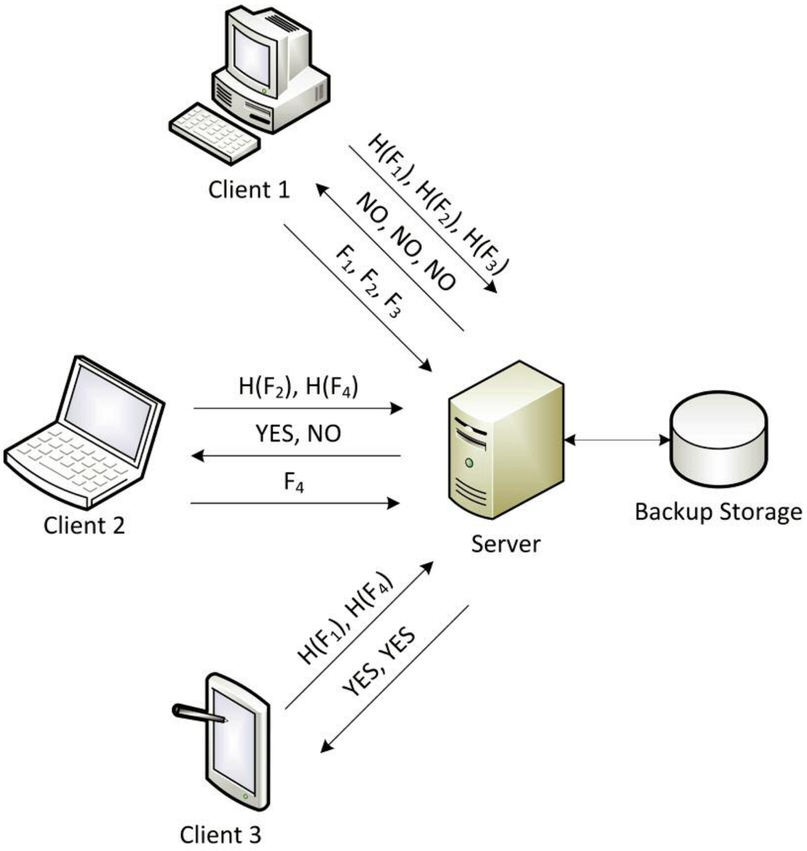


Figure 1: Simple client-side deduplication in which different clients sequentially request the server to store different files F_i. The client first sends hashes of the files, $H(F_i)$. The server checks if files with those hash values are already stored and, if not, the client sends the files.

Cryptography has traditionally been used to protect data while it is being transmitted over insecure networks or while it is at rest in static storage. These services remain important in the cloud as it is essential to protect both confidentiality and integrity of data while it is transmitted between client and cloud server and while it is at rest in cloud storage. At the same time, new approaches are also required for at least two reasons.

- Data in cloud storage is frequently shared between multiple parties, may be stored in geographically distributed nodes, and needs to be updated incrementally. This requires the development of practical techniques to allow cloud users to efficiently verify the integrity and availability of their data, including where it is located.
- We often want to process data in the cloud without necessarily trusting the cloud operator. Therefore, we want to be able to compute on encrypted data. This can include basic operations such as searching through encrypted records through to full-scale processing of any function. Gentry's theoretical breakthrough of fully homomorphic encryption in 2009 remains impractical in general, but exploring compromises which are both efficient and secure is an important theme of our project.

One main area of focus of our research is secure deduplication. By deduplication we mean that the server stores only a single copy of each file, regardless of how many clients asked to store that file, in order to make significant savings in both storage and bandwidth. Note that large files such as movies and software are very likely to be shared by many users. Generally, deduplication can be at client-side (which saves both storage and bandwidth) or server-side (which only saves storage). However, deduplication contrasts with users' desire for security: if two users A and B upload the same file encrypted under independent keys kA and kB, the server will receive independent ciphertexts and will thus be unable to perform deduplication.

One possible solution is to derive the encryption key from the file itself [1]; but this approach will only give security against an adversarial server with the unrealistic assumption that files are unpredictable. Other security issues arise irrespective of any encryption. For example, suppose that the cloud service provider (CSP) employs client-side deduplication (see Figure 1) in which the client first sends a short identifier to the CSP and the CSP tells the client to upload the full file only if it is not already stored. An adversarial user can create a template of a file (e.g., an employment contract of Bob) and attempt a number of uploads of files that only differ in one detail (e.g., salary) and at some point the upload will be halted by the CSP, meaning that this file is already stored (and thus learns Bob's salary) [3]. We are working on schemes which defend against such attacks by differentiating between files that are popular (and thus promise significant savings from deduplication) and those that are not.

References:

[1] J. R. Douceur et al.: "Reclaiming space from duplicate files in a serverless distributed file system", in IEEE Distributed Computing Systems, 2002, pp 617–624. IEEE, 2002.

[2] T. Grance, W. Jansen: "Guidelines on Security and Privacy in Public Cloud Computing", Special Publication 800-144, National Institute of Standards and Technology, December 2011.

[3] D. Harnik, B. Pinkas, A. Shulman-Peleg: "Side channels in cloud services: Deduplication in cloud storage", IEEE Security & Privacy, 8(6):40–47, 2010.

Please contact:
Colin Boyd, NTNU, Norway
colin.boyd@item.ntnu.no

A New Architecture for Developing Cryptographic Cloud Services

by Thomas Lorünser (AIT Austrian Institute of Technology GmbH), Daniel Slamanig (TU Graz), Thomas Länger (University of Lausanne) and Henrich C. Pöhls (Universiy of Passau)

The EU Horizon 2020 PRISMACLOUD research project is dedicated to enabling secure and trustworthy cloud-based services by improving and adopting novel tools from cryptographic research.

Relying solely on legal contracts and trusting the cloud is not a solution to the problems of security and privacy in the cloud. PRISMACLOUD [L1] [1] tackles these issues with the help of strong cryptographic primitives. Currently, the use of the cloud is not feasible for many security and privacy conscious purposes, such as eHealth and eGovernment, owing to the low pervasion of existing strong cryptographic primitives.

In order to tackle and organise the complexity involved with the construction of cryptographically secured services, we introduce a conceptual model denoted as the PRISMACLOUD architecture [2], which is organised in four tiers (Figure 1). These layers of abstraction help to specify and analyse security properties on different levels; they also define connection points between the different disciplines involved in the creation of secure and privacy preserving cloud services: cryptographers, software engineers/developers and cloud service architects. On the uppermost (i) application layer are the end user applications. Applications use the cloud services of the (ii) services layer to achieve the desired security functionalities. The cloud services specified there are a representative selection of possible services that can be built from the tools organised in the (iii) tools layer. In particular, they represent a way to deliver the tools to service developers and cloud architects in an accessible and scalable way. Together the tools constitute the PRISMACLOUD toolbox. Tools encapsulate the required cryptographic primitives and protocols from the (iv) primitives layer, which is the lowest layer of the PRISMACLOUD architecture.

Instead of directly integrating cryptography into applications or services, the PRISMACLOUD architecture introduces the tool layer as an additional level of abstraction: A tool represents a basic functionality and a set of requirements it can fulfil. It can therefore be regarded as an abstract concept which could be realised as a piece of software, e.g., a library, which is composed of various primitives which can be parametrised in various ways. From the tools of the toolbox, the services of the next layer can be built. A service can therefore be seen as a customisation of a particular tool for one specific application. It is a way to deliver the tool to system and application developers, the users of the tools, in a preconfigured and accessible way. They will be able to integrate the services without a deeper understanding of tools and primitives and ideally without even being an IT security expert. A service provides a full implementation of all the required features as well as concrete interfaces in the form of an application programming interface (API), suitable to be deployed as a cloud service. In PRISMACLOUD we have chosen to specify a selection of services that we will develop during the project that can showcase the suitability of the chosen primitives and the tools constructed from them within the selected use cases. The use cases also provide a way to validate the new concept in real world applications.

With this architecture we encapsulate the cryptographic knowledge needed on the lower layer inside the tools and their correct usage inside services. Building the tools requires in-depth cryptographic and software development knowledge. However, once built they can be used by cloud service designers to build cryptographically secure and privacy-preserving cloud services. These cloud services are then exposed to application developers who can combine them with other technologies and services into the real end-user applications.

In addition to the advantages outlined above, the PRISMACLOUD architecture further facilitates exploitation of project results. Each layer provides a dedicated project outcome with a specific exploitation path. Research progress on the layer of primitives leads to scientific progress and typically associated exploitation. Tool developers will be able to commercialise software developments and intellectual property rights. Service developers are able to quickly transform project results into products. Their services will be almost ready for deployment in production environments of cloud providers, hence they will be accessible to a broader community relatively soon after the project's end. The project also features a specific standardisation activity to disseminate the tools' specifications into standards to support further adoption.

What we termed the PRISMACLOUD architecture can be seen as a recipe to bring cryptographic primitives and protocols into cloud services that empower cloud users to build more secure and more privacy-preserving cloud services. In its core, we encapsulate the cryptographic knowledge in specific tools and offer basic but cryptographically enhanced functionality for cloud services. In PRISMACLOUD we will harvest the consortium members' cryptographic and software development knowledge to build the tool box and the services. The resulting PRISMACLOUD services hide and abstract away from the core cryptographic implementations and can then be taken by cloud service designers. On this level of cloud services, the PRISMACLOUD services will show how to provision (and potentially market) services with cryptographically increased security and privacy.

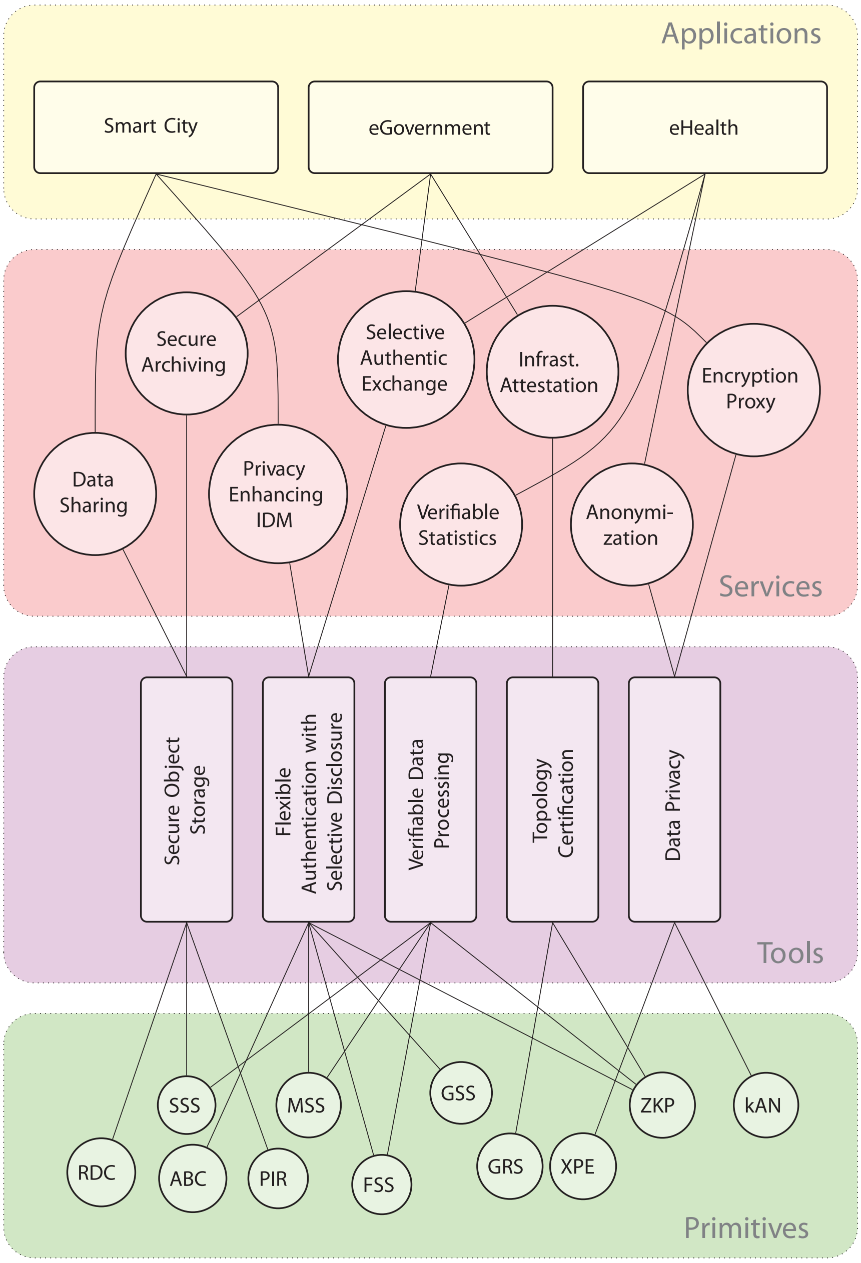


Figure 1: The PRISMACLOUD Architecture (Primitives abbreviations: RDC: Remote Data Checking; SSS: Secret Sharing Schemes; ABC: Attribute-Based Credentials; PIR: Private Information Retrieval; MSS: Malleable Signature Schemes; FSS: Functional Signature Schemes; GSS: Group Signature Schemes; GRS: Graph Signature Schemes; XPE: Format- and Order-Preserving Encryption; ZKP: Zero-Knowledge Proofs; kAN: k-Anonymity).

Links:
[L1] https://prismacloud.eu,
https://at.linkedin.com/in/prismacloud,
@prismacloud,
http://twitter.com/prismacloud,
http://cordis.europa.eu/project/rcn/194266_en.html

References:

[1] T. Lorünser et al.: "Towards a New Paradigm for Privacy and Security in Cloud Services", Cyber Security and Privacy, Vol 530 of CCIS, Springer, 2015.
[2] T. Lorünser, et al.: "PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services", 1st Workshop on Security, Privacy, and Identity Management in the Cloud, ARES 2016, to appear.

Please contact:

Thomas Lorünser
AIT Austrian Institute of Technology GmbH
+43 664 8157857
Thomas.Loruenser@ait.ac.at

Deprecating an Internet Security Standard with Cryptanalysis

by Marc Stevens (CWI)

An international team of cryptanalysts from CWI, Inria and NTU Singapore broke the core of the SHA-1 internet security standard in October 2015. They projected that breaking SHA-1 is much cheaper and can be achieved earlier than international security experts expected, which gained a lot of attention in the media. The team urged the industry to retract the standard earlier than planned. Their results ensured that an industry ballot to extend the issuance of SHA-1 certificates was withdrawn.

SHA-1 is a cryptographic algorithm to securely compute message fingerprints, which was designed by the NSA in 1995. It became an industry standard that is commonly used for digital signatures, which secure credit card transactions, electronic banking and software distribution. It is fundamental to internet security – for HTTPS (SSL/TLS) security, for example.

SHA-1 is a ‘hash function’. It generates from input, such as text or code, a short string of letters and numbers (a hash), which serves as a digital fingerprint for that message. Even a small change in the input, such as changing one letter in a message, will generate a very different and unpredictable output. When two different messages lead to the same hash, this is called a collision. Such collisions allow forgeries of digital signatures – a catastrophe for banking transactions, secure e-mails, and software downloads.

The industry standard was already theoretically broken in 2005 [1] but for a long time it remained difficult to make a practical attack. However, the researchers combined advanced mathematical methods by using graphics cards for their computations to speed up the computations and make the attack much more cost effective.

In September, a joint effort by CWI, Inria and NTU Singapore – also known as ‘the SHAppening’ [L2] – led to a successful ‘freestart collision attack’ on SHA-1, breaking the full inner layer of SHA-1. In early autumn, 2015, the researchers then estimated that it would cost only $US75,000-120,000 to rent Amazon EC2 cloud over a few months and conduct a full SHA-1 collision [2]. This indicated that collisions were already within the resources of criminal syndicates, almost two years earlier than previously expected [3], and one year before SHA-1 would be marked as unsafe in modern internet browsers in January 2017, in favour of its secure successor SHA-2.

Google Chrome users receive a warning when a certificate is signed with a SHA-1 based signature issued after 2015. Picture: Marc Stevens.

The team therefore recommended that SHA-1 based signatures should be marked as unsafe much sooner. In particular, they strongly urged against a proposal to extend issuance of SHA-1 certificates with another year in the CA/Browser Forum, for which the voting was scheduled briefly after the announcement. The proposed extension was not just because some companies were not ready yet, but also because millions of users with old software, mostly from developing countries, would not be able to access some websites anymore. However, owing to the demonstrated insecurity, the proposal for extension was withdrawn by Symantec before the meeting. Also the upcoming TLS 1.3 standard deprecated SHA-1 as a consequence of this team’s results. Mozilla, Google and Microsoft also adopted their planning regarding SHA-1.

“Although this is not yet a full attack, the current attack is not the usual minor dent in a security algorithm, making it more vulnerable in the distant future,” says Ronald Cramer, head of CWI’s Cryptology group [L1]. The research team adds: “As SHA-1 underpins more than 28 percent of existing digital certificates, the results of real-world forgeries could be catastrophic. We hope the industry has learned from the events with SHA-1’s predecessor MD5 and in this case will retract SHA-1 before examples of signature forgeries appear in the near future.”

The research team consisted of Marc Stevens (CWI), Pierre Karpman (Inria and NTU Singapore) and Thomas Peyrin (NTU Singapore). The research was partially funded by the Netherlands Organisation for Scientific Research Veni Grant 2014, the Direction Générale de l’Armement, and the Singapore National Research Foundation Fellowships 2012. The results have been presented at the 35th Annual IACR EUROCRYPT 2016 conference.

Links:
[L1] https://www.cwi.nl/research-groups/Cryptology
[L2] https://sites.google.com/site/itstheshappening/

References:

[1] X. Wang, Y. L. Yin, H. Yu: “Finding Collisions in the Full SHA-1”, CRYPTO 2005, LNCS, vol. 3621, pp. 17-36, Springer, 2005. http://link.springer.com/chapter/10.1007%2F11535218_2
[2] M. Steven s, P. Karpman, T. Peyrin: “Freestart collision for full SHA-1”, EUROCRYPT 2016, LNCS, vol. 9665, pp. 459-483, Springer, 2016, http://link.springer.com/chapter/10.1007%2F978-3-662-49890-3_18
[3] M. Stevens: “New collision attacks on SHA-1 based on optimal joint local-collision analysis”, EUROCRYPT 2013, LNCS, vol. 7881, pp. 245-261, Springer, 2013. http://link.springer.com/chapter/10.1007%2F978-3-642-38348-9_15

Please contact:

Marc Stevens, CWI, The Netherlands
marc.stevens@cwi.nl

Thwarting Uniqueness in Datasets of Spatiotemporal Trajectories

by Marco Gramaglia (UC3M and IMDEA Networks) and Marco Fiore (CNR-IEIIT)

Pervasive mobile communications make it easy to track individuals, a practice that both fosters new knowledge and raises privacy concerns. The uniqueness of human mobility patterns is critical to the latter, as it facilitates user re-identification in naively anonymised datasets. We propose a solution that guarantees the indistinguishability of spatiotemporal trajectories – an important step towards the open access of privacy-preserving datasets.

Collecting data generated by widespread digital transactions is an increasingly common practice. The likes of telecommunication network operators, mobile service providers, app developers and financial companies have the possibility to track the movements, preferences, activities and habits of large populations of individuals. Mining of such high-dimensional big data paves the way to new, compelling models across economic and scientific domains that could not be foreseen until a few years ago, and are in some cases becoming part of our everyday life. The other side of the coin is the emergence of novel privacy issues related to the collection, storage and exploitation of such sensible information.

A prominent case study are datasets of spatiotemporal trajectories collected, for example, via mobile network records available to telecommunication operators or geo-referenced time-stamped check-ins recorded by mobile applications. They have become an important instrument in large-scale analyses across a number of disciplines, including physics, sociology, demography, epidemiology, transportation and computer sciences: a recent survey is available in [1]. These datasets are commonly anonymised by replacing identifiers (e.g., name, phone number, account number, etc.) with random strings or non-reversible hashes.

However, this simple solution does not provide protection against attacks on individual privacy. Specifically, datasets of spatiotemporal trajectories suffer from elevate uniqueness: the distinctive patterns of each user allow him or her to be pinpointed among millions of other individuals with minimal knowledge, e.g., where he was at any five time instants during one year [2]. Uniqueness does not imply re-identification on its own; yet, it can pave the way to cross-database linkage.

Mitigating the uniqueness of spatiotemporal trajectories is then a very desirable facility towards robust (and open) datasets. However, attempts at ensuring indistinguishability of spatiotemporal trajectories through legacy techniques have failed. The typical approach is generalization: precision in space and time is reduced for all data up to the point where no individual trajectory is uniquely distinguishable in the dataset. Yet, the high dimensionality of the data (i.e., the large number of spatiotemporal samples recorded for each user) makes generalization ineffective: uniqueness is not removed even under very coarse spatial (i.e., tens of km) and temporal (i.e., days) granularities that disrupt data utility [2].

We perform an extensive analysis of the root causes behind the high uniqueness and poor anonimisability of datasets of spatiotemporal trajectories. By studying real-world datasets, we observe that typical human movement patterns are easily anonymised for most of their span (e.g., consider the mass of commuters sharing the same route on trains running between two cities in the morning and afternoon, every day). Each individual might also feature a small but not negligible number of 'peculiar' movements (e.g., one commuter goes to play a five-a-side football game in a pitch near his workplace on Tuesdays, delaying his trip back home). These latter movements result in spatiotemporal samples that are extremely hard to hide, and doom all other samples in the dataset to undergo a very

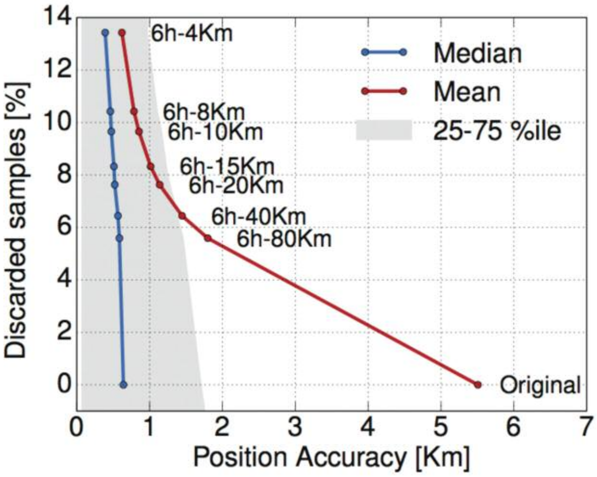


Figure 1: Spatial accuracy in a dataset 2-anonymised with GLOVE.

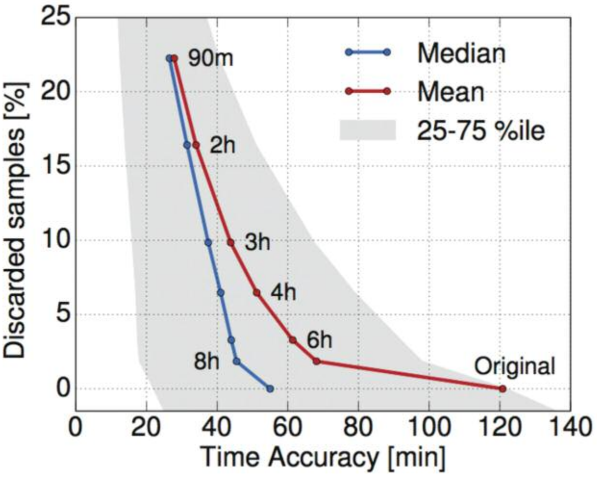


Figure 2: Temporal accuracy in a dataset 2-anonymised with GLOVE.

high loss of accuracy if they are to be anonymised.

Building on these findings, we have developed GLOVE, an algorithm that runs classical generalisation on a per-sample basis, i.e., it enforces the minimum reduction of granularity required to hide each sample separately, so that each complete trajectory is indistinguishable from other k-1 trajectories in the same dataset. GLOVE thus implements the ‘k-anonymity privacy criterion’. Our approach proves very effective: when run on large-scale datasets describing weeks of mobility of tens of thousands of users, GLOVE completely removes data uniqueness. More importantly, it does so while retaining a substantial level of accuracy. Figures 1 and 2 show the accuracy in space and time (x axes) of the GLOVE-generalised samples in a 2-anonymised dataset, expressed as the average, median and first-third quartiles of the overall distribution. Different points on the curves map to thresholds (tags along curves) beyond which the generalisation cost is considered excessive, and samples are discarded: clearly, lower thresholds yield a better precision but discard more samples (y axis).

Overall, one can expect good precision (in the order of hundreds of metres in space and of tens of minutes in time) in the anonymised data; fine-tuning is then possible by using the suppression thresholds above.

For a detailed description of our analysis, the GLOVE algorithm, and the performance evaluation, we refer the reader to [3].

References:
[1] D. Naboulsi et al.: “Large-scale Mobile Traffic Analysis: a Survey,” IEEE Communications Surveys and Tutorials, 18(1), 2016.
[2] Y. de Montjoye et al., “Unique in the Crowd: The privacy bounds of human mobility,” Nature Scientific Reports, 3(1376), 2013.
[3] M. Gramaglia, M. Fiore, “Hiding Mobile Traffic Fingerprints with GLOVE,” ACM CoNEXT 2015, Heidelberg, Germany, December 2015.

Please contact:
Marco Fiore, CNR-IEIIT, Italy
+39 011 090 5434
marco.fiore@ieiit.cnr.it

Using JavaScript Monitoring to Prevent Device Fingerprinting

by Nataliia Bielova, Frédéric Besson and Thomas Jensen (Inria)

Today’s Web users are continuously tracked as they browse the Web. One of the techniques for tracking is device fingerprinting that distinguishes users based on their Web browser and operating system properties. We propose solutions to detect and prevent device fingerprinting via runtime monitoring of JavaScript programs.

The use of sophisticated web tracking technologies has grown enormously in the last decade. Advertisement companies and tracking agencies are collecting increasing amounts of data about Web users in order to better advertise their products. Social media plugins also collect data to learn about online habits and preferences of their users. In the last five years, researchers have started to examine the mechanisms used for Web tracking. Recent research has shown that advertising agencies and networks use a wide range of techniques in order to track users across the Web.

Web tracking via cookies is well known. Cookies are stored in a user’s browser so that the tracking script can immediately recognise the user. However, another group of tracking techniques, called ‘device fingerprinting’, does not require storing anything in a user’s browser. Fingerprinting scripts make a snapshot of the configuration of the Web browser and operating system properties and then are able to distinguish a particular user from all other website visitors. Unlike cookies, this technique also works perfectly across sites, meaning that the tracker will know all the web sites that the user has visited if this tracker’s script is present on these sites. The Panopticlick project [L1] by Electronic Frontier Foundation was the first to demonstrate the power of fingerprinting in 2010. Since then, researchers have found new ways to distinguish Web users, for example through HTML5 Canvas fingerprinting, which was discovered only in 2012.

Within the French ANR projects Seccloud (Security of cloud programming) and AJACS (Analyses of JavaScript Applications: Certification and Security), in INRIA, we have proposed a new solution to protect Web users from being fingerprinted. We are developing a tool that formally guarantees that the scripts run in a browser are not fingerprinting the user. This can be done either by detecting and blocking tracking scripts, or by modifying their tracking behaviour. To do so, we developed a monitor that analyses a potentially tracking script, and computes how much fingerprinting information this script collects. The more information it collects, the more easily it can distinguish the user from all other visitors.

As a first step, we have developed a methodology to analyse how much identifiable information a tracker may learn about a user through an execution of a script. While a script runs, it collects some data about the Web browser and operating system configuration and sends this data back to the server. How much identifiable information did the tracker learn by observing this data? We have shown that this problem can be stated as an information-flow problem that answers the question: what is the probability that a server can identify a user after analysing the output of the script? If the probability is low, the user

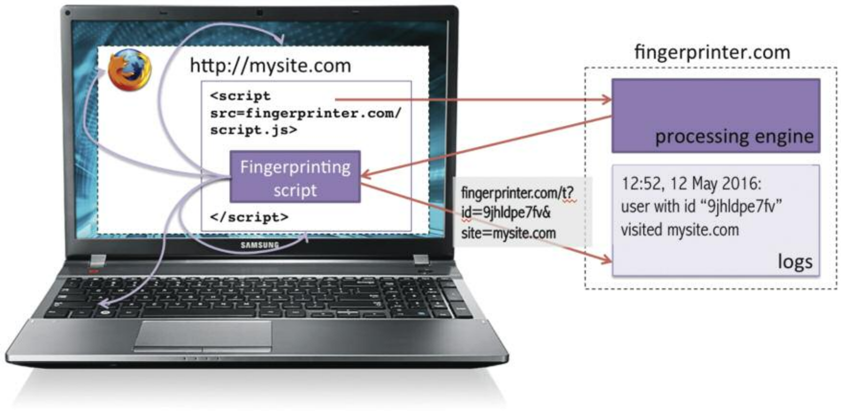


Figure 1: Device fingerprinting: a fingerprinting script collects data about Web browser and operating system properties, such as Web browser version, list of installed plugins, screen resolution, time zone etc., encodes it into a string and sends it back to fingerprinter.com.

is unlikely to be tracked. If the probability is high, this is a tracking script trying to identify the user.

We have also developed a quantitative information flow monitor [1] computing how much the tracker learns when running a script in the user's browser. The monitor uses a combination of dynamic and static analysis and over-approximates on-the-fly the amount of information that is learnt by running the script. If the amount of information is below a threshold, it is safe to send the output to the server. Otherwise, counter-measures need to be taken, such as shutting down the connection or providing forged but credible output. The theoretical foundations of such browser randomisation were developed in [2].

Next, we recently proposed a new version of a quantitative information flow monitor that is more precise in computing the knowledge of the tracker [3]. This new version expresses the monitoring of attacker knowledge in a general framework of semantics-based program analysis, and shows how a knowledge monitor can be combined with existing monitoring techniques for information flow control, such as the 'no-sensitive-upgrade' principle.

Link:
[L1] https://panopticlick.eff.org/

References:

[1] F. Besson, N. Bielova, T. Jensen: "Hybrid Information Flow Monitoring Against Web Tracking", IEEE CSF 2013.

[2] F. Besson, N. Bielova, T. Jensen: "Browser Randomisation against Fingerprinting: A Quantitative Information Flow Approach", NordSec 2014.

[3] F. Besson, N. Bielova, T. Jensen: "Hybrid Monitoring of Attacker Knowledge", IEEE CSF 2016.

Please contact:

Nataliia Bielova, Inria, France
+33 4 92 38 77 87
nataliia.bielova@inria.fr

CHERI: A Hardware-Software System to Support the Principle of Least Privilege

by Robert N. M. Watson, Simon W. Moore (University of Cambridge) and Peter G. Neumann (SRI International)

The CHERI hardware-software system has the potential to provide unprecedented security, reliability, assurance, ease of programmability, and compatibility.

Our University of Cambridge and SRI International team project is engaged in a multi-year hardware and software codesign project to produce the CHERI (Capability Hardware Enhanced RISC Instructions) system that provides fine-grained bounds checking as well as compartmentalisation managed by software and enforced in hardware. At its core is an old (historically) but new (in its present form) hardware data type: a tagged 128-bit fat-pointer capability that embodies an address, bounds, and permissions. The CHERI instruction set architecture (ISA) guarantees monotonically decreasing access rights (i.e., there can be no privilege escalation). The CHERI hardware tracks pointer integrity and enforces bounds checking. The CHERI ISA is defined in a formally based specification language, and several approaches to its formal analysis are underway. Three of our most recent papers are included in the references [1,2,3].

Software can utilize our capability hardware mechanism at a diverse range of levels. Our C compiler automatically assigns bounds to all pointers, mitigating well understood but frequently exploited buffer overflow attacks. Attempts to corrupt pointers in memory result in a clean failure rather than data or control-flow vulnerabilities. By combining code and data capabilities, compartments (e.g., sandboxes) can be constructed. Compartmentalisation can be used to prevent known exploits. By applying the principle of least privilege through fine-grained compartmentalisation, it is also possible to mitigate unknown future classes of exploits.

We have made the pragmatic choice to keep page-based virtual memory. Virtual memory is helpful in memory allocation and provides OS managed protection. Capabilities are managed by the software author and compiler. The hybridisation of the two approaches provides much flexibility and allows the two benefits of the two approaches to be exploited in a complementary manner. Where virtual memory is grounded in user and process separation, capabilities provide fine-grained in-address-space protection. For

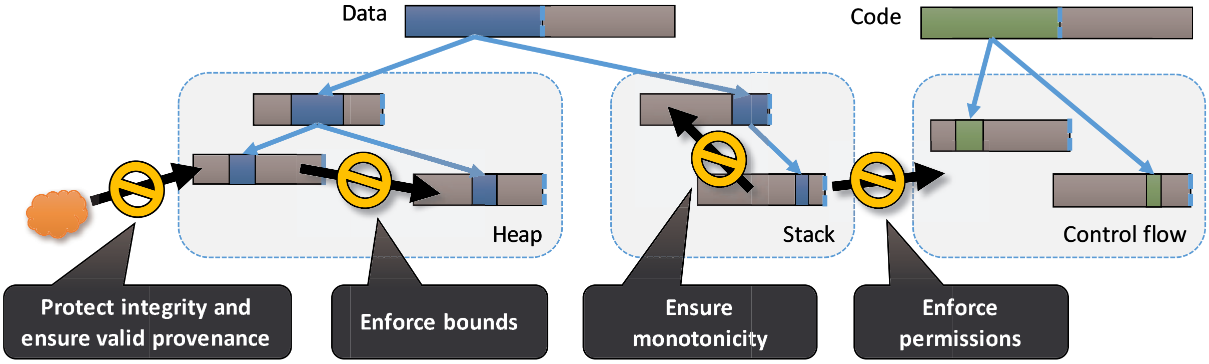


Figure 1: CHERI is a hybrid capability-system architecture supporting both conventional, pure-MMU operating-system designs (such as UNIX and Windows), pure capability-system designs, and hybrid operating-system designs that allow incremental deployment of CHERI's memory-protection properties within current large C-language TCBs such as operating-system kernels, key libraries, system services, and security-sensitive applications, such as web browsers.

example, a modern web browser will typically use process separation for each tab, separating your banking application from your social media. Such process separation scales poorly, limiting its use. In contrast, a capability system has orders of magnitude better performance and scales elegantly. Thus, in a browser it is possible to sandbox not only each tab but each image rendered, etc.

Our open-source project is supported by the U.S. Department of Defense Advanced Research Projects Agency (DARPA) and some other much smaller sources. It began in 2010, and will continue into early 2018, working towards transferring the hardware-software technology into practical systems. We are exploring significant potential for mainstream use.

References:

[1] J. Woodruff et al.: "The CHERI capability model: Revisiting RISC in an age of risk", ISCA 2014, Minneapolis, MN, USA, June 2014.
[2] D. Chisnall et al.: "Beyond the PDP-11: Architectural support for a memory-safe C abstract machine", ASPLOS 2015, Istanbul, Turkey, March 2015.
[3] R. N. M. Watson et al.: "CHERI: A hybrid capability-system architecture for scalable software compartmentalization, IEEE SSP, San Jose, CA, USA, May 2015.

These papers as well as further reports and publications can be found on the project website: http://www.cl.cam.ac.uk/research/security/ctsrd/

Please contact:

Peter G. Neumann
SRI International, UK
neumann@csl.sri.com

Robert N. M, Watson
University of Cambridge, UK
robert.watson@cl.cam.ac.uk

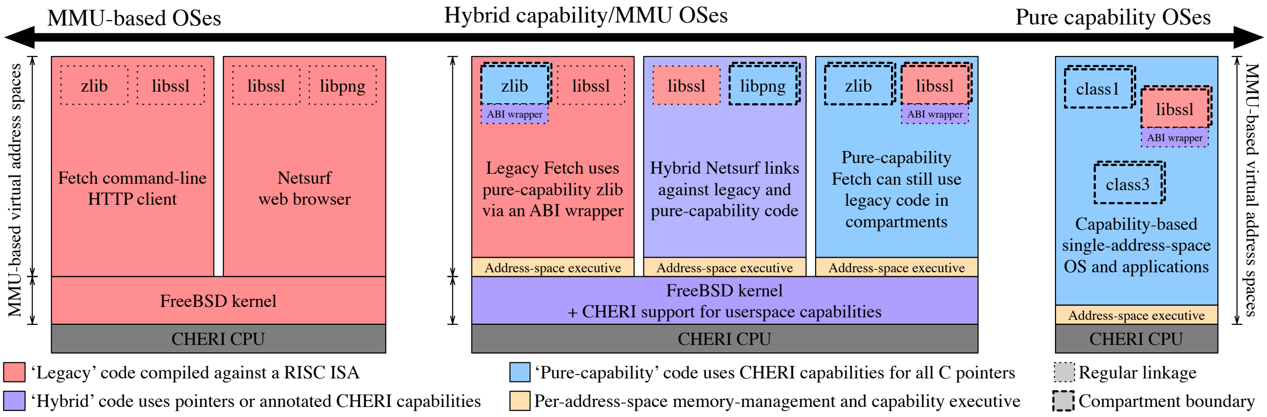

MMU-based OSes
Hybrid capability/MMU OSes
Pure capability OSes
MMU-based virtual address spaces
zlib
libssl
Fetch command-line HTTP client
libssl
libpng
Netsurf web browser
FreeBSD kernel
CHERI CPU
zlib
ABI wrapper
libssl
Legacy Fetch uses pure-capability zlib via an ABI wrapper
Address-space executive
libssl
libpng
Hybrid Netsurf links against legacy and pure-capability code
Address-space executive
zlib
libssl
ABI wrapper
Pure-capability Fetch can still use legacy code in compartments
Address-space executive
FreeBSD kernel + CHERI support for userspace capabilities
CHERI CPU
class1
libssl
ABI wrapper
class3
Capability-based single-address-space OS and applications
Address-space executive
CHERI CPU
MMU-based virtual address spaces
🟥 'Legacy' code compiled against a RISC ISA
🟪 'Hybrid' code uses pointers or annotated CHERI capabilities
🟦 'Pure-capability' code uses CHERI capabilities for all C pointers
🟧 Per-address-space memory-management and capability executive
⬚ Regular linkage
⬚ Compartment boundary

Figure 2: CHERI allows the operating system and compiler to enforce a variety of spatial memory-protection properties on pointers: strong integrity, valid provenance, bounds that enforce access to only the allocation, permissions that prevent inappropriate use, and monotonicity, which ensures that as privileges are removed from capabilities, they cannot be regained. These properties can be used to provide low-level memory safety for C — but also to construct higher-level security models such as software compartmentalisation.

Privacy-Preserving Indoor Localisation and Navigation

by Andreas Konstantinidis, Georgios Chatzimilioudis and Demetrios Zeinalipour-Yazti (University of Cyprus)

Internet-based Indoor Navigation (IIN) services have recently received considerable attention, mainly because GPS technology is unavailable in indoor spaces and consumes considerable energy. On the other hand, predominant Smartphone OS localisation subsystems currently rely on server-side localisation processes, allowing the service provider to know the location of a user at all times. We have devised an innovative algorithm for protecting users from location tracking by the localisation service, without hindering the provision of fine-grained location updates on a continuous basis. Our proposed Temporal Vector Map (TVM) algorithm allows a user to accurately localise by exploiting a k-Anonymity Bloom (kAB) filter and a bestNeighbors generator of camouflaged localisation requests, both of which are shown to be resilient to a variety of privacy attacks.

People spend 80-90% of their time in indoor environments, including shopping malls, libraries, airports and university campuses. The omni-present availability of sensor-rich mobiles has boosted interest in a variety of indoor location-based services, such as in-building navigation, inventory management, marketing, and elderly support through ambient and assisted living. To enable such indoor applications in an energy-efficient manner and without expensive additional hardware, modern smartphones rely on cloud-based Internet-based Indoor Navigation (IIN), which provide the accurate location (position) of a user upon request [1]. There are numerous IIN, including Skyhook, Google, Indoo.rs, Wifarer, Navizon, IndoorAtlas, ByteLight and our open-source in-house Anyplace (http://anyplace.cs.ucy.ac.cy/) service. These systems rely on geolocation databases (DB) containing wireless, magnetic and light signals, upon which users can localise.

At the University of Cyprus, we appreciate the benefit of indoor location based services (LBS) and our goal is to facilitate their wide acceptance [2]. At the same time, we feel that location tracking by IIN poses a serious imminent privacy threat, which will have an even greater impact than other existing forms of location tracking (i.e., outdoor GPS tracking or browser-based location tracking). This holds as IIN can track users at very fine granularity over an extended period of time.

We are developing hybrid techniques that on the one hand exploit the IIN utility, but on the other hand also offer controllable location privacy to the user. Particularly, we tackle the technical challenge of providing continuous localization to a mobile user u that can measure the signal intensity of its surrounding Access Points, with minimum energy consumption on *u*, such that a static cloud-based server s cannot identify *u*'s location with a probability higher than a user-defined preference p_u. We devise the Temporal Vector Map (TVM) algorithm [3], where a user *u* camouflages its location from *s*, by requesting a subset of *k* entries from *s*, where *k* is a user-defined constant. To understand the operation of TVM at a high level, consider Figure 1. An arbitrary user *u* moves inside building A, using the TVM smartphone application shown in Figure 2. While *u* requests reference locations from *s* pertinent to building A, it also requests reference locations related to arbitrary other buildings B and C. Particularly, *u* uses a hashing scheme that makes sure that for

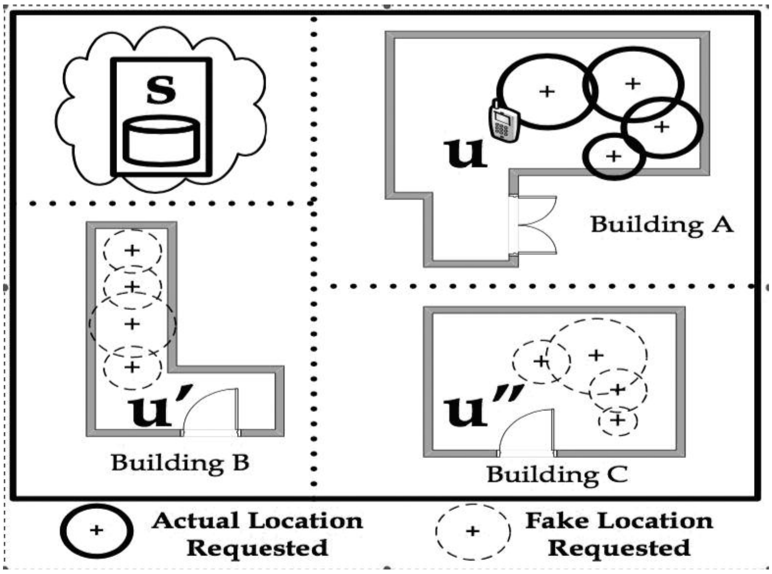
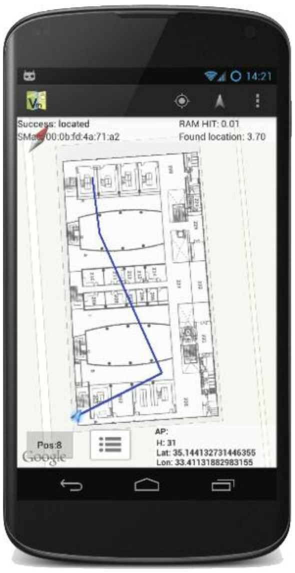


Figure 1: Indoor localisation of user u using the cloud-based IIN s. During the localisation, u requests k−1 camouflaged locations using the TVM algorithm, such that s can know the location of u only with probability 1/k.



Success: located
SMac 00:0b:fd:4a:71:a2
RAM HIT: 0.01
Found location: 3.70
AP:
H: 31
Lat: 35.144132731446355
Lon: 33.41131882983155

Figure 2: Our TVM prototype implemented in Android OS.

a given user-preference $k = 3$, s will not be able to distinguish u's request from requests made by $k-1$ arbitrary other users u' and u''. Under reasonable assumptions about the scope of IIN, we show that s can know u's location only within p_u, even while u is moving. Particularly, the TVM algorithm operates in two phases as outlined below.

In Phase 1 of TVM, u computes a k-Anonymity Bloom (kAB) filter structure, which provides location privacy for snapshot localization tasks. When u needs continuous localisation (e.g., as u moves), the kAB of Phase 1 itself is not adequate to preserve the privacy of u, since by issuing k independent requests, s can realise by exclusion that there are $k - 1$ invalid requests (as one of the requests will always relate to the real building A). This allows s to deterministically derive u's real location.

To circumvent the above problem, in Phase 2 of TVM, u uses the bestNeighbors algorithm to issue a set of camouflaged localisation requests that follow a similar natural movement pattern to that of u (i.e., dotted circles in Figure 1). This provides the illusion to s that there are k other possible users moving in space, thus camouflaging u among k other users. Since our TVM algorithm transfers only a partial state of the database from s to u, it requires less network traffic and smartphone-side energy than current privacy-aware approaches that transfer the complete database to u prior the localisation task. TVM is resilient to the (i) linking attack: the only uniquely identifying attribute is the fingerprint of a user's location. In fact, this is also the only attribute sent by the user to the server, therefore there are no other attributes that could link to the user's fingerprint value; and (ii) the homogeneity attack: there is an inherent diversity in the resulting k-anonymous set of TVM, since it uses hashing to generate a set of unique access point MAC values that has a uniform distribution over all values, and therefore, no information can leak due to lack of diversity in the sensitive attributes.

Links:
http://tvm.cs.ucy.ac.cy/
http://dmsl.cs.ucy.ac.cy/

References:

[1] Zeinalipour-Yazti, et. al.: "Internet-based Indoor Navigation Services", IEEE Internet Computing, 2016.
[2] G. Chatzimiloudis, et. al.: "Crowdsourcing with Smartphones", IEEE Internet Computing, Volume 16, 2012.
[3] A. Konstantinidis et. al.: "Privacy-Preserving Indoor Localization on Smartphones", IEEE TKDE, Volume 27, Pages: 3042-3055, 2015.

Please contact:

Demetrios Zeinalipour-Yazti
University of Cyprus
+357 22 892755
dzeina@cs.ucy.ac.cy

Social Fingerprinting – or the Truth About You

by Stefano Cresci, Marinella Petrocchi, Maurizio Tesconi (IIT-CNR), Roberto Di Pietro (Nokia Bell Labs), and Angelo Spognardi, (DTU)

Inspired by biological DNA, we model the behaviour of online users as "Digital DNA" sequences, introducing a strikingly novel, simple, and effective approach to discriminate between genuine and spambot online accounts.

Modelling the behaviour of online users, as well as analysing their properties, is of primary importance for a broad variety of applications – for example, to mine substantial information about events of public interest. Secondly, online behavioural analysis can be applied to make predictions: linking behaviours to some kind of ground truth in the past leads to predictions of what will likely happen in the future when similar behaviours take place.

Here, we consider online behavioural analysis as a means to detect fictitious and automated accounts, which distribute unsolicited spam, advertise events and products of doubtful legality, sponsor public characters and, ultimately, lead to a bias in public opinion and harm social relationships. Spambot detection is thus a must for the protection of cyberspace, in terms of both threats to users' sensitive information and trolls that may want to cheat and damage them. Unfortunately, new waves of malicious accounts present advanced features, making their detection with existing systems extremely challenging [1].

Inspired by biological DNA, we propose to model online user behaviour with strings of characters representing the sequence of a user's online actions [2]. Each kind of action (e.g., posting new content, following or replying to a user) can be encoded with a different character, in a similar manner to the bases of DNA sequences. According to this paradigm, online user actions represent the bases of their 'digital DNA'.

Digital DNA is a flexible way of modelling the different kinds of user behaviour that are observed on the internet. Its flexibility lies in the ability to choose which actions will form the sequence. For example, digital DNA sequences on Facebook could include a different base for each user-to-user interaction type: comments, likes, shares and mentions.

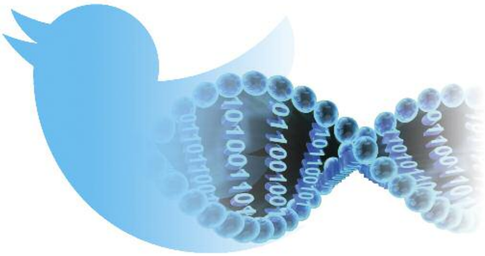
Like its biological namesake, digital DNA is a compact representation of information. For example, the timeline of a Twitter user could be encoded as a single string of 3,200 characters (one character per tweet).

In contrast with the supervised spambot detection approaches largely used in recent years, we have devised an unsupervised way to detect spambots by comparing their behaviour with the aim of finding similarities between automated accounts. We model the behaviour of spambots via their digital DNA and we compare it to that of genuine accounts.

We exploit digital DNA to study the behaviour of groups of users following the intuition that, because of their automated nature, spambots are likely to share more similarities in their digital DNA than will a group of heterogeneous genuine users.

This process is called digital DNA fingerprinting and encompasses four main steps: (i) acquisition of behavioural data; (ii) extraction of DNA sequences; (iii) comparison of DNA sequences; (iv) evaluation. First, we create datasets of verified spambots and genuine Twitter accounts. Then, we extract the digital DNA of the accounts; that is, we associate each account to a string that encodes its behavioural information.

Successively, we study similarities among the DNA sequences of our accounts. We consider similarity as a proxy for automation and, thus, an exceptionally high level of similarity among a large group of accounts serves as a red flag for anomalous behaviours. In particular, we quantify similarity by looking at the Longest Common Substring (LCS) among digital DNA sequences. We show that the similarity, as measured by the LCS, between the DNA sequences of spambots is much higher than that of genuine accounts, and we leverage this distinctive feature to perform our spambot detection. Finally, we compare our spambot detection results with those of other state-of-the-art approaches.



Modeling Twitter accounts via digital DNA. Illustration: Stefano Cresci.

Results show that our proposed technique outperforms best-of-breed algorithms that are commonly employed for spambot detection [2]. In addition, most of those state-of-the-art approaches require a large number of data-demanding features, as shown in [3]. Instead, our digital DNA fingerprinting technique on Twitter only exploits timeline data to perform spambot detection, thus being both effective and efficient. By relying on digital DNA, analysts can leverage a powerful set of tools that have been developed over decades for the analysis of biological DNA to validate their working hypotheses on online user behaviour.

Link: http://mib.projects.iit.cnr.it

References:

[1] E. Ferrara et al.: "The Rise of Social Bots", Communications of the ACM, 59(7), 2016.
[2] S. Cresci, et al.: "DNA-inspired online behavioral modeling and its application to spambot detection", IEEE Intelligent Systems, PrePrints, doi:10.1109/MIS.2016.29, 2016.
[3] S. Cresci et al.: "Fame for Sale: Efficient detection of fake Twitter followers", Decision Support Systems 80(4), pp. 56–71, 2015.

Please contact:

Marinella Petrocchi, IIT-CNR, Italy
+390503153432
marinella.petrocchi@iit.cnr.it

Flexible Decentralised Access Control using Invitation-Response Dialogue

by Arthur Melissen (Coblue Cybersecurity)

Distributed role-based access control (RBAC) has become a standard for decentralised systems to manage authorisation across networks. While this model is effective at providing authorization, it fails in providing the flexibility and authorisation accountability that organisations require today. We present an extension to standard distributed RBAC mechanisms by adding an invitation and response dialogue in the assignment of roles to entities for distributed resources, such as collections of shared files. This approach offers more flexibility for delegating roles across administrative domains and increases transparency and confidence in the authorisation structure of distributed resources.

Traditionally, decentralised systems have used distributed access control and simple public key infrastructure (SPKI) [1] mechanisms to manage which entities are provided access to a given resource. Authorisation for a resource is described using an access control list (ACL). Each entry in the ACL describes a set of entities and their assigned roles and authorisation characteristics, such as read and write permissions.

An entity that has a sufficiently high authorisation is able to modify the ACL itself and control the authorisations of other entities. Granting authorisations to other entities in the system is called delegation. We shall refer to entities that have the power to delegate authorisation to other entities as administrators of a resource.

Typically, existing SPKI systems delegate authorisation by letting administrators create a new entry in the ACL and signing it with an administrator's cryptographic key. The authorisation describes the role granted and a set of entities by their public key. The updated ACL is then distributed across all relevant entities in the network and the entities are made aware of the new authorisation.

While this approach works well, it lacks the flexibility and accountability that is often desired in a modern distributed networking context. We found several areas for improvement:

First, it is possible that the entity desires no authorisation at all for a given resource. In a distributed file system, an entity from one organisation could desire to never have any authorisation for sharing files from another organisation.

Second, in a decentralised environment it is not uncommon for entities from different administrative domains to share authorisation on a resource. For example, several organisations might be working together on a single project. Each organisation has their own structure and wants to control allocation of authorisation to a specific entity under their control. Examples might be a large company that wants to select a consultant for a particular authorisation on a project or a network administrator that wants to select a server based on expected load from the company's server collection. In traditional role-based access control systems, the administrator of one organisation would need to know the entity's public key of another organisation before granting authorisation. This requires prior dialogue and collaboration between domains and does not scale well. Authorisation and allocation decisions like these should be separated in two operations local to each organisation's domain, and without needing to select an already existing entity.

Third, entities might only be sparsely connected and have no way to directly verify the willing co-operation of other entities in the same ACL. This can lead to misconceptions about the participation of other entities.

To avoid these scenarios we have added an extra layer to traditional role-based access control in the form of an invitation-response dialogue between entities before authorisation is confirmed. In our model, instead of a list of authorisations to entities directly, the ACL of a resource consists of a list of role invitations.

Each invitation in an ACL is identified by its own public key. An invitation describes the life cycle of an association between an entity and a role for the resource the ACL is linked to. An example could be that an entity is invited to become an administrator for a certain filesystem. Invitations always start as invited, and can be accepted, rejected, or terminated. The invitation can start anonymous or be associated to a specific entity. An entity needs the private key of the invitation to claim it. This key can be distributed through the network and encrypted using the entity public key or through a private channel. Claiming an invitation is done by signing the invitation using the invitation's private key. If the invitation is accepted, the invitation is also signed using the entity's private key and distributed across the network. The entity is then able to use the authorisation described in the invitation for as long as the invitation is active.

Terminating an invitation is performed by signing a special 'end signature' field in the invitation. This can be done by the entity which claimed the invitation (the entity leaves this role), or by an administrator (the entity is removed from the role). Because invitations are part of the ACL, they can only be created by an administrator.

Results

Using an additional invitation layer in the ACL yields several advantages: Every entity possesses plausible deniability for abusing any authorisation that it did not accept itself. Authorisation delegation (a task for a delegator) can be separated from entity selection for that authorisation (a task for a delegatee). Additionally, entities in an ACL can verify the acceptance of authorisation of their peers without needing to contact each other directly. Together, these measures increase flexibility, transparency and accountability in setting up shared resources across administrative domains.

This work was carried out for the Secure Information Grid project [L1] under an RVO SBIR grant.

Link:

[L1] http://www.rvo.nl/sites/default/files/SBIR12C020%20Secure%20Information%20Grid.pdf

Reference:

[1] C. M. Ellison, B. Frantz, B. Lampson, et al.: "SPKI Certificate Theory", IETF Request for Comments 2693, 1998. http://www.ietf.org/rfc/rfc2693.txt

Please contact:

Arthur Melissen, Michel Eppink
Coblue Cybersecurity, The Netherlands
arthur@coblue.eu, michel@coblue.eu

Data Sharing Agreements: How to Glue Definition, Analysis and Mapping Together

by Carmela Gambardella, (Hewlett Packard Enterprise Italy), Ilaria Matteucci, and Marinella Petrocchi (IIT-CNR)

An electronic data sharing agreement (DSA) is a human-readable, yet machine-processable contract, regulating how organisations and/or individuals share data. Its smooth definition and fluid lifecycle management are key aspects for enabling data protection in various contexts, from e-government to the provision of business and healthcare services, for example.

Data sharing is becoming ever easier with the support of highly-connected ICT systems. Individuals, businesses and governments are increasingly choosing to use cloud infrastructure to store data, owing to recent reductions in cost and the functionalities provided by the cloud, such as easy sharing of data. Data sharing, however, poses several problems, including privacy and data misuse issues, as well as uncontrolled propagation of data. Thus, a secure and private way for data exchange, storage, and management is essential. The aim of the Coco Cloud project [L1] is to ful-

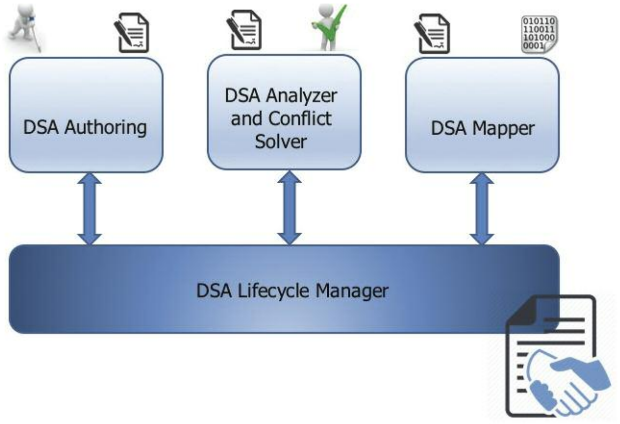


Figure 1: The Coco Cloud Data Sharing Agreement (DSA) system designed to manage different phases of DSA design, development, and use: DSA Authoring Tool, DSA Analysis and Conflict Solver Tools, and a DSA Mapper Tool, glued together by the DSA Lifecycle Manager.

fill these security and privacy issues, by providing a framework that permits the exchange of data by enforcing privacy policies to access and use data in a controlled way. This is supported by the concept of data sharing agreement (DSA). DSAs specify policies that are applied for accessing the data to which they are linked.

Here, we introduce the Coco Cloud DSA system designed to manage different phases of DSA design, development, and use: DSA Authoring Tool, DSA Analysis and Conflict Solver Tools, and a DSA Mapper Tool, glued together by the DSA Lifecycle Manager [1]:

- DSA Authoring Tool is in charge of creating and managing DSAs. The rules included in the DSA are created using a language called Controlled Natural Language for DSA [2], or, more concisely, CNL, which is based on specific dictionaries (ontologies). The tool is available as a web application that provides a user-friendly experience.
- DSA Analyser and Conflict Solver analyse the rules in a DSA and solve potential conflicts. A conflict exists when two policies simultaneously allow and deny an access request under the same contextual conditions. If a conflict is revealed, the conflict solver prioritises the rules to be enforced. The Analyser is available as a web service application and it exposes its functionalities through Application Program Interfaces (APIs).
- DSA Mapper translates the DSA policies from CNL into an enforceable XACML-based language. The mapping process takes as input the analysed DSA rules, translates them in the machine-processable language, and combines all rules in line with the conflict solver strategy. The outcome of this tool is an enforceable policy. The policy will be evaluated at each request to access and/or use the target data.
- DSA Lifecycle Manager orchestrates all the DSA System components. The DSA Lifecycle Manager provides the user with particular functionalities of the DSA System, according to the specific user's role (described below). Thus, users do not interact directly with the DSA System components tools, but via the DSA Lifecycle Manager.

The DSA System allows different types of user to edit DSAs. Users can log into the DSA system under three different roles, each with specific features, goals, and functionalities [3]:

- Law expert (for example, a lawyer) is familiar with legal and contractual perspective content of the agreement. Such a user is in charge of creating and managing the initial version of a DSA through the DSA Authoring Tool, instantiating legal rules.
- Policy expert is responsible for defining business policies and DSA metadata, for example a company policy expert that has to set up company specific agreements.
- End user can either extend, if requested, the DSA of the policy expert with her user-specific input or simply review and accept a DSA created by a policy expert for use with her data. An example of such a user is a patient in a hospital.

The Coco Cloud solutions to manage Data Sharing Agreements are assessed through the three project use cases, featuring the need for secure and private data sharing within the public administration, health care, and mobile scenarios.

We acknowledge contributions to the design and development of the DSA system by Gianpiero Costantino, IIT CNR, Pisa, Italy, Mirko Manea, Hewlett Packard Enterprise Italy, Anil Ozdeniz, ATOS, Turkey, and Jose Francisco Ruiz, ATOS, Spain.

Link:
[L1] http://www.coco-cloud.eu

References:

[1] J. Ruiz, et al: "The lifecycle of Data Sharing Agreements: how it works out", Springer APF 2016, in press.
[2] I. Matteucci, M. Petrocchi, M. L. Sbodio: "CNL4DSA: a controlled natural language for Data Sharing Agreements", ACM SAC 2010: 616-620.
[3] C. Caimi et al.: "Legal and Technical Perspectives in Data Sharing Agreements Definition", Springer APF 2015: 178-192.

Please contact:

Marinella Petrocchi
+390503153432
marinella.petrocchi@iit.cnr.it

Data Usage Control: Introducing a New Framework for Cloud and Mobile Environments

by Paolo Mori, Andrea Saracino (IIT-CNR) and Francesco Di Cerbo (SAP Labs France)

In the frame of the European project CoCoCloud (Confidential and Compliant Clouds) we propose a distributed and general framework to enforce usage control policies on data shared in the cloud environment.

Cloud services are becoming increasingly pervasive in almost every field of information technology. The reasons for this are clear: cloud computing allows specific data, such as documents, to be created and seamlessly accessed from anywhere on the globe, and also facilitates document sharing. Furthermore, mobile devices such as smartphones and tablets allow access to documents stored in the cloud anywhere, anytime. After a document has been published in the cloud, the data producer is handing over partial control of the document to the cloud provider and to the other users with whom the document is shared. It is important, therefore, that the sharing framework properly guarantees data security and privacy. Enforcing security and privacy on documents often requires the continuous monitoring of conditions concerning the subjects who access the document, the document itself and additional information related to the context in which access is performed.

To handle these issues, within the EU FP7 project ‘Confidential and Compliant Clouds’ [L1] we designed and implemented a distributed and general framework to enforce usage control policies on data shared in the cloud environment. The proposed framework enables monitoring and enforcement of security policies related both to the right to access specific documents (access control) and to use them over time (usage control). A peculiarity of usage control is that ongoing access to a document is interrupted as soon as a modification in the attributes of the subject, of the document, or of the environment causes a policy violation.

In the proposed framework, each document published in the cloud embeds one or more usage control policies (sticky policies). The policy specifies the conditions to access the document, e.g., the subject(s) authorised to access and their required features (i.e., attributes such as role, reputation, location, etc.), features of the document (size, creation date, etc.), and external conditions that build the context of environment (network connection, date and time, etc.) [2]. Furthermore, the policy allows specific actions on the controlled system to be forced. These are named obligations and are used, for instance, to send notifications to the document producer [1].

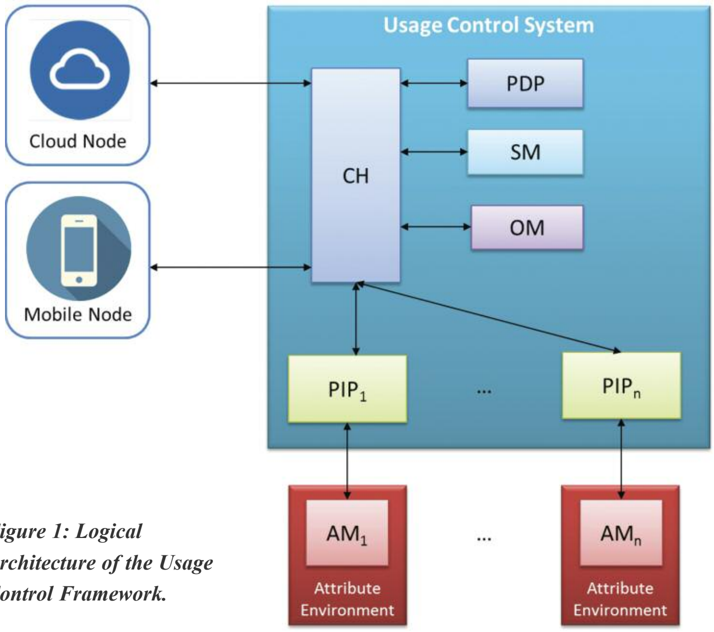


Figure 1: Logical Architecture of the Usage Control Framework.

Figure 1 shows the logical architecture of the proposed framework, which relies on the well established model defined by Sandhu [3]. The policy decision point (PDP) evaluates access and usage requests, matching them against the security policies, returning either permit or deny as an answer. The policy information points (PIPs) collect information concerning subject, object and environment, retrieving them from external components named attribute managers (AM). The cloud and mobile nodes enforce the security policies by granting or blocking access to documents, according to the decisions of the PDP. The obligation manager (OM) is responsible for handling the obligations contained in policies, forcing the cloud and mobile nodes to perform specific actions, such as sending a notification message when a document is accessed. Finally, the context handler (CH) manages the interactions among the previous components.

As discussed, the framework is designed to operate both in cloud environments and mobile devices. In the cloud use case, the enforcement is performed by managing access to data in the cloud through cloud services. The cloud service allows only those operations permitted by the policy, and is also able to revoke an ongoing access, closing the service when a policy condition is no longer matched. On mobile devices in contrast, usage control is enforced directly on the device. In particular, when an access request is performed, the document to be accessed is downloaded directly on the device, in a protected memory space not accessible to the user, nor to other apps running on the mobile device. The mobile node is embodied by an application that allows controlled access to the stored documents, denying the access when the PDP returns a deny decision. Security of files stored on the device is ensured by means of asymmetric key encryption and trusted computing base functionalities, which will ensure both data confidentiality and integrity.

The proposed framework is general and could be applied in a range of environments and applications, such as e-health or business company premises. In e-health, for example, the framework could be used to control the access rights of a practitioner to the electronic data of a patient. One way in which it could be applied in this environment is to restrict access to patient data, from a mobile device, to practitioners that are directly responsible for the patient and / or only when the practitioner is on the hospital premises. Even if the practitioner has the clinical record of the patient opened, once he or she leaves the hospital, the position acquired from the mobile device changes, and access is revoked: the application will automatically close the document and forbid further access attempts until the conditions match the policy again. It is also possible to enforce a specific retention period for patient data, guaranteeing that the data will be deleted in order to comply with data privacy regulations.

Link: [L1] http://www.coco-cloud.eu/

References:

[1] F. Di Cerbo, et al.: “Sticky policies for mobile devices”, in Proc. of the 18th ACM Symposium on Access Control Models and Technologies, SACMAT ‘13, 257-260, 2013.

[2] A. Lazouski et al.: “Stateful usage control for android mobile devices”, in Proc. of the Security and Trust Management – 10th International Workshop, STM 2014, 97–112, 2014.

[3] J. Park, R. Sandhu: “The UCONABC usage control model”, ACM Trans. Inf. Syst. Secur. 7(1), 128-174, 2004.

Please contact:

Paolo Mori and Andrea Saracino
IIT-CNR, Italy
paolo.mori@iit.cnr.it,
andrea.saracino@iit.cnr.it

Francesco Di Cerbo
SAP Labs France,
francesco.di.cerbo@sap.com

Robust and Scalable DTLS Session Establishment

by Marco Tiloca, Christian Gehrmann and Ludwig Seitz (SICS)

The Datagram Transport Layer Security (DTLS) protocol is highly vulnerable to a form of denial-of-service attack (DoS), aimed at establishing a high number of invalid, half-open, secure sessions. Moreover, even when the efficient pre-shared key provisioning mode is considered, the key storage on the server side scales poorly with the number of clients. SICS Swedish ICT has designed a security architecture that efficiently addresses both issues without breaking the current standard.

Secure communication is a main requirement in increasing numbers of applications, ranging from plant monitoring to home automation; from certified e-mail to e-commerce. Given the increasing number of applications relying on datagram protocols, the IETF has standardised the DTLS protocol [1], which is designed to be as similar as possible to the widely adopted TLS protocol.

Two DTLS peers, namely client and server, establish a secure session by performing a handshake. Typically, the client takes the initiative, by sending a ClientHello message to the server. During the handshake, the two peers establish and exchange the security material used later on. To this end, they may adopt an efficient key provisioning mode based on symmetric pre-shared keys (PSKs), so avoiding the computational complexity of public key cryptography and the management of a public key infrastructure. This has made PSK increasingly popular, as it is particularly suitable for applications like smart metering and building automation, where servers might be resource-constrained devices operating over low-bandwidth networks.

Nevertheless, the DTLS handshake displays two relevant security and performance issues.

Firstly, the server is highly vulnerable to a specific denial-of-service (DoS) attack. Specifically, an adversary can repeatedly send ClientHello messages to the server, and force it to start performing a considerable number of handshakes. While a preliminary Cookie exchange with the client can complicate the attack performance, it does not fundamentally protect the server against a DoS mounted by a determined and resourceful adversary. Hence, the server can still be induced to establish a considerable amount of half-open DTLS sessions, to exhaust its network resources and make it less responsive, or even unavailable, to legitimate clients.

Secondly, if the PSK provisioning mode is adopted, the server may have to store and manage a considerable number of pre-shared keys, possibly one for every possible client. This scales poorly with the number of clients and considerably complicates key provisioning operations, especially in dynamic environments.

SICS Swedish ICT [L1] has designed an efficient security architecture based on a Trust Anchor entity in a trusted relation with multiple DTLS servers. The architecture addresses the two identified DTLS issues, by combining the two following improvements.

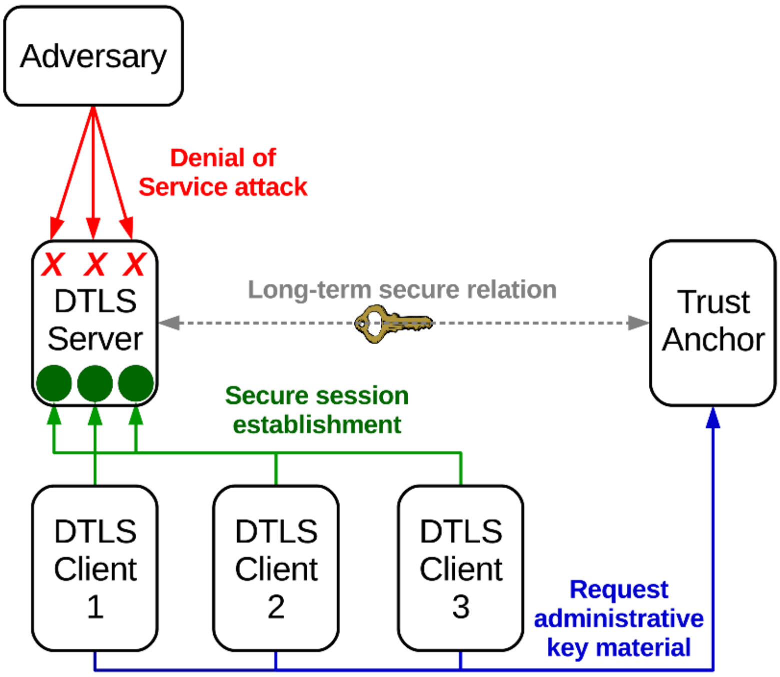


Figure 1: Security architecture for robust and scalable DTLS session establishment.

First, we have defined a preventive solution to the considered DoS attack. In particular, the server is able to identify invalid ClientHello messages and promptly abort the handshake execution at the first step, so practically neutralising the DoS attack and substantially limiting its impact. Besides, one message round trip between client and server can be avoided, as the cookie exchange is no longer necessary.

Second, we have defined an alternative PSK scheme that reduces the number of pre-shared keys stored by the server to one only, so preventing scalability and management issues and greatly reducing the load on the server. This is achieved by shifting the load of key management to the trust anchor and requiring clients to perform an additional message round trip.

Our approach displays a number of benefits. First, it relies on a standardised method to extend ClientHello messages, and does not require changes to the DTLS standard. Second, no additional message exchange between client and server is required, and even the cookie exchange is no longer necessary. Third, it does not significantly contribute to the computing overhead of client and server, as the handshake process maintains the same order of computational complexity. Finally, our improvements can also be easily readopted in the TLS protocol, without changing the actual standard.

We implemented our DTLS improvements in the library Scandium [L2] and performed an experimental performance evaluation. Results show that, when compared with the original DTLS protocol, our approach: i) improves a server's robustness against DoS; ii) reduces the time a server is exposed to a promptly neutralized DoS instance; and iii) improves service availability and scalability of key storage.

A comprehensive description of the architecture described above and the performance evaluation is available in [2].

Our approach is currently considered in the European project SEGRID [L3], which is devoted to improving cyber security in smart electricity grids. The project partners SICS Swedish ICT and the European Network for Cyber Security (ENCS) [L4] have been cooperating to integrate the presented DTLS improvements in a real substation automation system. This will contribute to make secure communication between RTU units based on DTLS and the IEC104 protocol more robust and scalable, hence more reliable and resilient. Final tests and performance evaluation will be performed in the project testbed SITE.

Links:
[L1] https://sics.se
[L2] https://github.com/mkovatsc/Scandium
[L3] http://www.segrid.eu
[L4] https://encs.eu

References:

[1] E. Rescorla and N. Modadugu: "RFC 6347, Datagram Transport Layer Security Version 1.2.", Internet Engineering Task Force, 2012.
[2] M. Tiloca, C. Gehrmann, L. Seitz: "On Improving Resistance to Denial of Service and Key Provisioning Scalability of the DTLS Handshake", International Journal of Information Security, Springer, 2016 (To appear)

Please contact:

Marco Tiloca
SICS Swedish ICT
marco@sics.se

Client-Server Framework for Securely Outsourcing Computations

by Thijs Veugen (TNO)

In the current age of information, with growing internet connectivity, people are looking for service providers to store their data, and compute with it. On the other hand, sensitive personal data is easily misused for unintended purposes. Wouldn't it be great to have a scalable framework, where multiple users can upload personal data, which allows the servers to offer services on these data without ever revealing any data to the servers? TNO and CWI in the Netherlands have developed such a framework.

At first sight it might appear to be a magic trick, but with modern cryptographic tools it is actually possible to compute with data without ever learning the data itself. In a joint research effort [1], TNO and CWI have developed such a framework. Centrum Wiskunde & Informatica (CWI), with their state-of-the-art expertise on cryptography, fine-tuned existing techniques to the client-server setting. This enabled the Dutch organisation for applied scientific research (TNO) to implement and test such a framework for a particular application – in this case a recommendation system.

Secure computations. Source: Beeldbank TNO.

In recommendation systems, service providers can recommend products to their customers based on personal data from many users. To avoid leakage of these personal data, service providers use secret sharing. This enables them to compute the recommendation, while remaining oblivious to the contents. Only the user requesting the output will be able to combine all shares of the recommendation and learn the result.

Although similar secure recommendations systems have been developed before, they were either less secure, or less efficient. This framework is the first one that uses fast cryptographic techniques within a 'malicious security model'. By precomputing a lot of input independent data, the two servers were able to compute a recommendation within 0.34 seconds, using data from 10,000 users. The framework can be extended to an arbitrary number of servers, and as long as at least one behaves in an honest way, no data is leaked. Since secret sharing requires no additional cryptographic keys, the number of framework users is easily scaled up.

This secure client-server framework, which enables any kind of computation to be outsourced to the servers, is just one example of the applications of secure multi-party computation. In this field, many parties jointly compute a function on their private inputs without revealing the inputs to another party. Depending on which party is inputting data, which party receives the output, and which parties are doing the computations, many different applications are possible [2]. Some examples include: genomic research by biobanks, network anomaly detection by network administrators and financial reporting within a consortium.

TNO and CWI [L1, 2, 3] intend to extend the current work by exploiting techniques from the field of secure multi-party computation [3] within various application domains. This will open up unforeseen opportunities and collaboration models for organisations.

Links:

[L1] https://www.tno.nl/en/collaboration/expertise/early-research-programme/early-research-program-making-sense-of-big-data/
[L2] http://www.commit-nl.nl/projects/trusted-healthcare-services
[L3] http://projects.cwi.nl/crypto/

References:

[1] T. Veugen, R. de Haan, R. Cramer, F. Muller: "A Framework for Secure Computations With Two Non-Colluding Servers and Multiple Clients, Applied to Recommendations" IEEE TIFS, March 2015.

[2] P. Laud, L. Kamm: "Applications of Secure Multiparty Computation", CISS, 2015.

[3] R. Cramer, I.B. Damgård, J.B. Nielsen: "Secure Multiparty Computation and Secret Sharing", July 2015.

Please contact:

Thijs Veugen
TNO, The Netherlands
thijs.veugen@tno.nl

A Root of Trust for the Personal Cloud

by Benjamin André (Cozy Cloud), Nicolas Anciaux, Philippe Pucheral and Paul Tran-Van (Inria)

We are witnessing an exponential accumulation of personal data on central servers: data automatically gathered by administrations, companies and web sites, but also data produced by individuals themselves and stored in the cloud for convenience (e.g., photos, agendas, raw data produced by smart appliances and quantified-self devices). Unfortunately, there are many examples of privacy violations arising from abusive use or attacks, and even the most secured servers are not spared.

The Personal Cloud paradigm has recently emerged as a way to allow individuals to manage under their control the collection, usage and sharing of data in different contexts and for different types and sensitivities of data, as requested by the World Economic Forum [1]. Initiatives like Blue Button and Green Button in the US, MiData in Great Britain and MesInfos in France give body to this paradigm by returning personal data retained by companies and administrations to individuals in a practical way. This user-centric vision illustrates the gravity shift of information management from organisations to individuals. However, at the same time as individuals recover sovereignty of their data, they also inherit the burden of organising this personal data space, and more importantly of protecting it against attacks and loss.

While much research work is tackling the organisation and semantic exploitation of the user's workspace, far less attention has been paid to security issues. Existing security solutions range from encrypting the personal data with an independent tool (e.g., TrueCrypt or BoxCryptor) before storing it on a cloud provider or relying on decentralised storage (such as OwnCloud, SandStorm, SeaFile, Unity or OpenPDS personal cloud platforms), letting the individual decide where to store his data. In both cases, data is usually encrypted with keys, which are in turn encrypted with the user's password. Hence, the password is de facto the root of security and the Achilles heel of these systems since all data are definitely lost if the user forgets his password or can be leaked if the password is compromised. This is a critical point considering that a personal cloud is expected to concentrate the complete digital estate of an individual. The sharing functionality among users is also very limited, implemented either by manually exchanging links to files or by compiling the access control within the encryption (e.g., by encrypting the file key with the recipient's public key) making access control static and cumbersome to manage.

We promote a different approach, called Secure Personal Cloud, where the root of security is made of secure hardware and the access control policies are easily extracted from the personal cloud itself, with minimal user interaction. Our solution is based on the tight integration of a Personal Cloud platform (Cozy [L1]) with a trusted component (PlugDB [L2]). Cozy is an open-source solution developed by Cozy Cloud. It is able to gather personal data from multiple sources and data providers, to organise it in a document database (CouchDB) and to synchronize it with multiple devices of the same user. PlugDB is a secure database engine embedded in a low-cost tamper-resistant hardware device (i.e., a combination of smartcard technology and Flash storage in a USB form factor token) [3]. It is able to store data/metadata associated to Cozy documents, query them, manage access control rules and encrypt/decrypt data [2]. PlugDB is a research prototype from INRIA. Combining these two components allows the architecture depicted in Figure 1 to be set up.

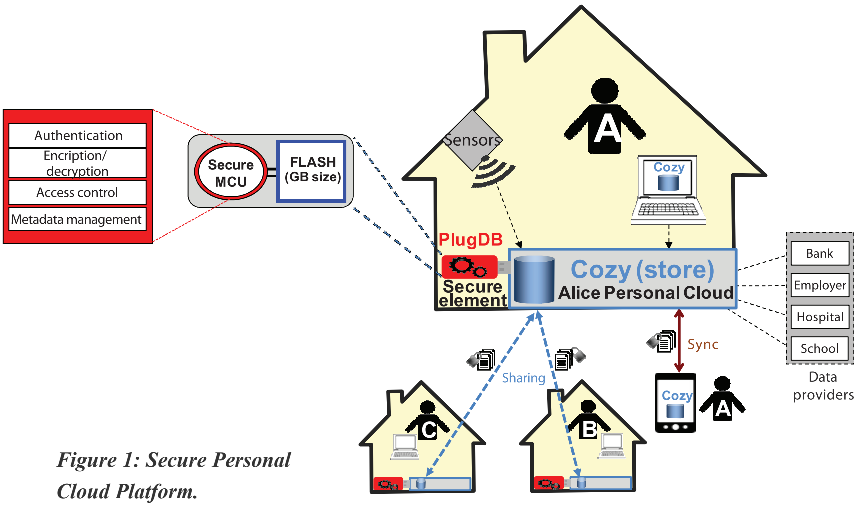


Figure 1: Secure Personal Cloud Platform.

This architecture works as follows. Heterogeneous data issued by external sources (e.g., banks, employers, hospitals, commercial web sites) and by personal appliances (e.g., quantified-self devices, smart meters, domestic sensors, cameras) are all transformed into documents. Document metadata is extracted and stored in PlugDB and documents themselves are encrypted by PlugDB before being integrated in the Cozy store. Encryption keys never leave the secure sphere of PlugDB.

Once encrypted, documents can be safely stored in the cloud for resiliency reasons or exchanged among users. Hence, PlugDB acts has a doorkeeper protecting the complete digital environment managed by Cozy. At the time an application/user asks for a Cozy document, the request is routed to PlugDB which evaluates the access control policy and decrypts the requested document if the authorisation check succeeds. Thanks to PlugDB tamper-resistance, sticky policies can be safely enforced when documents are shared among individuals. Encryption keys and access/usage control rules are transferred along with the shared document and are enforced at the recipient side, with no way for the recipient user to tamper with the processing on his own platform. The implementation of a proof-of-concept of this architecture is partly supported by the SECSi French PIA (Programme Investissement Avenir) project.

Important scientific, technological, societal and legal issues are raised by such Secure Personal Cloud architecture. Notably, our objective is to enable the execution of distributed queries linking the personal data of several individuals with the guarantee that neither the result of the query, nor the observation of all intermediate steps of the execution discloses any information about a particular individual [4]. In other words, Privacy-by-Design big data treatments can be implemented on personal data. Another important challenge is to ease the declaration and administration of access control policies by the individuals. Our hope is that the Secure Personal Cloud approach will provide a credible alternative to the systematic centralisation of personal data on servers and will pave the way for new privacy-by-design architectures.

Links:
[L1] https://cozy.io/fr/
[L2] https://project.inria.fr/plugdb/

References:

[1] S. Abiteboul, B. André, D. Kaplan: "Manage your digital life in your personal info management system", Communications of the ACM, 2015, 58 (5), pp.32-35.

[2] N. Anciaux, S. Lallali, I. Sandu Popa, P. Pucheral: "A Scalable Search Engine for Mass Storage Smart Objects", Proc. of the 41th International Conference on Very Large Data Bases (VLDB), Hawaï, PVLDB 8(9): pp 910-921, September 2015.

[3] N. Anciaux, et al.: "MILo-DB: A Personal, Secure and Portable Database Machine", Distributed and Parallel Database Journal (DAPD), 32(1), 2014.

[4] C. To, B. Nguyen, P. Pucheral. 'Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture', ACM Transaction on Database Systems (TODS), to appear (http://tods.acm.org/).

Please contact:

Benjamin André
Cozy Cloud, France
benjamin@cozycloud.cc

Philippe Pucheral
University of Versailles & Inria, France
Philippe.Pucheral@inria.fr

VirtuWind – Security in a Virtual and Programmable Industrial Network Prototype Deployed in an Operational Wind Park

by Ioannis Askoxylakis, Nikolaos Petroulakis, (FORTH), Vivek Kulkami and Florian Zeiger (Siemens)

The wind power industry is a good example of an industrial network with strict performance, security, and reliability requirements. The VirtuWind project aims to develop and demonstrate a software defined network (SDN) and network function virtualisation (NFV) ecosystem, based on an open, modular and secure framework.

Applications are becoming increasingly networked and distributed, especially in industrial domains, such as smart grid, factory automation, process automation, transportation and logistics. Many of these applications have very stringent requirements on the underlying communication network(s). This is currently addressed by using complex and proprietary network protocols and mechanisms, but this approach has major drawbacks: substantial engineering, operations and maintenance efforts; complex configuration of devices and services; and significant (planned) down times during system upgrades. Thus, there is a trend in industrial networks to move away from closed, implementation-specific solutions towards more open solutions. Open, standardised solutions come with their own problems, however: increased openness makes intra-domain operation and security more critical than ever before and different network providers may implement the same functionality differently, with interoperability and inter-domain operation becoming a huge concern.

VirtuWind will develop and demonstrate a software defined networking (SDN) and network function virtualization (NFV) ecosystem, based on an open, modular and secure framework [1]. The project showcases a representative use case of an industrial network by demonstrating a prototype of an industrial control network for wind park operations. It also addresses the challenges in intra-domain and inter-domain scenarios of real wind parks, and validates the economic viability of the demonstrated solution. The wind park control network has been chosen as a professional application in VirtuWind as wind energy has now established itself as a mainstay of sustainable energy generation. By envisioning lower capital expenditure and operational expenditure costs in control network infrastructure, VirtuWind will play an important role in assisting the wind energy sector to reduce costs. The VirtuWind solution also has the potential to offer multiple benefits to the communication networks of other industrial domains.

Introducing revolutionary concepts, such as SDN and NFV, to the communication networks of critical infrastructures, requires a careful investigation of the new security risks, since new threats – not encountered in legacy systems – will occur [2]. More specifically, SDN is currently only used in closed environments, such as data centres. However, the use of SDN in cross-domain setups and the absence of multi-operator collaborative incident detection mechanisms introduces new threats. The nature of software increasingly used in SDN and NFV environments comes with additional security threats, such as data forging, application programming interface (API), controller and management exploitation which need to be avoided by means of suitable mechanisms, e.g., strong authentication, access control, application isolation and sandboxing, flow integrity and conflict resolution as well as threat detection and encrypted interfaces.

One of the core objectives of VirtuWind is to assure security-by-design for the SDN and NFV ecosystem. To this end, VirtuWind aims to establish comprehensive threat and risk frameworks for industry-grade SDN networks. Suitable mechanisms will be developed for network monitoring and intrusion detection for SDN networks. More specifically, VirtuWind aims to address the following requirements:

Authentication, Authorization and Accounting (AAA)

The presence of mechanisms ensuring AAA functions, distributed horizontally and vertically on the SDN, if needed, are necessary for validating identities and requests, and for providing logging of the associated events. Authorisation (access control) and other control plane elements, along with the associated interfaces, will provide isolation and QoS-awareness to the overlaying applications. Mechanisms for ensuring accountability of controller actions affecting cyber-physical systems will be enabled. In addition, north bound interfaces (interfaces to the business applications) should allow applications to express their requirements in terms of network policies, e.g., flow isolation and QoS profiles. Based on the information exchanged through this interface, authentication and authorisation of stakeholders could be realised via access and role-based lists for different levels of function granularities.

Secure Interfaces

The SDN infrastructure will be reachable from beyond a network services platform's domain and needs protection from misuse and abuse. More precisely, security mechanisms for the protection of controller and inter-controller interfaces should be established. In addition, the definition of security mechanisms for north-/southbound and inter-controller interfaces, securing the controller can prevent adversaries from applying Denial of Service (DoS) attacks. Design principles followed by VirtuWind will guarantee that secure communication for all interfaces (north-/south-/east-/west-/bound) is possible. The communication channel between each SDN layer will be well protected (e.g., OpenFlow protocol is protected by Transport Layer Security (TLS)). Security measure techniques such as secure coding, deployment of integrity checks, and most importantly, application digital signing, will be used. Moreover, all communication channels can be hardened using TLS security.

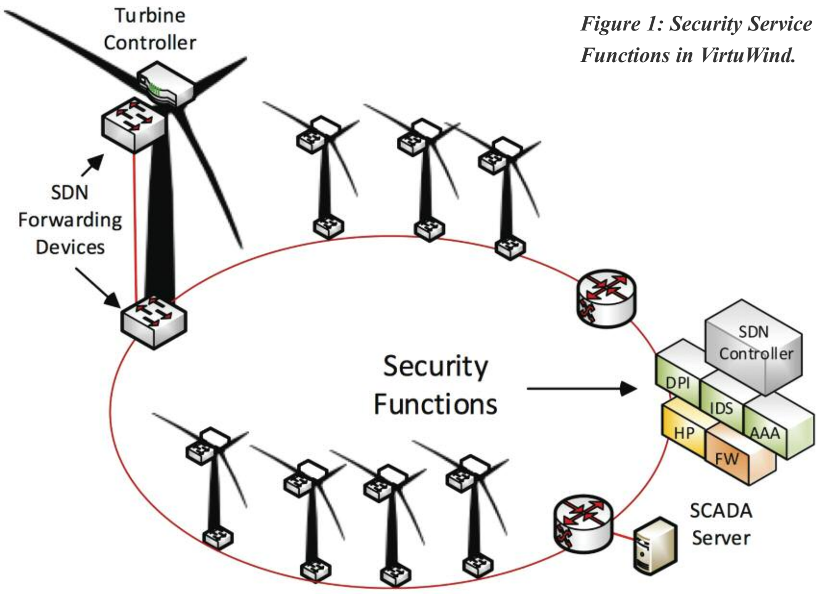


Figure 1: Security Service Functions in VirtuWind.

Incident Detection Analysis and Prevention

The development of intra- and inter-domain incident detection mechanisms including real-time detection, analysis and prevention is necessary for the trace-backs and audits enhancing root cause analysis during incident response, and failure analysis mechanisms. To achieve this objective, VirtuWind will deploy network monitoring and intrusion detection for identification of attacks and run-time network adaptation for attack response and mitigation mechanisms. Mechanisms such as firewalls (FW), intrusion detection systems (IDS) and deep packet inspection systems (DPI) should be in place to detect malicious activity on the SDN, assess its impact, and evaluate the system's response and attack mitigation effectiveness. The intrusion detection mechanism will be also based on 'honeypot' (HP) technology that can visualise and show in real-time the attacks in the inter-domain SDN. Application, control and data plane should feature the appropriate elements (e.g., dummy devices) and interfaces (e.g., supporting mirroring and redirect traffic) to enable the deployment of data and/or control plane SDN honeypots and the backend assessment of the information they aggregate.

VirtuWind project is one of the 5G-PPP phase-1 Innovation Action projects under the Horizon 2020 framework. This three-year project commences on 1st July, 2016. The VirtuWind consortium consists of strong industry (Siemens, NEC, Deutsche Telecom, Intel, Intracom, WorldSensing) and academic partners (FORTH (ERCIM member), Kings College London, Technical University Munich) covering the whole value chain of programmable networks. The consortium is striving for a common vision of creating industrial capability of SDN/NFV in Europe.

Link:
http://www.virtuwind.eu

References:

[1] N. Petroulakis et al.: "VirtuWind: Virtual and Programmable Industrial Network Prototype Deployed in Operational Wind Park", EUCNC 2016
[2] Threat Landscape and Good Practice Guide for Software Defined Networks/5G, ENISA 2016

Please contact:

Ioannis Askoxylakis
ICS-FORTH, Greece
asko@ics.forth.gr

Bypassing Malware Obfuscation with Dynamic Synthesis

by Fabrizio Biondi, Sébastien Josse, and Axel Legay (Inria)

Black-box synthesis is more efficient than SMT deobfuscation on predicates obfuscated with Mixed-Boolean Arithmetics.

Malware – programs that exhibit malicious behaviour – poses a significant threat to computer security. Government, industry, and individuals spend billions of euros each year to defend themselves from malware or recover from malware attacks. To fight malware, antivirus programs such as those produced by Norton, Kaspersky and Malwarebytes must be able to determine whether a file contains malware; this is known as malware analysis. Malware analysis can be performed either on-demand, i.e., when requested by the user, or on-access, i.e., when the user invokes a file and it has to be analysed before the system runs it. On-access analysis has to be completed in a very short time to avoid making the system unresponsive. The TAMIS team at the High Security Lab of Inria Rennes is pushing the state of the art in open-source automated malware analysis by unifying many different techniques into a single tool and developing new theoretical foundations for malware deobfuscation and classification.

Executable files are the most common carriers of malware, since they already have execution privileges. Since statically analysing or dynamically executing every possible execution trace of the executable would be prohibitively expensive, particularly in the on-access analysis scenario, antivirus programs use symbolic analysis. Important tools for symbolic analysis include the KLEE-based S2E tool and the popular IDA Pro reverse engineering environment. Symbolic analysis represents a set of traces as a set of constraints over the variables of the traces, and are able to analyse all such traces at once. However, this depends on the ability to create and maintain a set of constraints representing such traces. SMT solvers are employed to decide the satisfiability of the constraints.

To hinder symbolic analysis, malware creators employ obfuscation techniques [1]. Obfuscation consists of complicating the malware's code into an equivalent representation that is harder to analyse symbolically. For instance, obfuscation can be used to:

- Make the control flow of the executable depend on symbolic variables by inserting into the assembly code of the executable a conditional jump statement whose target depends on a variable. The analysis will not be able to coherently keep track of all possible executions of the program since they depend on the possible values of the variable, and thus will not be able to know how to proceed with the analysis of the traces.
- Embed a virtual machine with instructions generated on-the-fly in the code and execute the real code on the virtual machine, making it harder to follow the program flow.
- Encrypt and pack parts of the malware to be decrypted and executed from memory only at runtime, hindering static analysis.
- Modify the malware by acting on its memory space.
- Bloat the size of the constraint set to be maintained by the symbolic representation. This is the case with Mixed-Boolean Arithmetic (MBA) obfuscation [2], where a polynomial function f and some statements equivalent to zero ei...ek are used to transform and diversify a given statement s into a complex equivalent statement using the formula $s = f^{-1}\left(\sum_{i=1}^{k} e_i + f(s)\right)$ making it much harder to analyse. MBA obfuscation is commonly used by DRM systems deployed by Irdeto, for instance, but has also been detected in malware compilation chains.
- Make it impossible for the antivirus to reconstruct the control flow of the malware, thus hindering fingerprinting and allowing the malware creator to hide malicious code in parts of the binary that the analysis mistakenly considers as dead code. Obfuscating conditionals (e.g., with MBA obfuscation) makes it hard for the antivirus to recognize which parts of the code are reachable and which are dead.

Given the wide variety of available techniques and their complexity, it is very hard to counteract obfuscation in the limited time given by the on-access scenario. We will focus on the last of the cases listed, where the common deobfuscation approach is to use SMT solvers like STP, Z3 or Boolector to determine the satisfiability of the MBA-obfuscated conditionals.

The solution we propose is to employ dynamic synthesis techniques [3] to decide satisfiability instead of deobfuscation. While deobfuscation tries to understand the behaviour of an obfuscated statement by studying it, synthesis instead interrogates the statement as a black box by feeding it inputs and studies the corresponding outputs. Since a conditional statement is just a function from its inputs to a Boolean value, finding inputs for which the statement can be true and false is sufficient to determine its satisfiability. Hence, synthesis is able to determine the satisfiability of a statement without having to understand it, just by analysing its input-output behaviour on an appropriate number of experiments.

We have analysed MBA-obfuscated 64-bit conditional statements and tried to understand their behaviour using multiple state-of-the-art SMT solvers, and using our own synthesis-based approach. Since the strength of the MBA obfuscation depends on the degree of the polynomial used, we have experimented with different polynomial degrees. The results are reported in our working paper, available at https://hal.inria.fr/hal-01241356v1 , and summarised in Table 1.

It is clear from the table that dynamic synthesis is less affected by the degree

MBA polynomial degree	Solution time for SMT solvers (s)			Dynamic synthesis time (s)
	STP	Z3	Boolector	
2	0.679	3.680	0.748	5.022
3	4.339	26.976	3.183	6.000
4	17.368	101.520	31.916	6.407
5	54.895	172.228	36.439	7.935

Table 1: Solution time for SMT solvers and dynamic synthesis against MBA obfuscation.

of the polynomial used in the obfuscation than SMT solvers. Since the size of the obfuscated statement grows exponentially with the degree of the obfuscation polynomial, SMT solving time also tends to grow significantly. On the other hand, since synthesis just interrogates the obfuscated statement, the statement's size is much less relevant. While on small-degree polynomials SMT solvers outperform synthesis, such a low level of obfuscation is not representative of the sophisticated techniques used by malware in the wild. On the other hand, the scalability of the synthesis method shows promise against real malware obfuscation, since synthesis sidesteps the deobfuscation problem.
On-access malware analysis is a crucial protection against infection, and efficient deobfuscation techniques are fundamental to detecting malware with limited time. Thanks to synthesis, we will be able to create more efficient malware analysis techniques, taking an important step towards a more secure cyberenvironment.

Our research is supported by the Pôle d'excellence Cyber, bringing together Inria, DGA, Supélec and the Bretagne region.

References:

[1] S. Schrittwieser, et al.: "Protecting Software through Obfuscation: Can It Keep Pace with Progress in Code Analysis?", ACM Computing Surveys (CSUR) 49 (1), 4.
[2] Y. Zhou, A. Main, Y. X. Gu, H. Johnson: "Information Hiding in Software with Mixed Boolean-Arithmetic Transforms", Information Security Applications: 8th International Workshop, WISA 2007, Revised Selected Papers, 2007.
[3] R. Balaniuk: "Drill and join: A method for exact inductive program synthesis", in Logic-Based Program Synthesis and Transformation – 24th International Symposium, LOPSTR 2014, Canterbury, UK, Revised Selected Papers, 2014.

Please contact:

Fabrizio Biondi and Axel Legay
Inria, France
fabrizio.biondi@inria.fr,
axel.legay@inria.fr

SPLIT: Security Protocol Interaction Testing in Practice

by Dimitris E. Simos (SBA Research)

The SPLIT project applies methods from the field of combinatorial (interaction) testing and model-based testing with the aim of providing quality assurance to software security protocols. The project thus makes a significant contribution towards protecting the information of communicating parties in a digitally connected society.

Security protocols are communication protocols that guarantee the security properties (authentication or confidentiality) by defined rules and cryptography methods. The mathematics community tried to suppress revelations that the NSA BULLRUN and PRISM projects eavesdropped on user communications as well as planting backdoors in cryptographic systems that protect our data [1]. Computer scientists may need to re-verify the popular cryptography methods and protocol designs for secure communication (e.g., TLS/SSL, SSH) in order to win back public trust in security mechanisms and products. Even when the security protocols are designed perfectly, backdoors may also be proposed during the implementation of the protocols and pave the way for breaches of security by potential attackers. The SPLIT project addresses this important security problem and proposes different models and algorithms to verify the security of the related protocol implementations automatically and reveal the infused backdoors.

In particular, the security aspects of protocol implementations have so far not been thoroughly tested and potential security vulnerabilities can have a severe impact on their intended functionality. Part of the reason for this is that security testing still lacks automation and thus requires a lot of resources.

SPLIT [L1] faces the challenges of developing automated security testing methods that can analyse security protocols and prove that they have been implemented securely, and of bringing security testing into the software development life cycle early on as part of an ICT process. We have three specific goals:

1. Methodology for security protocol interaction testing: We aim to create new models and establish algorithmic foundations for model-based testing [2] and combinatorial testing [3], respectively, so that a wide range of security protocols and their respective implementations can be evaluated for detecting vulnerabilities with guaranteed levels of trustworthiness in security testing results. A framework for detection of flaws in protocol specification will be provided, which checks whether an implementation is vulnerable to different types of attacks.

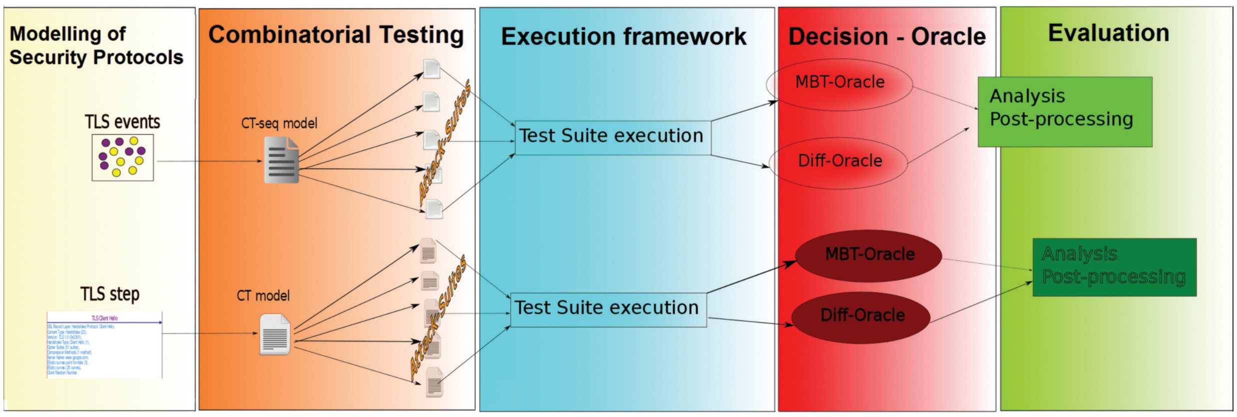


Figure 1: Methodology of the SPLIT project.

2. Improving automation for security testing: We aim to ensure and improve automation during the security testing process by combining the aforementioned testing methodologies. In particular, even in the early phases of software development, the availability of a testing framework for security can significantly improve the likelihood of detecting security related faults early, thereby contributing to the overall quality of the generated software.

3. Provide quality assurance: We aim to provide quality assurance of implementations of security protocols and to prove that they have been implemented securely. We will do so on two levels: One will be to examine the order of execution of events of the protocol at a macro level, the other will be to examine each major step atomically and take a detailed look at error handling at each step. This way we also attempt to show the correctness of the protocol itself.

The SPLIT project has been running since February 2016 and is funded by the BRIDGE Early Stage Program (a funding scheme of the FFG, the Austrian Research Promotion Agency). The project is led by SBA Research in collaboration with Graz University of Technology and OBJENTIS Software Integration, all located in Austria. University of Texas at Arlington and the National Institute of Standards and Technology (NIST), both based in USA, serve in the project's advisory board.

Currently, a group of ten researchers – mathematicians, software engineers and security specialists – is working in this project towards an automated testing framework based on combinatorial methods that can be used for X.509 certificate testing. Work on model-based testing approaches for the description of attacks that can occur in the TLS protocol and combinatorial coverage measurements for TLS cipher suites recommendations is also in progress.

Link:
[L1] https://www.sba-research.org/split/

References:

[1] A. Odlyzko: "The Mathematical Community and the National Security Agency", in Notices of the American Mathematical Society, Volume 61, Number 6.
[2] I. Schieferdecker, J. Grossmann, M. Schneider: "Model-based security testing", in Proc. of the Model-Based Testing Workshop at ETAPS 2012, p. 1–12, 2012.
[3] D. Kuhn, R. Kacker, Y. Lei: "Practical combinatorial testing", NIST Special Publication 800-142, 2010.

Please contact:

Dimitris E. Simos, SBA Research, Vienna, Austria
dsimos@sba-research.org

Gorille: Efficient and Relevant Software Comparisons

by Philippe Antoine, Guillaume Bonfante and Jean-Yves Marion (Loria)

Binary code analysis is a complex process that can only be performed by skilled cybersecurity experts whose workload just keeps increasing. Gorille greatly speeds up their daily routines, while providing them with more in-depth knowledge.

During our work on the complexity of algorithms and on computational models, we developed an interest in malware and viruses. Malicious software – which have been increasingly discussed in the mainstream media lately with the rise of advanced cyber attacks – represent a practical case in which hackers push cybersecurity tools to their limits by placing them in the worst-case scenario. Currently, there simply aren't enough skilled engineers available to cope with the ever increasing amount of data required for cyber defence. Since the threats are still relatively new and still evolving, professionals in this area still lack some automated tools to allow them to engage in a process of continuous improvement. This is true for cybersecurity generally, but particularly for the specific branch of binary code analysis known as reverse engineering.

Binary code analysis has become a major topic of research in the last decade. Use cases include vulnerability detection, testing, clustering and classification and malware analysis. Perhaps one of the best known tools so far is bindiff [1], a comparison tool for binary files designed to quickly find differences in similar software (before and after a patch for instance) using their disassembled code. Our system Gorille takes a different approach, looking for similarities instead of differences. This design is more efficient when the compared binary files differ more than they share code. This philosophy permits us to build a scalable solution, capable of running comparisons against a database with millions of samples in seconds on a regular laptop.

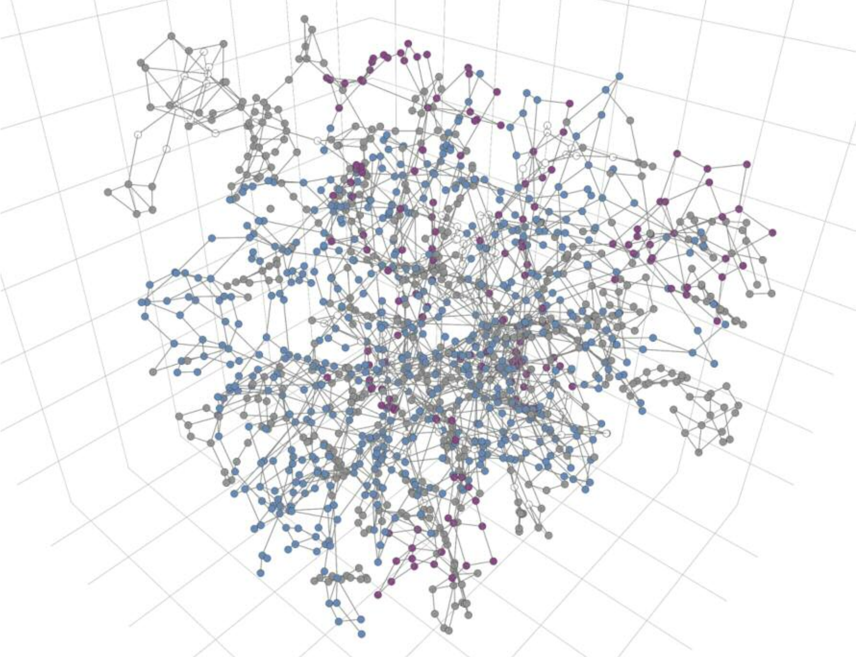


Figure 1: 3D representation of a control flow graph.

Furthermore, Gorille's refine output, connecting almost-identical pieces of code, can be used in several ways for retro-engineering as shown in [2]: function identification or malware classification into families for example. Thanks to the automation of the process, the addition of new samples to a knowledge database is simple, making it painless to share information before the next version of the malware pops up.

In order to achieve meaningful results, Gorille and other solutions strive towards a high level of semantics for the binary code. Control flow graphs provide a fair level of abstraction to deal with the binary codes they represent. This structure is currently being thoroughly used in state-of-the-art papers [3] and is the basic input for Gorille. After applying some graph rewriting rules to normalise these graphs, our software tackles the subgraph search problem in a way which is both efficient and convenient for that kind of graph. This technique is described as morphological analysis since it recognizes the whole shape of the malware.

That being said, some pitfalls still need to be considered. First, the output will only be as good as the input data. And it is known that static disassembly cannot produce the perfect control flow graph since software on a Turing machine are able to modify themselves, thus making this problem an undecidable one. As a matter of fact, malware heavily use obfuscation techniques such as opaque predicates to hide their payloads and confuse analyses. Dynamic analysis should then be used along with static disassembly to combine their strengths.

Another dangerous pitfall feared by every expert is the 'false positives rate': false alarms that result in precious time being wasted assessing the reality of the threat. Shared binary code is not always relevant as software often has embedded static standard libraries. Gorille's solution to this issue lies in graph rewriting. By rewriting classic subgraphs into configuration-based special nodes, we obtain an even higher abstraction of the control flow graph.

There is enormous potential to get more out of Gorille: for instance, by building more knowledge databases to recognize packers; by making it compatible with different kinds of binary code such as java or ARM; or by following process executions to check they do not get out of their usual control flow graph (meaning a bug is exploited). The next breakthrough we are working on related to the data flows which will bring additional useful information to control flows, thanks to brand new results in abstract interpretation or data tainting.

The research institute LORIA in Nancy, France, aims to do more than science with Gorille. As part of its involvement in the local economy, a spinoff called Simorfo will be created in 2016 to put the morphological analysis technology to test on the market. This will be one more achievement after other collaborations in cybersecurity such as joint work with TRACIP, a local cyber-forensics company, or lybero.net, the latest spinoff from the cryptography team created in March. Simorfo aims to become a European leader in cybersecurity, providing innovative solutions and measurable returns on investment to its clients through the various skills of its team.

Link:
http://www.lhs.loria.fr/wp/?page_id=96

References:

[1] H. Flake: "Structural Comparison of Executable Objects", DIMVA, 2004, http://www.zynamics.com/downloads/dimva_paper2.pdf.

[2] G. Bonfante, J.-Y. Marion, F. Sabatier: "Gorille sniffs code similarities, the case study of Qwerty versus Regin", 10th Int. Conference on Malicious and Unwanted Software, Oct 2015, https://hal.inria.fr/hal-01263123/

[3] A. Abraham et al.: "GroddDroid: a Gorilla for Triggering Malicious Behaviors", 10th Int. Conference on Malicious and Unwanted Software, Oct 2015, https://hal.inria.fr/hal-01201743

Please contact:

Philippe Antoine
LORIA, France
philippe.antoine@loria.fr

Vulnerability Prediction Against Fault Attacks

by Nisrine Jafri, Axel Legay and Jean-Louis Lanet (Inria)

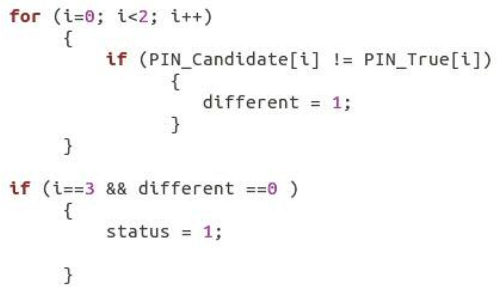
Fault-injection exploits hardware weaknesses to perturbate the behaviour of embedded devices. Here, we present new model-based techniques and tools to detect such attacks developed at the High-Security Laboratory at Inria.

Embedded systems are computer systems with a dedicated function within larger mechanical or electrical systems. Unlike classical computer units, they are embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many common devices, including smart phones, cars, smart cities, and robots. The number of embedded systems is growing continuously at a rate of more than 10% per annum, and by 2020 there are predicted to be over 40 billion devices worldwide (five to ten embedded devices per person on earth). It is thus very important that the engineering process for embedded systems development includes techniques to assess a wide range of safety/availability/security requirements.

'Fault injection' is an attack where the hardware is used to create exploitable errors at the software level. This includes modifying a value read from memory and modifying the program flow using different techniques including: laser, voltage modification, or even clock glitches [1]. The Row Hammer attack [2] is a classic example of a fault injection. The idea behind the Row Hammer attack was to design a program that repeatedly accesses a certain row of transistors in the DRAM memory. The effect was to stress the row until the charge from that row leaks into the next one. This electromagnetic leakage can cause a bit flip such that transistors in the adjacent row of memory have their state inverted.

The power of fault injection can be illustrated with a simple PIN verify program. This C program, which is described in Figure 1, compares a PIN candidate with the true PIN. In the case that the two are equals, variable status is set to 1, otherwise it remains at 0. Observe that if the two PINs are different there is no way to obtain status=1 simply by exploiting the software layer. However, this can be done by mutating the value of the x86 binary code. Figure 2, which represents the binary code for Figure 1, shows this modification via the mutation of one bit that corresponds to the value of status. This mutation can be performed via bit reset, for example.

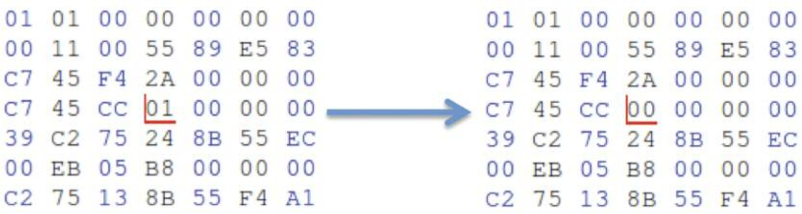
One of our goals is to propose a formal model-based tool to detect faults of this type. The major difficulty is that contrary to classical security vulnerabilities such as buffer overflow, fault injection detection requires not only modelling the software but also the hardware and its interactions. Consequently, applying formal models leads to two challenging problems that are: (i) To develop techniques that produce mutations of binary code, which correspond to a hardware fault injection, and (ii) To offer techniques that analyse such code.



```
for (i=0; i<2; i++)
     {
         if (PIN_Candidate[i] != PIN_True[i])
               {
                  different = 1;
               }
     }
if (i==3 && different ==0 )
     {
         status = 1;

     }
```

Figure 1: Part of C code where the attack is performed.



```
01 01 00 00 00 00 00          01 01 00 00 00 00 00
00 11 00 55 89 E5 83          00 11 00 55 89 E5 83
C7 45 F4 2A 00 00 00          C7 45 F4 2A 00 00 00
C7 45 CC 01 00 00 00   --->   C7 45 CC 00 00 00 00
39 C2 75 24 8B 55 EC          39 C2 75 24 8B 55 EC
00 EB 05 B8 00 00 00          00 EB 05 B8 00 00 00
C2 75 13 8B 55 F4 A1          C2 75 13 8B 55 F4 A1
```

Figure 2: Machine code before and after fault injection.

For Challenge (i), our tool relies on existing fault models and mutation techniques. Obtaining such models is a major effort, which is beyond the scope of this article. For challenge (ii), we propose to use model checking [3]. The approach has already been used at high-level code, but little has been done at the binary level. In fact, the main obstacles to model checking machine code are modelling a complex processor and exceptional control flow.

To bypass these issues, we used the intermediate representation of the LLVM compiler framework. LLVM is a collection of modular and reusable compiler and toolchain technologies. Such an intermediate representation offers a much simpler syntax and semantics than a high-level programming language, and thus eases a logical encoding of the verification problem considerably. For this reason, it has recently become increasingly common to analyse programs not on the source code level but on the level of compiler intermediate representation (IR) instead. This approach has several advantages: first, the IR has much simpler syntax and semantics than high-level language; second, the program that is analysed using the IR is much closer to the program that is actually executed on the computer since semantical ambiguities have already been resolved by the compiler.

The first step in our process is thus the translation of machine code to LLVM IR. There are several tools that can be used for this purpose. Our experiments show that MC-sema [L1] is a best compromise for x86 architecture. Mc-sema is a framework for translating x86 binaries into LLVM bytecode. MC-sema models x86 instructions as operations on a register context structure that contains all registers and flags, and instructions semantics are expressed as modifications of structure members. In the future, we will have to explore alternatives for other architectures. Indeed, x86 is restricted to a small number of embedded systems. Here, what matters is the proof of concept.

Now that we have the intermediate representation of our binary file, the second step is to verify it. There are several alternatives for verifying LLVM among which one finds DIVINE, or a translation to classical tool such as SPIN. As fault injection mainly introduces safety/invariant perturbations, we propose to use LLBMC [L2]. This tool employs a bounded model checking using an SMT-solver for the theory of bitvectors and arrays and thus achieves precision down to the level of single bits. Bounded model checking was originally introduced in the context of hardware and is known to be best for safety issues.

In conclusion, this paper presents a proof-of-concept approach for fault-injection analysis via formal model. It has been successfully applied to case studies, including the example given above. For the approach to be deployed one has to improve our fault models as well as to extend LLVM and Mc-sema to a wider class of instruction of x86 as well as to other architectures such as ARM, the standard for smart phones.

Links:
[L1] https://github.com/trailofbits/mcsema/
[L2] http://llbmc.org/

References:

[1] H. Bar-El, et al.: “The Sorcerer’s Apprentice Guide to Fault Attacks”, in Proc. of IEEE, vol. 94, issue 2, pp:370-382, 2006.
[2] D. Gruss, C. Maurice, S. Mangard: “Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript”, 13th Conf. on DIMVA, 2016.
[3] C. Baier, JP. Katoen: “Principles of model checking”, MIT Press 2008.

Please contact:

Nisrine Jafri
Inria, France
nisrine.jafri@inria.fr

Challenges in Android Malware Analysis

by Valérie Viet Triem Tong (CentraleSupelec), Jean François Lalande (INSA Centre Val de Loire) and Mourad Leslous (Inria)

The best protection against malware is to execute it: a security paradox.

Android has become the world’s most popular mobile operating system, and consequently the most popular target for unscrupulous developers. These developers seek to make money by taking advantage of Android users who customise their devices with various applications, which are the main malware infection vector. Indeed, the most likely way a user will execute a repackaged application is by downloading a seemingly harmless application from a store and executing it. Such an application will have been modified by an attacker in order to add malicious pieces of code. Consequently, a user will have to deal with one of the many different types of malware, such as aggressive adware that constantly display ads making the device unusable, ransomware that encrypt user’s data and require a ransom to be paid to decrypt it or remote administration tools (RAT) that take control of the device and allow the attacker to use it as his own.

To fight repackaged applications containing malicious code, most official application marketplaces have implemented security analysis tools that try to detect and remove malware. In this battle between application stores and malware developers, the latter are a step ahead. Malware developers have imagined a lot of countermeasures to defeat security analysis. These countermeasures can be divided into two main approaches: avoiding static analysis and avoiding dynamic analysis.

A static analysis of an application consists of analysing its code and its resources without executing it. For instance, this can simply amount to listing all the permissions required by the application, while checking that these permissions cannot be used maliciously. Static analysis is also used to evaluate the similarity between the application under review and well-known malicious code. Thus to avoid static analysis detection, a developer needs only create unreachable or unintelligible malicious code. Obfuscation techniques, encryption and dynamic loading of code are used to achieve this and disqualify static analysers.

Conversely, dynamic analysis stands for any kind of analysis that requires executing the application in order to observe its actions. Dynamic analysis grants understanding of how an application interacts with other objects in its environment. This kind of analysis is not influenced by the nature of the code executed, whether obfuscated, encrypted or protected by any other means against static analysis. As a matter of fact, the main protection against dynamic analysis coined by malware developers is merely to delay execution of the malicious code. This can be done by waiting for a special event, such as a command sent by a remote server before triggering the malicious code. Moreover, if the malicious code is hard to trigger, dynamic analysis will most likely detect nothing.

The Kharon project [L1] goes a step further from classical dynamic analysis of malware (http://kharon.gforge.inria.fr). Founded by the Labex CominLabs and involving partners of CentraleSupélec, Inria and INSA Centre Val de Loire, this project aims to capture a compact and comprehensive representation of malware. To achieve such a goal we have developed tools [1] to monitor operating systems’ information flows induced by the execution of a marked application.

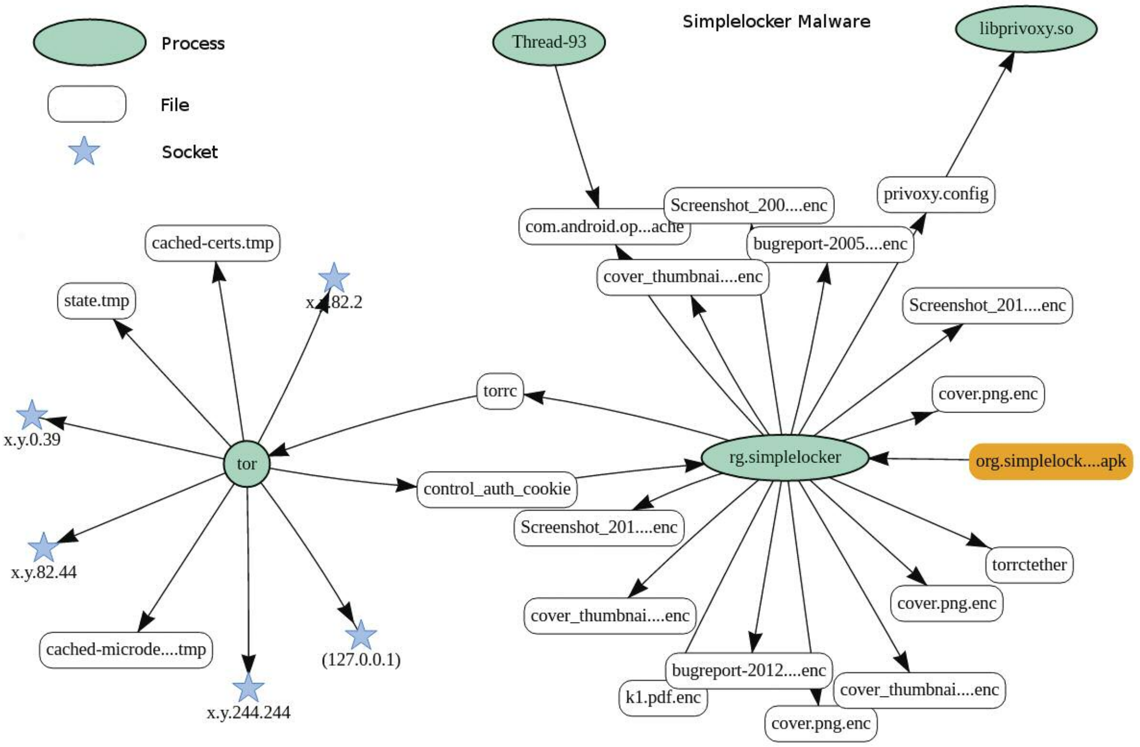


Figure 1: Comprehensive representation of malware.

Figure 1 illustrates an example of such a representation. The studied application's code (.dex file) has been marked and monitored. The graph explains how this piece of code has infected the operating system: which files, sockets and processes have been created or modified. Finally, if the malicious code has been executed, the graph summarises the attack. For example, the execution that has led to the graph represented in Figure 1 has been computed from the observation of the execution of a ransomware : SimpleLocker [2]. The graph shows that the malware starts by encrypting a user's files (*.enc files) and then initiates a remote communication through the TOR anonymous network to check if the user has paid the ransom.

In the Kharon project, we support the idea that the best way to understand malware impact is to observe it in its normal execution environment i.e., a real smartphone. Additionally, the main challenge is to be able to trigger malicious behaviours even if the malware tries to escape dynamic analysis.

In this context, we have developed an original solution that mainly consists of 'helping the malware to execute'. In other words we slightly modify the bytecode of the infected application in order to defeat the protection against dynamic analysis and we execute the suspicious code in its most favourable execution conditions. Thus, our software helps us understand malware's objectives and the consequences on the health of a user's device.

Based on these observations, our main research direction and challenge is to develop new and original protections against malicious applications that try to defeat classical dynamic analysis.

Link:

[L1] http://kharon.gforge.inria.fr/

References:

[1] A. Abraham et al.: "GroddDroid: a gorilla for triggering malicious behaviors", in 10th International Conference on Malicious and Unwanted Software, MALCON 2015, IEEE Computer Society, pp. 119-127, 2015.

[2] N. Kiss, J.-F. Lalande, M. Leslous, V. Viet Triem Tong : "Kharon dataset: Android malware under a microscope", in Learning from Authoritative Security Experiment Results, IEEE Symposium on Security and Privacy Workshop, 2016.

Please contact:

Valérie Viet Triem Tong
CentraleSupélec, France
+33 99 84 45 73
valerie.viettriemtong@centralesupelec.fr

Cybersecurity in Robotic Systems

by Vicente Matellán, Francisco J. Rodríguez –Lera and Jesús Balsa (University of Léon)

The robotics industry is set to suffer the same problems the computer industry has been facing in recent decades. This is particularly disturbing for critical tasks such as those performed by surgical, or military robots, but it is also challenging for the ostensibly benign household robots such as vacuum cleaners and tele-conference bots. What would happen if these robots were hacked? At RIASC (Research Institute in Applied Science in CyberSecurity) we are working on tools and countermeasures against cyber attacks in cyber-physical systems.

Robots are set to face similar problems to those faced by the computer industry when the internet spread 30 years ago. Suddenly, systems whose security had not been considered are vulnerable. Industrial robots have been working for decades, physically protected by walls and cybernetically by their isolation. But their protection is no longer assured: manufacturing facilities are now connected to distributed control networks to enhance productivity and to reduce operational costs and their robots are suffering the same problems as any other cyber-physical system.

Manufacturers of robots for critical applications were the first to express concern. Defence and security robots, which, by definition are exposed to hostile attacks, were the first robots to be hardened. But some other applications, such as medical robots, are equally critical.

Currently, medical robots are usually tele-operated systems, which exposes them to communications threats. Applied to tele-surgical robots these problems can be grouped into four categories:

- Privacy violations: information gathered by the robot and transmitted to the operator is intercepted. For instance, images or data about a patient's condition can be obtained.
- Action modifications: actions commanded by the operator are changed.
- Feedback modifications: sensor information (haptic, video, etc.) that the robot is sending to the operator is changed.
- Combination of actions and feedback: the robot has been hijacked.

At RIASC [L1] we think that the real challenge will be the widespread use of service robotics. Household robots are becoming increasingly common (autonomous vacuum cleaners, tele-conference bots, assistants) and as Bill Gates observed [1] this is just the beginning. The software controlling these robots needs to be secured, and in many cases the software was not designed with security problems in mind.

Many service robots, for instance, are based on Robotic Operating System (ROS). ROS started as a research system, but currently most manufacturers of commercial platforms use ROS as the de facto standard for building robotic software. Well-known and commercially successful robots like Baxter (in Figure 1) are programmed using ROS and almost all robotic start-ups are based on it owing both to the tremendous amount of software available for basic functions and to its flexibility.

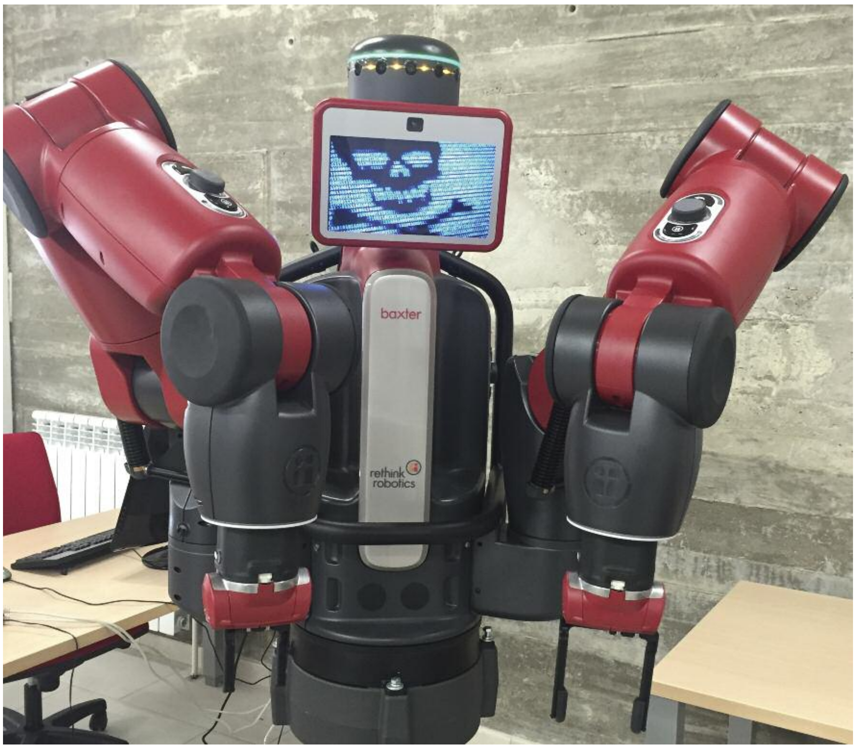


Figure 1: Hacked Baxter robot.

ROS [L2] is a distributed architecture where 'nodes', programs in ROS terminology, 'publish' the results of their computations. For instance, a typical configuration could be made up by a node that receives sensor data (is 'subscribed' to that data) and publishes information about recognized objects in a 'topic'. Another node could publish the estimated position of the robot in a different topic. And a third one could 'subscribe' to these two topics to look for a particular object required by the user.

Messages in this set-up are sent using TCPROS the ROS transport layer which uses standard TCP/IP sockets. This protocol uses plain-text communications, unprotected TCP ports, and exchanges unencrypted data. A malicious malware could easily interfere with these communications, read private messages or even supersede nodes. Security was not a requirement for ROS at its conception, but now it should be. New ROS 2 [L3] is being developed using Data Distribution Service middleware to address robotics cyber vulnerabilities.

The situation is potentially even worse in cloud robotics. There are several companies whose robots use services in the cloud, which means that readings from robot sensors (images, personal data, etc.) are sent over the internet, processed in the company servers and sent back to the robot. This is nothing new – it happens every day in our smartphone apps – but a smartphone is under our control; it does not move, it cannot go to our bedroom by itself and take a picture, it cannot drive our car.

Talking about cars, self-driving cars are currently one of the best-known instance of "autonomous service robots" and a good example of cloud robotics. Many cars are currently being updated remotely [L4] and most cars use on-line services, from entertainment to localization or emergency services.

Risk assessment should be the first step in a broad effort by the robotics community to increase cybersecurity in service robotics. Marketing and research are focused on developing useful robots, but cybersecurity has to be a requirement: robots need cyber safety. Hacking robots and taking control of them may endanger not only the robot, but humans and property in the vicinity.

Links:
[L1] http://riasc.unileon.es
[L2] http://ros.org
[L3] http://design.ros2.org/
[L4] https://www.teslamotors.com/blog/summon-your-tesla-your-phone

References:
[1] B. Gates: "A robot in every home", Scientific American, pp. 4-11, Jan. 2007, http://www.scientificamerican.com/article.cfm?id=a-robot-in-every-home
[2] M. Quigley, et al.: "ROS: An open-source Robot Operating System", in ICRA Workshop on Open Source Software, 2009, https://www.willowgarage.com/sites/default/files/icraoss09-ROS.pdf

Please contact:
Vicente Matellán
Grupo de Robótica, Escuela de Ingenierías Industrial e Informática, Universidad de León, Spain
+34 987 291 743
vicente.matellan@unileon.es

Co-engineering Security and Safety Requirements for Cyber-Physical Systems

by Christophe Ponsard, Philippe Massonet and Gautier Dallons (CETIC)

Many safety critical systems, like transportation systems, are integrating more and more software based systems and are becoming connected. In some domains, such as automotive and rail, software is gradually taking control over human operations, and vehicles are evolving towards being autonomous. Such cyber-physical systems require high assurance on two interrelated properties: safety and security. In this context, safety and security can be co-engineered based on sound techniques borrowed from goal-oriented requirements engineering (RE).

Transportation systems are increasingly relying on software for monitoring and controlling the physical word, including to assist or replace human operation (e.g., drive assistance in cars, automated train operations), resulting in higher safety-criticality. At the same time, the increasing connectivity of (cyber-physical) systems also increases their exposure to security threats, which in turn can lead to safety hazards. This calls for a co-engineering approach to security and safety [1].

Requirements engineering (RE), a key step in any system development, is particularly important in transport systems. Over the years, very efficient methods have been developed both for dealing with safety and security. Goal-oriented requirements is a major RE approach that has developed the concept of obstacle analysis primarily to reason on safety [2]. An obstacle can be considered as any undesirable property (e.g., a train collision) that directly obstructs system goals (e.g., passenger safety) which are desired properties. This work has later been revisited to deal with security [3]. It introduced the notion of malicious agents having interest in the realisation of some anti-goal (as the dual of 'normal' agents cooperating to the achievement of a system goal). Table 1 compares the safety and security approaches side by side and highlights their strong common methodological ground.

While generally considered separately, we have combined safety and security approaches for co-engineering purposes – an approach that makes intuitive sense given their strong common foundations, including the ability to drive the discovery of hazards/threats and to identify ways of addressing them. A recent exhaustive survey by the MERGE ITEA 2 project showed the main trends in the area [L1]:

- Safety is at the inner core of the system, providing de facto better isolation. Security layers or different criticality levels are deployed around it.
- Models are used both for safety and security. Safety impact of security failures are considered, hence connecting the two kinds of analysis.
- Both security incidents and system failures are monitored so global system dependability can be continually evaluated.

Based on the Objectiver requirements engineering tool [L2], we experimented with some variants of co-engineering involving different roles working cooperatively on the same model: the system engineer for global system behaviour and architecture, the safety engineer to identify failure modes and their propagation and security engineers to analyse

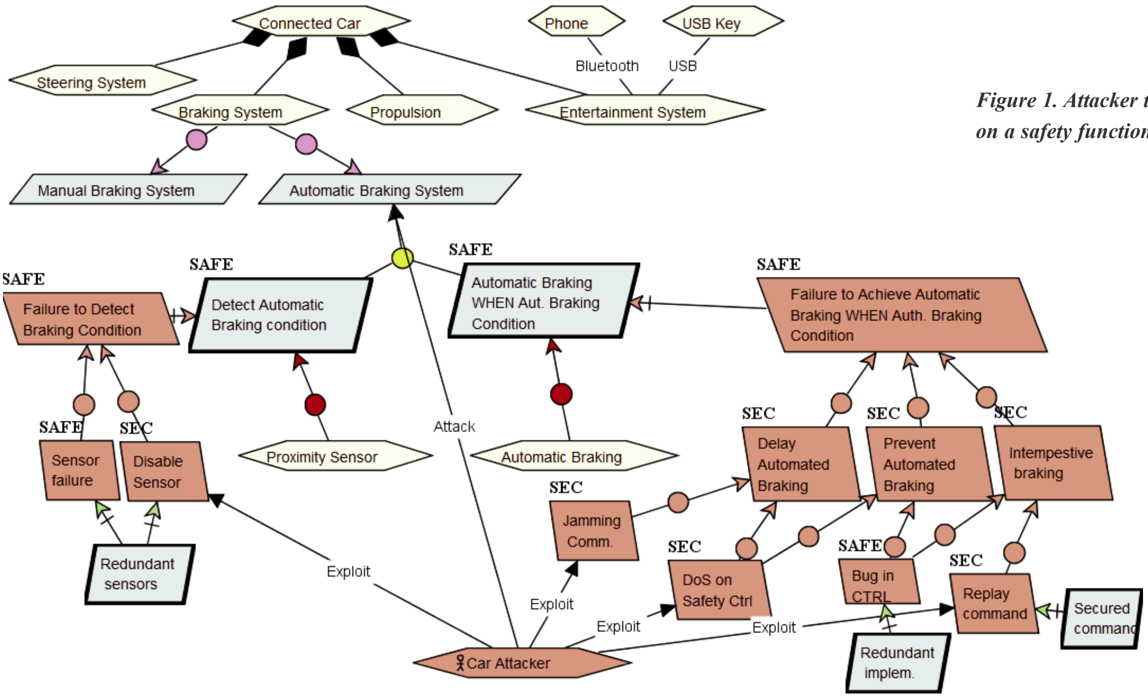


Figure 1. Attacker tree on a safety function.

possible attacks. Proposed resolutions relating to security and safety are reviewed in a second round. Regular global validation reviews are also organised with all analysts.

Figure 1 shows an excerpt of the security/safety co-engineering of a connected car featuring automated braking based on the SAE recommended practices [L3]. The top level shows the general system structure and identifies the main sub-systems. The automated braking sub-system is then detailed based on two key milestones: condition detection and then braking. Next to each requirement, a mixed view of the result of the hazard/threat analysis is shown (these are usually presented in separate diagrams). Specific obstacles are tagged as SAFE or SEC depending on the process that identified them. Specific attacker profiles can also be captured (unique here). Some resolution techniques proposed in [2] and [3] are then applied, e.g., to make the attack unfeasible or to reduce its impact. Some resolutions can also address mixed threats and reduce the global cost to make the whole system dependable.

The next step in our research is to delve deeper into cyber-threats in the context of railway systems. On the tool side we plan to adapt our method to mainstream system engineering tools and methods, such as Capella and in the scope of the INOGRAMS and a follow-up project [L4].

Links:

[L1] http://www.merge-project.eu
[L2] http://www.objectiver.com
[L3] http://articles.sae.org/14503
[L4] https://www.cetic.be/INOGRAMS-2104

References:

[1] D. Schneider, E. Armengaud, E. Schoitsch: "Towards Trust Assurance and Certification in Cyber-, Physical Systems, SAFECOMP Workshops, 2014.

[2] A. van Lamsweerde, E. Letier: "Handling Obstacles in Goal-Oriented Requirements Engineering", IEEE Trans. on Software Engineering, Vol. 26 No. 10, Oct. 2000.

[3] A. van Lamsweerde et al: "From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering", in Proc. of RHAS Workshop, 2003.

Please contact:

Christophe Ponsard
Tel: +32 472 56 90 99
christophe.ponsard@cetic.be

	Safety Engineering	Security Engineering
Goal Category	Safety Goal	Security goal
Obstacle variant	Hazard	Anti-goal (or Threat)
Finest refinement	Root cause	Vulnerability
Agent	Environment (unexpected)	Attacker (malicious)
Impact	Damage to people and things, priority over all other requirements (e.g., availability)	Measured in business terms, e.g., system availability, reputation
Refinement Methods	Fault Tree Analysis, HAZOP, FMECA	Attack trees, Threat trees
Risk management techniques	Obstacle elimination, Obstacle reduction, Obstacle tolerance	Vulnerability removal/isolation, Attack recovery, Attack impact reduction
Analysis Type	Design-time analysis. Updates infrequent. But learning from past accidents is an important activity.	Run-time monitoring to discover vulnerabilities, suspect behaviours. Frequent updates to patch.
Standards	IEC61508 (generic), ISO26262 (automotive), IEC50128 (railways), DO178B/C, etc	Common criteria

Table 1: Comparison of safety and security engineering approaches.

Cyber-Physical Systems: Closing the Gap between Hardware and Software

by Marcel Caria, TU Braunschweig

SHARCS (Secure Hardware-Software Architecture for Robust Computing Systems) is defining new ways to create more secure and trustworthy ICT systems.

We are currently witnessing a tremendous expansion of computerisation – of 'smart' entities and devices – in multiple new areas, such as health care (smart medical implants), automotive (smart cars), urban development (smart cities), power supply (smart grids), and others. This development is inevitably leading society as a whole, and the individuals within it, to increasingly rely on critical applications that sense and control systems in our physical environment. These 'cyber-physical' systems (CPS) use a blend of embedded devices and traditional computing systems, and a variety of communication channels. Our increasing reliance on these systems necessitates improved security [1].

The SHARCS project [L1] aims to establish new and secure-by-design CPS strategies. The intended solutions are supposed to be platform-agnostic, and may also be applied to virtualised environments, such as clouds and other (more traditional) ICT systems. The project started last year with four academic and three industrial partners: Foundation for Research and Technology – Hellas (Greece), Vrije Universiteit Amsterdam (Netherlands), Chalmers University of Technology (Sweden), Technische Universität Braunschweig (Germany), Neurasmus BV (Netherlands), OnApp Limited (UK), IBM – Science and Technology LTD (Israel), and Elektrobit Automotive GmbH (Germany). The project started in January 2015 and has a duration of three years with final outcomes being available in early 2018.

The current approach in security research (as well as in existing security solutions) is largely top-down and demand driven. Security-critical applications, software components, services or protocols (whether known to be vulnerable or not) are protected with piecemeal security tools and patched on demand. Attackers often try to bypass strong protection by redirecting their attacks to software layers below the seemingly strong defensive mechanisms.

Regarding these layers as a chain of software components makes it evident that a system is as secure as its weakest link. Thus, for a system to really be secure, all layers of the software stack must provide the same level of security. In other words: applications, compilers, libraries, drivers, hypervisors, and the operating system, must all be hardened, which may still be insufficient, considering the hardware layer below. We propose that the hardware itself must be secured and enabled to provide the appropriate primitives and capabilities for all the software layers built on top.

SHARCS aims to address the above problems by pushing security mechanisms down the system stack, from software to hardware, which is not only known to be much harder to bypass, but also improves performance, simplicity, and power usage. The three planned operational models (see Figure 1) are: New security functions are ideally pushed to the hardware level (left hand side). However, modifying all levels is not always possible, therefore we provide two more relaxed models. The one shown in the middle requires no hardware changes and all features are communicated to a commodity processor (x86 or ARM) using a hypervisor. The other one (on the right hand side) implements no features at the CPU, and there

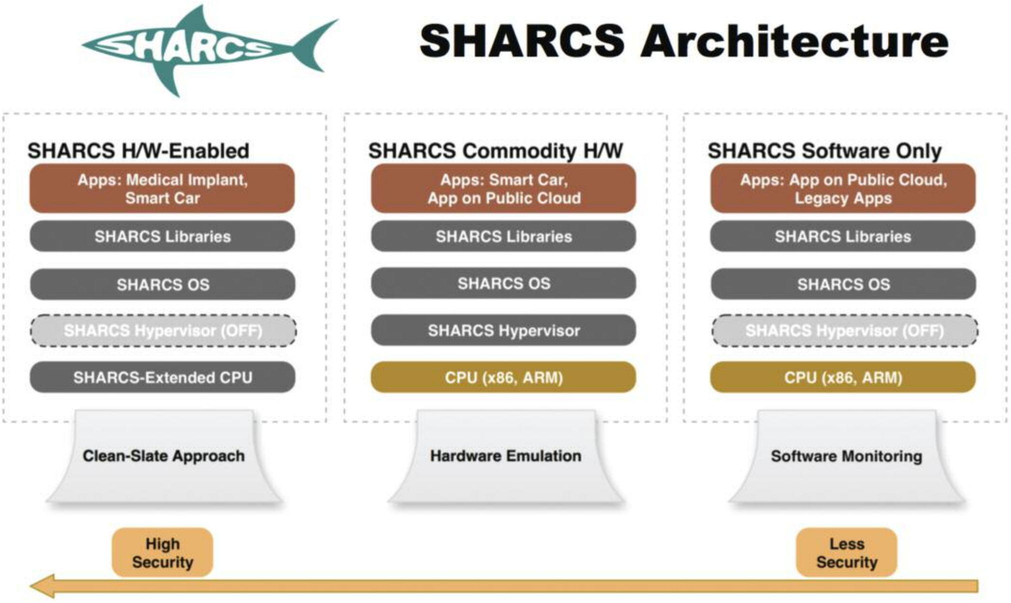


Figure 1: The three planned operational models in SHARCS.

is also no hypervisor available. To realise this last model, we link the application with SHARCS libraries and add kernel modules to the OS, which embed code for reliable and secure monitoring of applications at run-time.

The implementation of core security functions in hardware is one of the central project goals. Techniques like Instruction Set Randomization, Control-Flow Integrity (CFI) [2], and Dynamic Information Flow Tracking will be combined and implemented in hardware, and then supported by the higher (software) layers of the framework. However, security for legacy applications must be provided through security extensions (such as CFI enforcement), which we plan to develop as an integral part of our framework. These extensions should be usable in a transparent fashion, even with proprietary binaries, which will, however, require network requests and assistance from the application's vendor. We thus expect that not all legacy applications will benefit from our framework.

We expect the technologies designed and built in SHARCS to be finally deployed on a very diverse set of security-critical applications. We, therefore, plan to develop an evaluation methodology to assess all security benefits of our framework that have direct security gains in each application domain. This benchmark will also take into account the resource requirements of the examined security features, as well as their typical performance and energy overheads. We consider a security framework's platform independence as vital for its broad employment, which is why we aim to demonstrate SHARCS' universal applicability through the deployment in three real-world use cases: i) a secure, implantable neuromodulator for automatic seizure prevention, ii) secure application execution in an untrusted public cloud environment, and iii) a secure Electronic Control Unit for automotive applications.

Link: [L1] http://sharcs-project.eu

References:

[1] B. Schneier: "The Internet of Things Is Wildly Insecure-And Often Unpatchable", Wired Magazine, January 6, 2014

[2] V. van der Veen, et al.: "Practical Context-sensitive CFI", in Proc. of the ACM Conference on Computer and Communications Security (CCS), Denver, Colorado, US, 2015.

Please contact:

Sotiris Ioannidis, FORTH-ICS, Greece
+30 2810391945
sotiris@ics.forth.gr

SENTER: A Network of the European Centres of Excellence in Cyber Crime Research, Training, and Education

by Evangelos Markatos (ICS-FORTH), Egidija Veršinskienė and Evaldas Bružė (L3CE)

Having exceeded the size of 75 Billion USD in 2015, the worldwide size of the cybersecurity market is expected to reach 170 USD in 2020 increasing rapidly year after year [1]. This market is fueled mainly by cybercrime [2] which has recently reached a cost of 445 billion USD [3]. If left unchecked, cybercrime will have devastating consequences for the development and deployment of our digital society.

To address this issue, in recent years we have witnessed the creation of several national centres of excellence (CoEs) in the area of cybercrime all over Europe. Although some of the CoEs' have made significant achievements, which have been praised in public media as well as within the scientific community, most of the centres have been operating largely in isolation from each other, pursuing different goals, and this has frequently resulted in duplication of effort.

To overcome this fragmentation of resources, SENTER pulled the national centres of excellence together and created a network of the centres of excellence in the area of cybercrime research, training, and education. Having (i) a close relationship with the national law enforcement agencies, (ii) vast experience in developing training courses related to cybersecurity and cybercrime, and (iii) access to high quality R&D infrastructures, the network is in the best position to provide new training methods/techniques and expertise.

The key objectives of SENTER are:
- to create a single point of reference for the European Commission in the area of cybercrime;
- to provide a sustainable international cross-organisational partnership by establishing an international collaboration model;
- to establish interest groups, which will optimise the efforts of existing national centres and avoid fragmentation and duplication of work;
- to create a community of the national centres in the area of cybercrime research training and education, a community that will set its objectives, its common activities, its common goals;
- to facilitate the transfer and adoption of best practices from leading countries to other countries in order to minimise the competence gaps;
- to increase awareness at an international level of the newest scientific and educational achievements in the selected domains (computer forensics, network forensics, mobile forensics, etc) and to speed up the process of scientific achievement productisation and time-to end-user usage;
- to establish a collection of best practices and lessons learned from all CoE projects that can be reused in future CoE national and international projects, and introduce better

value/costs of new centre establishment;
- to define and pilot a business model that could be used in resource-limited member states and EU regions;
- to pilot the joint development of training programs and common international trainer groups for the selected competence areas;
- to establish cross continental/regional (USA, Latin, Asia, Africa, Australia) partnerships with other networks of similar nature;
- to create a long term partnership and collaboration model with related EU agencies.

Having mobilised the European cybercrime centres of excellence, SENTER is by definition a project with a wide European base and with ambitious European goals. From Greece to Lithuania and from Spain to Poland, national centres of excellence in cybercrime will join their activities in order to collectively improve their work: by reducing fragmentation, by avoiding duplication, by sharing experience, and by sharing resources. The collaborating centres will align their agendas, will expose and elaborate on their areas of expertise, will create a common portal, a common identity, and above all, a joint community: a community with a clear European identity so that individual centres break through the barriers of their member states to benefit from and have impact on the wider European family. The network will create joint internet groups in a few highly-focused and carefully-selected areas: network forensics, computer forensics, open source intelligence. Within these groups member states will be able to collaborate, exchange ideas, plan common activities, exchange staff and test prototypes. In this way the network will be much more than the sum of its parts: it will create expertise which would not have been created otherwise.

The network, however, will not cater only to its current members. To spread the impact to other member states, the network will establish best practices – guides for new centres of excellence being planned in countries that do not yet have such a centre, but would like to create one, and could benefit from previous experiences. The network will create the pathways that enable the expertise to roll from one member state to another and eventually to all the rest of the member states across Europe.

SENTER is a joint effort of the Mykolas Romeris University, the Lithuanian Cybercrime Centre of Excellence for Training, Research and Education (L3CE), the Ekonomines konsulatcijos ir tyrimai (EKT), the Masaryk University (MU), the Howest University, the French Cybercrime Centre of Excellence (CECyF), the Tallinn University of Technology (TTU), the University of Applied Science Albstadt-Sigmaringen (UASAS), the International Cyber Investigation Training Academy (ICI), the Foundation for Research and Technology – Hellas (FORTH), the Jožef Stefan Institute (JSI), and the States of Jersey Police.

This work is co-funded by the Internal Security Fund of the European Union. This project has been funded with support from the European Commission.

SENTER may be contacted at egidija@l3ce.eu and may be followed on twitter @senterproject.

References:

[1] Steve Morgan: "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020", Forbes/Tech Dec 20, 2015.
[2] Wall, David: "Cybercrime: The transformation of crime in the information age", Vol. 4. Polity, 2007.
[3] Canadian Underwriter: "Global annual tab for cyber crime US$445 billion, cyber insurance market forecast to grow to US$20 billion-plus by 2025: AGCS", September 9 2015, http://www.canadianunderwriter.ca/insurance/global-annual-tab-for-cyber-crime-us-445-billion-cyber-insurance-market-forecast-to-grow-to-us-20-1003793978/

Please contact:

Egidija Veršinskienė, Evaldas Bružė
Lithuanian Cybercrime Centre of Excellence for Training, Research, Development and Education (L3CE)
egidija@l3ce.eu, evaldas@l3ce.eu

Evangelos Markatos
FORTH-ICS, Greece
markatos@ics.forth.gr

A Network of Internet Probes for Fighting Cyber Attacks

by Ernő Rigó and Mihály Héder (MTA SZTAKI)

This article introduces a network of advanced internet honeypot probes for gaining situational awareness relating to cyber-attacks. The system is being built on behalf of Hun-CERT. The project is run by MTA SZTAKI and is sponsored by the Council of Hungarian Internet Providers (CHIP).

Individuals with criminal intent will attempt to gain access to any computer that is connected to the internet. Their goal may be to steal data, to gain control over the computer and use it to attack further targets, or to limit the user's access to their data to extort a ransom.

One way of attacking computers connected to the internet is by trying to break into them from the network. This is done by exploiting vulnerabilities in the operating system, additional software or their insecure configuration. Of course, not all computers have the same software and there are differences in the way they are updated and configured. A viable strategy for an attacker is, therefore, to attempt an attack on every computer that is accessible – usually by employing an automated script or attack bot. More sophisticated attackers discover the network in a less intrusive way before an attack. They even create databases of targets so when a new zero-day exploit is discovered, they can attack quickly and in a targeted fashion [1].

To discover attackers and their activity patterns, MTA SZTAKI has started to deploy honeypot probes on various subnets managed by the Hungarian ISPs. The probes are physically implemented as Raspberry Pi computers. In the future, these will be supplemented by virtualized probes – there is already an express demand for them.

The honeypot activity means that the nodes mimic the functionality of real internet services. Currently, the research is focused on implementing the SSH, SMTP and HTTP services. These facilities all run in Docker containers to maximise their isolation while maintaining a low-resource profile. Besides these sources, the firewall of the probe is able to record suspicious network activity on other network ports.

The implemented SSH facility allows attackers to gain access to the honeypot and to issue shell commands. In this way, the nature and the method of attack can be identified. The system also collects the username and password pairs that are being tried by the attackers, which can help in designing passwords that are more secure.

The goal of the SMTP functionality is to mimic a mail server. In a similar fashion to the SSH component, the attackers are allowed to issue commands that are recorded and later analysed. In the final version, the HTTP port will be able to act like a known content-management-system, like Drupal or Joomla.

The probes connect to the operations centre by establishing a VPN connection. This is how the data are collected. Each probe has a unique certificate and each is treated as a potentially hostile host by the centre. This is a safety measure for the unlikely event that a probe actually becomes hacked. The centre itself utilises Logstash, ElasticSearch and Kibana for processing, storing and analysing the logs.

Many R&D problems have been identified and overcome in this project. An important issue was the limited resources of the probe Pi hardware – the available honeypot software needed too many resources; therefore, new SSH, SMTP and HTTP honeypot components were necessary.

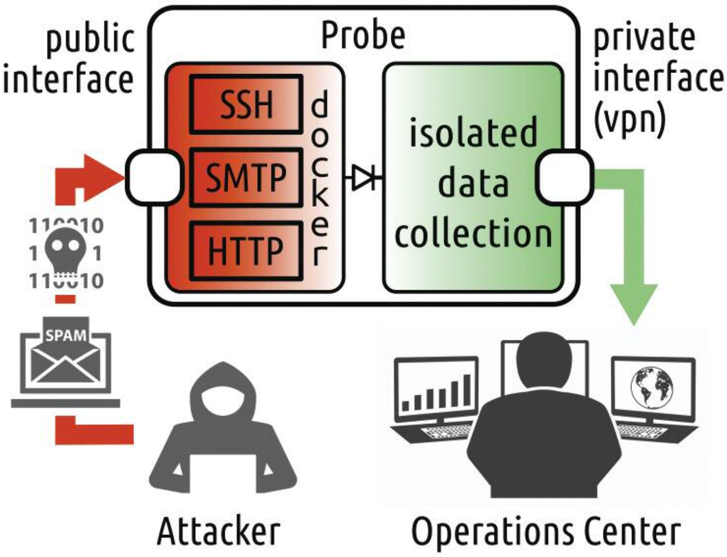


Figure 1: The role of the probe in collecting cybersecurity data.

An interesting problem is defining the actual behaviour of the honeypots in a way that the real nature and purpose of the system remain unknown to an attacker for as long as possible.
Another important research problem is that the probes must have different profiles at all levels of the network protocols, even TCP/IP. Otherwise, once an attacker has identified a probe, it could discover the rest easily. This requires advanced, kernel-level customisation of the host operating system. We handle these recurring configuration and customisation tasks with the Ansible orchestration tool.

An interesting question is the optimal number of probes on the network operated by the Hungarian ISPs. In our current batch, we have 60 probes, some of which are not yet deployed. However, we believe that the final number should be around 300 – one in each IP autonomous subnet. This estimate, of course, might change as experience is accumulated with the current probe network.

The data collected have many uses. Some aggregated information will be made available to the general public. Other more detailed information will be accessible to the ISPs that are participating in the project (currently around 80% of the Hungarian ISPs). Naturally, each ISP will access the details of their own network and only limited information about the other ISPs. Finally, all of the information will be available to Hun-CERT – allowing it to warn every ISP about potential threats and to coordinate countermeasures.

Besides human consumption, the data can be used to feed DNS-based blacklists, which everyone can use to configure their firewall, and SSH, HTTP and SMTP servers. As well, the data can be used for BGP black hole routing at the ISP level.

Reference:

[1] L. Bilge, T. Dumitras: “Before we knew it: an empirical study of zero-day attacks in the real world”, in Proc. of the ACM conference on Computer and Communications Security, 2012.

Please contact:

Ernő Rigó, Mihály Héder
MTA SZTAKI, Hungary
+36 1 279 6266, +36 1 279 6027
rigo.erno@sztaki.mta.hu,
mihaly.heder@sztaki.mta.hu

CyberWISER-Light: Supporting Cyber Risk Assessment with Automated Vulnerability Scanning

by Anže Žitnik (XLAB), Antonio Álvarez Romero (ATOS) and Stephanie Parker (TRUST-IT)

As one of the outputs of the WISER project, CyberWISER-Light provides a quick way for SMEs to make a first assessment of their cyber risk status.

Most of us rely on information and communication technologies (ICT) in our professional lives as well as private day-to-day activities. Although this brings huge benefits in many areas, we rarely think about the threats introduced by our increasing dependence on ICT. As the number of security-related cyberspace incidents continues to increase, it is important to be aware of the potential impact that incidents such as identity misappropriation, information theft or disruption of critical services can have on individuals and businesses. SMEs, representing the highest proportion of European businesses, are the most vulnerable to cybercrime. The biggest obstacle in the process of limiting the growth of cybersecurity incidents is the lack of awareness of individuals, business decision makers and even IT professionals, which leads to insufficient risk management and inadequately resilient security information systems and networks.

WISER delivers a cyber-risk management framework to assess, monitor and suggest mitigation options for cyber risks in real time, while incorporating socio-economic impact aspects, building on current state of the art methodologies and tools, and leveraging best practices from multiple industries and international initiatives. The WISER framework [L1] features cyber-risk modelling techniques [1] and monitoring tools that observe the state of ICT infrastructure and services in an organisation. These provide the information necessary to evaluate risk levels and drive decision support tools to recommend effective mitigation options based on cost-benefit analysis of the risk impact. The aim of WISER is to increase cyber risk awareness as well as make cybersecurity understandable to management personnel and facilitate their decisions about risk management and inclusion of cybersecurity systems.

CyberWISER-Light is the first product emerging from the WISER project. It is free of charge and enables self-assessment of cyber risk exposure with minimal effort and time required by the end-user. Designed with SMEs and the general public in mind, CyberWISER-Light provides a very first approach to cybersecurity to a wide variety of companies with no experience or awareness in the field. It features a questionnaire about the business and ICT profile of the company and an automatic website vulnerability scanning tool. The vulnerabilities found are put into the context of the business based on the insights the user provides in the questionnaire. The assessment result includes a general risk assessment score and a report of vulnerabilities found and suggestions for mitigation measures. The report gives a very basic yet relevant picture of a company's cybersecurity position as a step towards defining a corporate cybersecurity strategy, regardless of the size of the company.

The questionnaire consists of 28 questions and performs the assessment, which takes into account the business company profile, the internal organisation and the risk exposure of the sector it operates in, as well as the technical aspects of its ICT profile, identifying the basic measures that must be adopted to assure technical and organisational ICT Security.

The web application vulnerability scanner automatically gathers responses from the targeted website and compares them to a database of known vulnerabilities to find which vulnerabilities might be present in the web application. A vulnerability scan can be carried out from outside the company's infrastructure which means that no installation or modification of hardware or software on the premises is required. Another advantage is that vulnerability scans can be scheduled to run continuously on a time schedule or after changes in the monitored web application.

The vulnerability scanner in CyberWISER-Light is based on com-

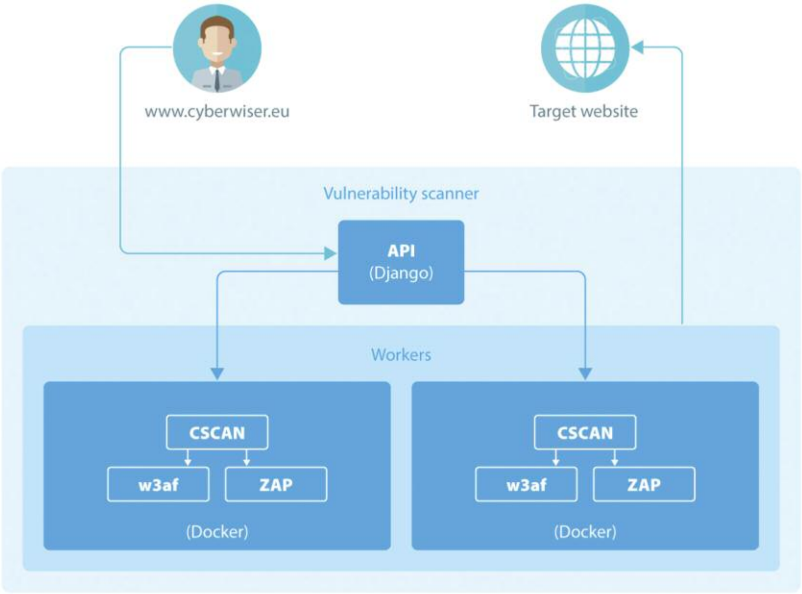


Figure 1: The vulnerability scanner solution in CyberWISER-Light.

bining results from several existing tools for vulnerability scanning, such as W3af [L2] and OWASP ZAP [L3]. These tools are running enclosed in a Docker [L4] container, which enables us to easily deploy several instances to cope with the increasing workload of the vulnerability scan requests. The architecture of our vulnerability scanning solution is presented in Figure 1. We can set up multiple Docker containers running the vulnerability scanning tools depending on the amount of vulnerability tests that need to be processed. The simple API developed in the Django framework [L4] manages task scheduling and communication with the worker programs. Our solution permits a vulnerability scan to be triggered with a single call to the API, with the option to include custom settings or use the default parameters for the vulnerability testing.

The WISER project is an Innovation Action funded by the European Union's H2020 research and innovation programme under Grant Agreement no 653321. The project started in June 2015 and brings together a multidisciplinary consortium of partners including technology providers, risk management experts, market experts and service providers for piloting. WISER partners are: Atos Spain (coordinator), Trust-IT Services Ltd (UK), Stiltefsen SINTEF (Norway), XLAB (Slovenia), AON SpA (Italy), Rexel Developpement SAS (France) and Enervalis (Belgium).

Links:
[L1] http://www.cyberwiser.eu/
[L2] http://w3af.org/
[L3] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[L4] http://www.docker.com/
[L5] https://www.djangoproject.com/

Reference:

[1] A. Refsdal, B. Solhaug, K. Stølen: "Cyber-Risk Management",. SpringerBriefs in Computer Science, 2015.

Please contact:

Anže Žitnik
XLAB d.o.o., Slovenia
+386 1 244 77 50
anze.zitnik@xlab.si

CISA: Establishing National Cyber Situational Awareness to Counter New Threats

by Florian Skopik, Maria Leitner and Timea Pahi (AIT Austrian Institute of Technology)

The final draft of the Network and Information Security (NIS) Directive stipulates that operators of essential services and digital service providers must report certain security incidents to competent authorities or national computer security incident response teams (CSIRTs) in their member state. It is the authorities' job to collect and process information about security incidents to increase network security in all organisations by issuing early warnings, assisting in mitigation actions, or distributing recommendations and best practices. However, before an appropriate response to a severe cyber situation can be undertaken, it is essential to establish cyber situational awareness – which turns out to be a tricky task.

The smooth operation of critical infrastructures, such as telecommunications or electricity supply is essential for our society. In recent years, however, operators of critical infrastructures have increasingly struggled with cybersecurity problems. Through the use of ICT standard products and the increasing network interdependencies, the attack surfaces and channels have multiplied. New approaches are required to address this serious security situation. One promising approach is the exchange of security incident information and status information of critical services across organisational boundaries with strategic partners and national authorities. The main goal is to create an extensive cyber situational awareness picture about potential threats and ongoing incidents, which is a prerequisite for an effective preparation and assistance in case of large-scale incidents.

The Challenges of Establishing Situational Awareness

Critical services, such as energy supply, transportation and banking services, are largely managed by private operators. Since these services are essential to maintaining public order and safety, it is the state's responsibility – and in the state's best interest – to guarantee the security of the related infrastructures [1]. A formal arrangement between the public and private sectors must therefore be established. Ideally, the state would directly support infrastructure providers to secure their service operations by providing them with important security information. The infrastructure providers, in turn, would provide to the state, security-relevant information, such as the status of their service or indicators of compromise in their networks. This data from every single organisation is essential to create a clear picture and cyber situational awareness of the operational environment, thus to create the basis for justified and effective decision-making by authorities at a national level.

In recent years, technical solutions for capturing network data and processing within organisations have been developed [2], and high-level security strategies have been already formulated in the national scope [3]. However, the question of how technical information from cyberspace can be processed and presented in such a cyber-situational awareness picture, is a challenging problem for which there is still no adequate solution. The objective of the project CISA (Cyber Incident Situational Awareness) is to fill this gap and create a link between the technical data and the strategic decisions required to mitigate cyber threats at national level. Cyber situational awareness (CSA) is a required capability of national stakeholders and governments to effectively perform their operations relying on the contemporary knowledge about the technical status of critical infrastructures. This situational awareness requires a holistic methodology to synthesise perception, identify and visually represent the current trends, and construct future projections.

Design Principles of the CISA Approach

The CISA approach carefully follows considered design principles to facilitate its fast adoption. The full approach is sketched in Figure 1. CISA foresees private as well as governmental stakeholders to share information with a cybersecurity centre, and covers all management and decision levels from the organisational scope to the (pan-)national scope in order to provide a holistic picture of the cyber threats in the state. Here it is important to establish an understanding of the numerous categories of relevant information, which need to be treated differently. For instance, low level technical information, such as IP addresses of command and control servers or descriptions of technical vulnerabilities, need to be modelled and shared according to different policies compared with higher-level business information, such as the potential economic impact of certain service outages. In that sense, CISA aims to adopt organisational structures and existing reporting channels (e.g., links to CSIRTs) to avoid any unnecessary overheads and lower the barriers for all stakeholders to use and support CISA. It is noteworthy that CISA respects the human-in-the-loop model. This means it attempts to support the appropriate balance between manual human-controlled activities, such as incident classification or preparation of recommendations, and automatic processes, such as intrusion detection, big data analysis etc.

The model foresees that numerous cyber situational awareness pictures are created in a cybersecurity centre – depending on the type of affected decision maker (civil, military) and the level at which the decisions need to be made (operational, tactical, strategic). These situational awareness pictures may be further enriched with external information, originating from open-source intelligence (OSINT), CSIRTs as well as closed (national, European) intelligence sources.

Eventually, recommendations to carefully selected recipient circles are issued to mitigate the effects of ongoing/recent incidents and to increase the preparedness for future ones (e.g., through distributing early warnings).

the planned system. Therefore, exercises with external stakeholders on a national scale are planned together with the competent authorities. CISA is a two-year national project running from 2015 to 2017 and is funded by the Austrian security-research program KIRAS and by the Austrian Ministry for Transport, Innovation and Technology (BMVIT).

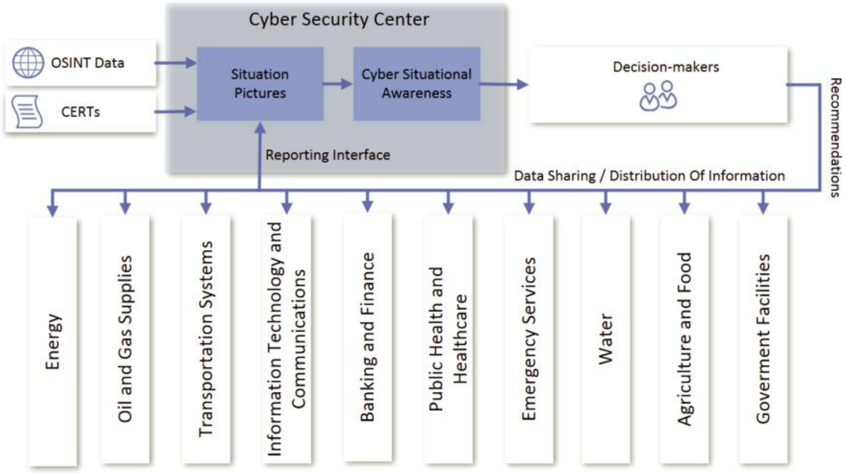


Figure 1: Approach to establishing national cyber situational awareness for competent decision makers.

The Project CISA and its Consortium

In order to attain these ambitious goals and finally ensure the wide applicability of developed tools and procedures, the project consortium consists of a vital mix of academics with deep knowledge in security (Austrian institute of Technology, SBA Research), security solution vendors and service providers (Thales Austria, T-Systems Austria), and industry practitioners (Repuco, Infraprotect). Furthermore, the involvement of legal experts (Vienna Centre for Legal Informatics (WZRI), Netelligenz e.U.) is essential to ensure compliance with regulations and the legal framework and by the employment of a data protection impact assessment and privacy enhancing technologies the necessary privacy requirements are fulfilled. Eventually a project in this area can only be successful with the active involvement and support of the competent authorities (Ministry of the Interior, Ministry of Defence and Sports, Federal Chancellery). In addition to the development of scientific methods, the proper demonstration of the applicability of CISA's results in a real-world environment is of paramount importance in order to test and evaluate

Link:
http://www.kiras.at/projects/detail/?tx_ttnews[tt_news]=535&cHash=519847e6fc040eac8cb0a6af14a1f47b&L=1

References:

[1] Network and Information Security (NIS) Directive; https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive, 15/03/2016.
[2] Leopold, H., Bleier, T., & Skopik, F.(2015) Cyber Attack Information System. Springer-Verlag Berlin Heidelberg.
[3] ENISA, National cyber Security Strategies, Practical Guide on Development and Execution, December 2012

Please contact:

Florian Skopik
AIT Austrian Institute of Technology, Austria
+43 664 8251495
florian.skopik@ait.ac.at

On Reducing Bottlenecks in Digital Forensics

by Martin Schmiedecker and Sebastian Neuner (SBA Research)

Digital rensic investigators currently face numerous challenges, some of which include: the increased digitalisation of our lives, vast case sizes owing to ever increasing storage capacity and the large number of personal devices in use. The goal of our SpeedFor project is to develop new methodologies to reduce the manual work required for digital investigators. Among other things we harvest information from file sharing networks to identify files by extending the forensic process. In an initial proof-of-concept we obtained information from the BitTorrent network to identify up to 2,500 terabytes of data.

Digital forensics has received increasing attention in recent years, as more and more crimes are conducted exclusively by, or with the involvement of, computers. Tools and methods of digital forensics are used by private investigators as well as law enforcement analysts all over the world. One of the challenges in digital forensics is the vast amount of data that needs to be analysed. Commodity hard drives with eight terabytes and more storage capacity are standard nowadays, and are readily obtained. Current forensic processes, however, do not scale well to multi-terabyte workloads. Our project SpeedFor aims to fundamentally increase the performance of current state-of-the-art forensic methods and decrease the manual work necessary for a forensic analyst by developing new methods to increase the use of parallelised data processing within the specific environment of digital forensics, and identifying the best methods to exclude a possibly vast number of files and file system artefacts that are not specific to a case.

We aim to achieve these objectives by leveraging the information specific to large file-sharing networks, in particular we use the BitTorrent protocol as source of information. Prior to sharing a set of files in the network, the data is split in to ‘chunks’ to facilitate parallel data transfers. These chunks are then hashed, and stored in the meta-information of the Torrent swarm [1]. By crawling popular torrent swarms, as well as the few remaining BitTorrent websites, the computational power of the initial seeders can be used for good i.e., a methodology to identify files and file fragments based on data from publicly available file-sharing networks.

Our prototype, dubbed peekaTorrent, will be published at the upcoming DFRWS conference. peekaTorrent is based on the open-source forensic tools bulk extractor [2] and hashdb [3], and can be readily integrated into forensic processes. It improves the current state of the art on sub-file hashing twofold: compared to previous approaches we hash sub-file parts larger than pure sector-based hashes. Figure 1 shows a graphical representation. Previously the hard drive sectors were used as input for hash functions like SHA-1, shown as the second layer on the bottom of Figure 1 for hard drives which use 512 bytes respectively 4K sectors. We propose to extract the already available data using larger hash windows which overlap with the BitTorrent specification. Our method is less prone to false-positives for files that share common data seg-

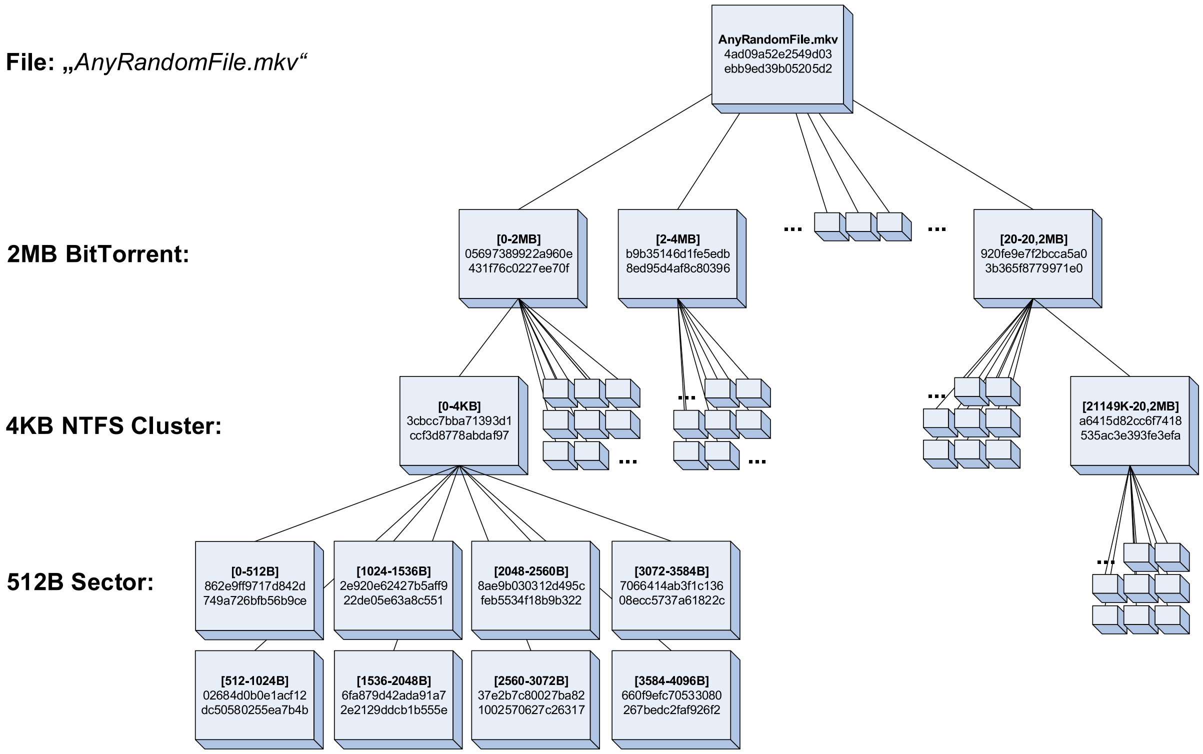


Figure 1: Sub-file hashing as used in peekaTorrent.

ments due to the larger area to be hashed.

Secondly, we solve the problem of an a-priori sub-file hash database being required by creating one that can be shared openly. We collected more than 2.5 million torrent files and built their corresponding hashdb databases, which are freely available on the project website. Note that no participation in file-sharing activity is needed as the torrent metadata or 'metainfo' already contains all the necessary information including the sub-file hash values. We publish all data sets, tools and our paper openly – you can find the source codes and the hashdb files released under open-source licence on our website https://www.peekatorrent.org. Overall, we expect these methods to help investigators around the globe as this information can be used for file and file fragment identification as well as for effective file whitelisting.

Link:
[L1] https://www.peekatorrent.org

References:

[1] Bram Cohen. The BitTorrent Protocol Specification, BEP-3, online, http://www.bittorrent.org/beps/bep_0003.html

[2] Simson L. Garfinkel: "Digital media triage with bulk data analysis and bulk_extractor", Computers & Security 32: 56-72, 2013

[3] Simson L. Garfinkel, Michael McCarrin: "Hash-based carving: Searching media for complete files and file fragments with sector hashing and hashdb", Digital Investigation 14: S95-S105, 2015.

Please contact:

Martin Schmiedecker
SBA Research, Austria
mschmiedecker@sba-research.org

Multi-View Security and Surveillance at MTA SZTAKI

by László Havasi and Tamás Szirányi (MTA SZTAKI)

The Distributed Events Analysis Research Laboratory (DEVA) has more than 10 years of research experience in security and surveillance, including multi-view systems of optical, thermal, infra-red and time-of-flight cameras, as well as LIDAR sensors. The laboratory's research and development work has been addressing critical issues of surveillance systems regarding the protection of critical infrastructures against incursions and terrorist attacks.

The DEVA laboratory has been involved in several security related projects funded by the European Commission and the European Defence Agency, contributing significant improvements regarding multi-view computer vision and target tracking efforts. During a recently finished project (PROACTIVE, EU FP-7 [L1, L2]) that included several European partners in defence and security, a holistic IoT framework was developed enabling enhanced situational awareness in urban environments in order to pre-empt and effectively respond to terrorist attacks. The framework integrates many novel technologies enabling information collection, filtering, analysis and fusion from multiple, geographically dispersed devices. At the same time, the framework integrates advanced reasoning techniques in order to intelligently process and derive high level terrorist oriented semantics from a multitude of sensor streams.

The DEVA Laboratory is responsible for processing and understanding multi-modal visual information from cameras and 3D sensors, sampled in different time instants, and situated in different locations. Special emphasis is on the fusion of different sources, such as satellite or airborne image data for remote sensing, potentially amended with terrestrial and UAV based imaging.
In our surveillance projects, an important issue is the tracking of objects/targets, and the detection and recognition of events by using multi-view camera networks, including infra-red sensors. In these applications calibration is always a problem, since security scenarios usually require quick installation and continuous troubleshooting. Another challenge is the co-registration of optical cameras and infra sensors for 3D tracking, since features of different modalities are usually hard to associate and compare.

In a recently finished project (PROACTIVE, EU FP-7) that included several European partners in defence and security, our main task was the visual tracking and analysis of human and vehicle behaviour [1] and crowd events.

The project addressed some specific emergency situations involving man-made or natural disasters and terrorism, i.e., frequent threats within our society. Avoiding an incident and mitigating its potential consequences requires the development and deployment of new solutions that exploit the recent advances in terms of technological platforms and problem solving strategies.

PROACTIVE produced an end-user driven solution. PROACTIVE prototypes include the following parts:

- *Terrorist Reasoning Kernel:* the reasoning layer provides the needed intelligence in order to infer additional information regarding the incoming suspicious event stream. This layer aids law enforcement officers by reasoning about threat levels of each incoming event and potentially inferring its association with a possible terrorist attack.
- *Context Awareness Kernel:* these processing modules provide semantic description about the environment and the static and moving (e.g., foreground) objects and sufficient information about the suspicious events and actions.
- *C2 platform:* the command and control platform is a multi-touch and multi-user web-application that provides a graphical user interface and enables the user to view maps (2D/3D), devices/sensors and alerts from the system.

The capabilities of Context Awareness Kernel could be demonstrated with different scenarios including the showcasing of the advantages of a multispectral sensor network:

Monitoring activities in crowded scenes

Analysing the dynamic parameters of motion trajectories and sending signals when ‘running’ movements are detected [L3]. Running pedestrians can also find a place to hide and observe the area. Crowd density estimation provides information for the definition of a top view mask image where the crowd density might cause errors during tracking. Alarms are generated when the average detected speed is higher than 2 m/s, and the detected object and its trajectory are highlighted with red (Figures 1 and 2).

Monitoring the parking area

In this scenario the objective was to validate the waiting/parking time durations in different areas (including where parking is prohibited). Object interactions were also investigated: the vehicle and driver connections were continuously checked and alarms were raised when possibly suspicious loitering movements were detected.
To measure the parking duration, the behaviour analyser module followed the state changes/transitions and associated timestamps while the tracking method remained stable. In the following figure the parking car in the restricted area and the loitering human are marked with red (Figure 3).

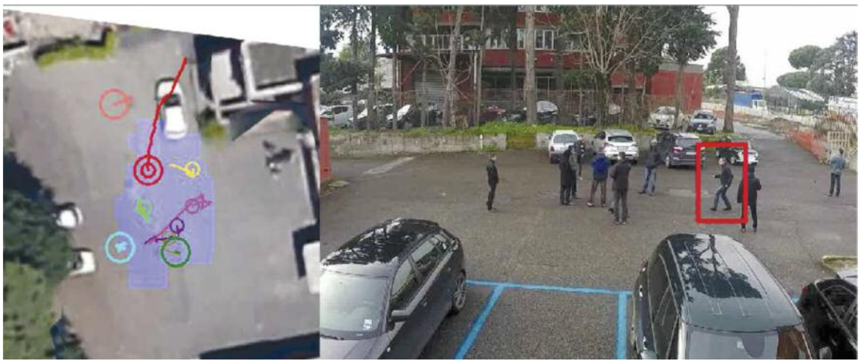


Figure 1: Feature level fusion of multispectral (EO, IR) views which highlights mismatches and ‘invisible’ human shapes.

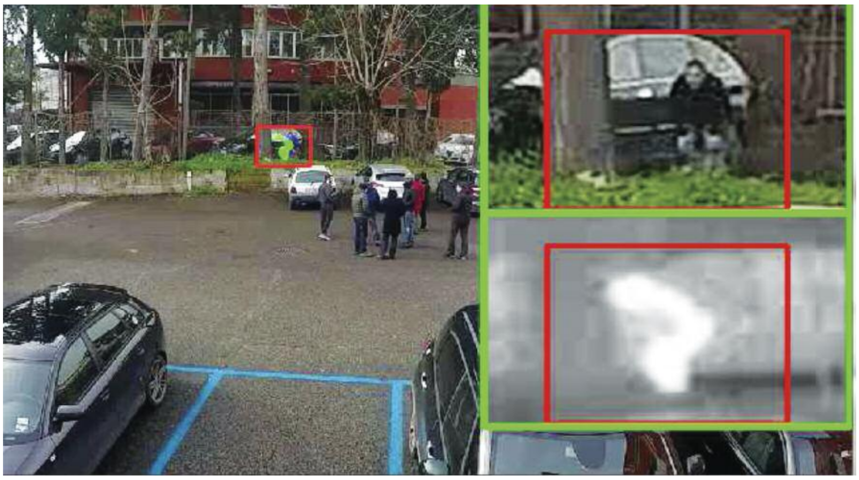


Figure 2: In this example, the general sensor configuration contained four cameras with overlapping fields of view.

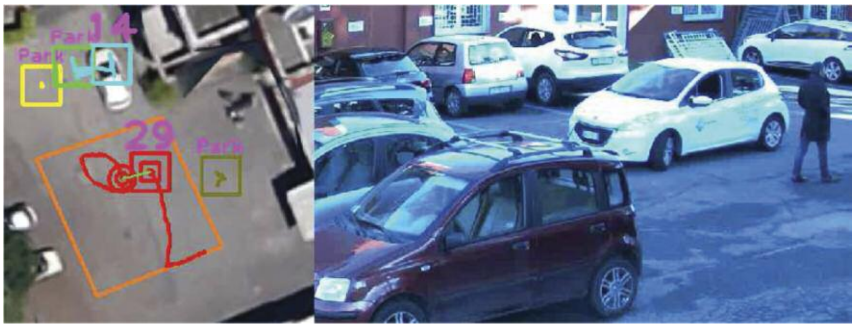


Figure 3: The sensor configuration was comprised of three cameras.

As a continuation of the project, we are working on augmenting terrestrial camera networks with airborne (UAV) and satellite (Sentinel-2) information to get up-to-date and full surveyed area scans of critical infrastructures.

Links:
[L1] http://web.eee.sztaki.hu/home4/node/36
[L2] http://cordis.europa.eu/project/rcn/103500_en.html
[L3] http://link.springer.com/article/10.1007%2Fs12652-016-0369-0

Reference:

[1] D. Varga et al.: “A multi-view pedestrian tracking method in an uncalibrated camera network”, IEEE International Conference on Computer Vision Workshops, Santiago de Chile, 2015.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7406382

Please contact:

Tamas Sziranyi
MTA SZTAKI, Hungary
sziranyi@sztaki.mta.hu

IT Security meets Austrian history – CCS 2016
© Hofburg Vienna
© Hofburg Vienna, Foto Manfred Seidl

23rd ACM Conference on Computer and Communications Security first time in Vienna (second time in Europe since 2000)!

24 – 28 October 2016, Hofburg Palace, Vienna, Austria

Program outline

- **Presentation of about 160 top scientific papers (selected out of 800+ submissions)**
- **Scientific / industrial tutorials and invited industrial speakers (industrial track)**
- **Panel discussions with representatives of science, industry and politics**
- **Several workshops co-located with CCS 2016**

Keynote Speakers

Martin Hellman (ACM Turing Award Winner 2015) **Ross Anderson (University of Cambridge)**

More information: https://www.sigsac.org/ccs/CCS2016/

hosted by SBA Research

Call for Participation

STM 2016 – 12th International Workshop on Security and Trust Management

Heraklion, Crete, Greece, 26-27 September 2016

Security and Trust Management (STM) is a Working Group of ERCIM. STM 2016 is the eleventh workshop in this series and will be held in Heraklion, Crete, Greece, on September 26-27, in conjunction with the 21st European Symposium on Research in Computer Security (ESORICS 2016).

The workshop will present papers from academia, industry, and government presenting novel research on all theoretical and practical aspects of security and trust in ICTs. Topics include:

- Access control
- Anonymity
- Applied cryptography
- Authentication
- Complex systems security
- Data and application security
- Data protection
- Data/system integrity
- Digital rights management
- Economics of security and privacy
- Formal methods for security and trust
- Identity management
- Legal and ethical issues
- Mobile security
- Networked systems security
- Operating systems security
- Privacy
- Security and trust for big data
  Trust models
- Security and trust in cloud environments
- Security and trust in content delivery networks
- Security and trust in crowdsourcing
  Trusted platforms
- Security and trust in grid computing
- Security and trust in the Internet of Things
- Security and trust in pervasive computing
- Security and trust in services
- Security and trust in social networks
- Security and trust management architectures
- Security and trust metrics
  Social implications of security and trust
- Security and trust policies
- Trust assessment and negotiation
- Trust in mobile code
- Trust management policies
- Trust and reputation systems
- Trustworthy systems and user devices.

More information:
http://stm2016.ics.forth.gr/

European Research and Innovation

High-Density Data Storage in Phase-Change Memory

by Haralampos Pozidis, Nikolaos Papandreou, Thomas Mittelholzer, Evangelos Eleftheriou (IBM Research Zurich)

We are entering into an exciting era for data storage and memory, and as a consequence, computing as a whole. Next-generation, revolutionary memory technologies are at the advanced development stage in semiconductor fabs around the world and promise to enable new applications in the near future.

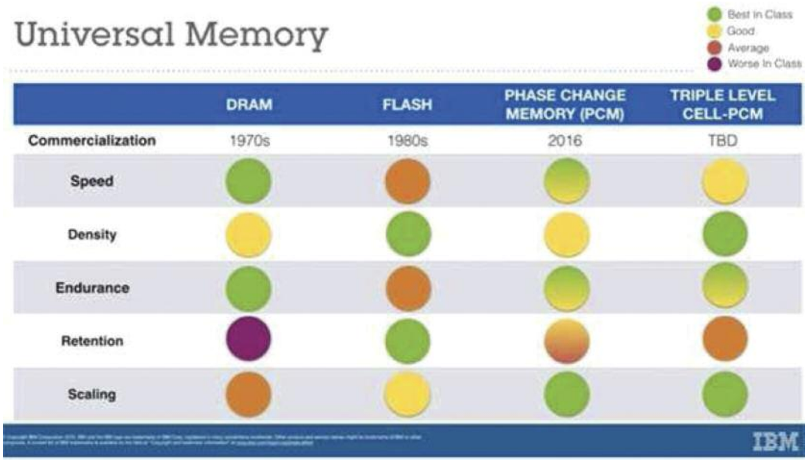
Memory and storage technologies have always been at the core of information technology and have enabled huge leaps in the efficiency, performance and usability of computing systems. Two of the most prominent examples are DRAM (dynamic random access memory) and Flash memory, both of which revolutionized the way computers interact with and process data. In the past several decades both DRAM and Flash have been riding the exponential growth curve offered by the continuous reduction of the semiconductor technology node, fueled by steady advances in lithography. However, lately, both technologies have been experiencing a scaling slow-down. DRAM devices with 8Gbit die capacity have only recently been announced, whereas for NAND Flash the lateral scaling has stopped at the 15nm node and exploration of three-dimensional stacking has begun in order to maintain density growth.

In the quest for high memory density, low latency and storage-like cost, all major semiconductor manufacturers have invested in the research and development of new materials and devices with better scalability prospects than conventional ones. As a result of these efforts, in the past decade or so, we have witnessed the emergence of several new memory technologies. The exciting new prospect of most of these memories is that they exhibit “universal” properties, i.e., properties akin to both main memory and storage. On one hand, these memories can be written and read fast, have very high write endurance, can be written in place and have byte-level granularity, making them suitable for main memory applications. On the other hand, they are nonvolatile and can be manufactured at very high density, which are typical characteristics of mass storage devices.

The promise of universal memories lies not only on their superior scalability potential, but also on the prospect of enabling a whole new set of applications that are rapidly emerging in the fields of databases, analytics processing and big data in general. This is mainly because of the possibility of offering memory devices with very large storage capacity, and latency close or similar to that of DRAM. Such a capability could enable such tasks as keeping entire databases in memory and processing queries in real time, without the need for complex cache hierarchies and cache management policies. Similarly, analytics on very large datasets could also be run considerably faster, without the performance penalties associated with disk or Flash accesses.

One of the prominent universal memory technologies is the so-called phase-change memory (PCM). PCM is based on chalcogenide alloys, i.e., alloys containing elements of group VI of the periodic table (such as Se or Te), typically combined with group IV/V elements (such as Ge, Sn, As, Sb). These materials exist in two phases, a highly conductive, poly-crystalline state and a highly resistive, amorphous state. Transition between the two phases is achieved by heating the material using electrical pulses in a nanoscale memory cell consisting of a phase change material placed between two electrodes. The two material phases exhibit drastically different electrical resistance and can be used to store 1 bit of information (logical 0 or 1).

A key requirement for PCM (or any other universal memory) to become competitive with incumbent memories and to eventually enter the market is the cost per bit of the technology, which needs to be at least lower than that of DRAM. One common way to reduce the cost per bit is to increase the memory density by storing multiple (more than one) bits per physical cell. One big advantage of PCM is that it is, in principle, highly amenable to multi-bit storage, because of the large (typically 3-4 orders of magnitude) resistivity contrast between its two extreme phases. A relative comparison of



Universal Memory

🟢 Best in Class
🟡 Good
🟠 Average
🟣 Worse in Class

	DRAM	FLASH	PHASE CHANGE MEMORY (PCM)	TRIPLE LEVEL CELL-PCM
Commercialization	1970s	1980s	2016	TBD
Speed	🟢	🟠	🟢🟡	🟡
Density	🟡	🟢	🟡	🟢
Endurance	🟢	🟠	🟢🟡	🟢🟡
Retention	🟣	🟢	🟡🟠	🟠
Scaling	🟠	🟡	🟢	🟢

Figure 1: Relative comparison of memory technologies in terms of main characteristics.

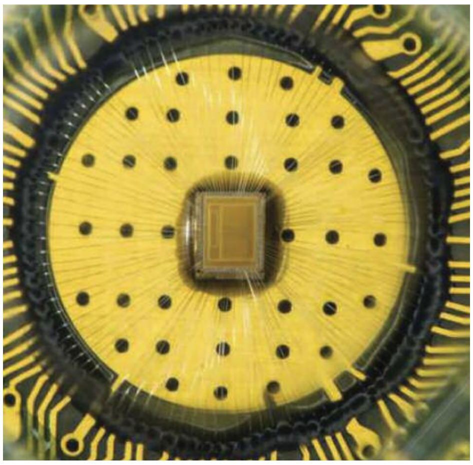


Figure 2: Close-up picture of a phase-change memory chip used in the 3bits/cell demonstration.

existing memory technologies with PCM is shown in Figure 1.

Multi-bit storage in PCM is achieved by forming intermediate states which represent different degrees of partial crystallization within the phase change material volume. However, a number of reliability issues hamper the realization of multiple bits per cell in PCM devices. In particular, two of the predominant issues are the instability of the electrical conductivity of the material with time elapsed after programming (resistance drift) and the sensitivity of the stored states to ambient temperature variations. Both of these phenomena are exacerbated by increasing the number of bits stored in a cell, because the signal margin between adjacent states is then reduced.

Our work at IBM Research – Zurich has been focused on finding effective solutions to the above problems and thus enabling reliable multi-bit storage in PCM. Specifically, we have developed three key technologies for that purpose. The first is a novel metric that is used to read the information stored in a PCM cell that is almost invariant to resistance drift, i.e., exhibits significant stability over time. Conceptually, this new metric measures a quantity akin to the proportion of amorphous phase material within the volume of the PCM cell, which is stable over time in contrast to the electrical resistance that is varying. The second technique is a signal processing scheme that adapts the level detection thresholds placed between signal states in such a way as to always guarantee the best possible distinction between adjacent states, despite any resistance variations due to drift or temperature changes. Last, but not least, a novel coding scheme shapes the data stored in the PCM cells so that information is stored not on the actual signal levels, but on their relative order within a collection of cells, called a codeword.

The judicious combination of the above three innovations has been instrumental in addressing all the major reliability concerns in multi-bit PCM. In particular, we have been able to demonstrate, for the first time, highly reliable data storage at 3bits/cell density in an array of 64 kcells that have been pre-written 1 million times [1] (Fig. 2). Furthermore, we demonstrated successful retention of the stored data over a period of 10 days in the presence of ambient temperature variations between 25 and 75 degrees Celsius. These results help establish the practical viability of multi-bit PCM, which has always been considered a difficult problem, and pave the way for truly competitive PCM products with new promising applications.

Our current work centers around the exploitation of PCM technology in future computing systems, in particular storage systems and servers. As a first step, in collaboration with the University of Patras, in Greece, we have developed a phase-change memory (PCM) sub-system attached to the POWER8® processor via the Coherent Accelerator Processor Interface (CAPI). The POWER8® processor architecture with its CAPI interface provides an efficient communication mechanism to PCM over the PCI Express link. In a platform comprising a POWER8® server, an FPGA card and custom DIMMs made of legacy 128 Mb PCM chips, we demonstrated 128-byte accesses from/to PCM at consistently very low latency, namely up to 3.1 µs and 8.8 µs for 99% of the write and read operations, respectively. These results were recently presented at the 2nd OpenPOWER Summit [2] and demonstrate the potential of using PCM as a fast storage tier directly attached to the processor through an I/O link.

IBM and POWER8 are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product or service names may be trademarks or service marks of IBM or other companies.

Link:
http://www.research.ibm.com/labs/zurich/sto/memory/

References:

[1] M. Stanisavljevic, et al.: "IEEE Intl. Memory Workshop", Paris, May 2016.
[2] http://openpowerfoundation.org/presentations/low-latency-access-to-phase-change-memory-in-openpower-systems/

Please contact:

Haralampos Pozidis, IBM Research Zurich, Switzerland
hap@zurich.ibm.com

CAxMan: Design for Additive Manufacturing Made Easy and Cost-effective

by Giulia Barbagelata (STAM), Marco Attene (CNR-IMATI) and Tor Dokken (SINTEF)

CAxMan will establish novel workflows and services for discrete manufacturing (combinations of additive and subtractive), by showcasing the CAx-technologies as cloud-based services and workflows, from design to production of physical prototypes.

High-tech software for engineers is expensive – often too expensive for small and medium-sized enterprises (SMEs) to use regularly. In the EU project CAxMan (Computer Aided Technologies for Additive Manufacturing) researchers are developing special cloud enabled design and simulation solutions addressing additive manufacturing (AM) and targeting the needs of SMEs. AM is a technology that builds 3D objects by adding layer-upon-layer of material, contrary to subtractive manufacturing by which 3D objects are constructed by cutting excess away from a solid block of material.

An engineer's most important tool is a computer: be it a bridge, a car or a lawn mower, every product these days is designed on a computer. Its suitability for purpose is often tested through computer simulations well prior to the first prototype; at least in theory. This is actually the case for subtractive manufacturing. For AM, dedicated tools for computer aided technologies (CAx) are fragmented, and in many important aspects rudimentary or completely lacking.

It is the mission of the thirteen CAxMan partner institutions (covering seven EU countries and including research, IT-industry, service providers and manufacturing industries) to form an innovative and world class team to improve this situation.

The idea is to develop new design and simulation technologies addressing the specificities of additive manufacturing and to make them available as cloud services, exploiting the infrastructure of the FP7 project CloudFlow [L1].

The cloud infrastructure will make it easy for both small and large enterprises to access these new technologies. Expensive specialised software will no longer be installed on the engineer's computers, but will run via internet on the cloud. On this open platform, products may be designed and simulated. The available servers provide high performance computing (HPC) solutions, capable of solving very complex problems.

The project will establish novel workflows and services for additive and subtractive manufacturing by addressing analysis/simulation-based design, analysis/simulation of process planning, and showcasing the CAx technologies for two use cases:

- Use Case 1: NUGEAR is an example of a product that is too expensive to produce by subtractive manufacturing alone, where additive manufacturing is used to create tailored workpieces to reduce the use of subtractive manufacturing to attain the required surface quality. The NUGEAR (NUtating GEARbox) is an innovative gearbox that couples the mathematical concept of nutation with bevel gears [1]. The main bottleneck of NUGEAR's manufacturing is the production of internal bevel gears (bevel gears whose pitch cone angle is larger than 90°), which are needed in the nutating gearbox.
- Use Case 2: Injection moulds as an example of a product that incorporates functional cavities into a single component, where production by subtractive manufacturing would require multiple components. One of the biggest and most complex constraints is the thermal regulation of the mould: poor thermal regulation can result in a bad plastic part with a lot of defects. Therefore, cavities are used as cooling channels, which must be properly

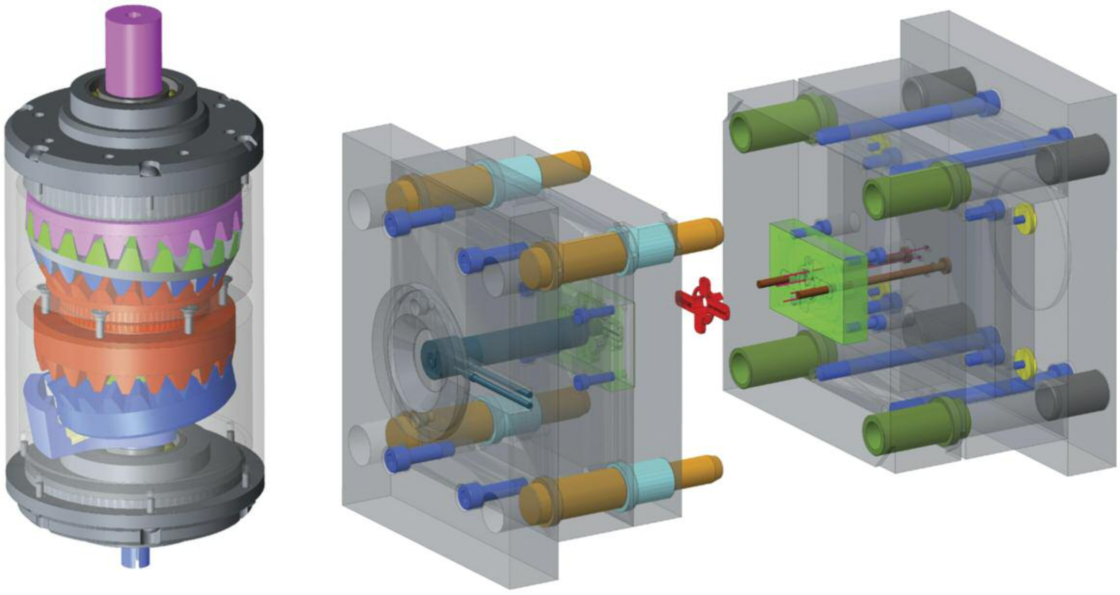


Figure 1: The two use case demonstrators that will be used to assess CAxMan developments: the NUGEAR (left) and an Injection Mould (right).

designed and pose serious constraints due to the subtractive manufacturing.

In principle the layer-by-layer approach of additive manufacturing makes it possible to build components of any level of complexity. However, in practice, the situation is more complicated: support structures have to be added to avoid errors in material deposition, the part has to be oriented in order to obtain suitable surface finish, physical limitations and constraints have to be taken into consideration as well as the actual behaviour of the material during the process, etc. As most 3D printing today is based on STL-files, interoperability with design is currently poor.

In CAxMan a feedback loop will be established between design and process planning for additive manufacturing. The process planning starts by analysing the design and, after having specified the process to be used, a process plan is generated. This will provide requests for revision to the design phase before passing the process plan on to manufacturing and ensuring that the final manufactured object is as close to the design as possible. Such interoperability will significantly shorten the lead time and will enable the development of much more flexible and effective design environments for additive manufacturing applications.

The objectives of CAxMan are to establish cloud based toolboxes, workflows and a one stop-shop for CAx-technologies supporting the design, simulation and process planning for additive manufacturing. The analysis-based design approaches will make it possible:
- To reduce material usage through internal cavities and voids, maintaining component properties;
- To optimise distribution and grading for multi-material processes;
- To facilitate the manufacture of components which are currently very difficult to produce by subtractive processes;
- To enhance analysis-based process planning for additive manufacturing including thermal and stress aspects, and their interoperability with the design phase;
- To enable the compatibility of additive and subtractive processes in production.

Unlike current CAD/CAE/CAM tools, CAxMan will guarantee unpreceded interoperability among product development steps, will focus on cost effectiveness and will be developed expressly for AM.

In conclusion, the CAxMan set of CAD/CAE/CAM tools will speed up and improve the design/engineering/manufacture process and optimise the AM process, for the benefit of designers, engineers and manufacturers of mechanical products who want to get the best out of AM and reduce production costs.

CAxMan has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 68044.

Link:
[L1] http://www.eu-cloudflow.eu

Reference:

[1] P. Fanghella, L. Bruzzone, S. Ellero and R. Landò: “Kinematics, Efficiency and Dynamic Balancing of a Planetary Gear Train based on Nutating Bevel Gears”, Mechanics Based Design of Structures and Machines: an International Journal, vol. 44, Issue 1-2, 2016.

Please contact:

Giulia Barbagelata, Stam S.r.l., Italy
g.barbagelata@stamtech.com

Marco Attene, CNR-IMATI, Italy
marco.attene@ge.imati.cnr.it

Tor Dokken, SINTEF, Norway
tor.dokken@sintef.no

ERCIM “Alain Bensoussan” Fellowship Programme

ERCIM offers fellowships for PhD holders from all over the world. Topics cover most disciplines in Computer Science, Information Technology, and Applied Mathematics. Fellowships are of 12-month duration, spent in one ERCIM member institute. Fellowships are proposed according to the needs of the member institutes and the available funding.

In the current round (30 April deadline), 25 fellowships were granted.

Application deadlines for the next round: 30 September 2016

More information: http://fellowship.ercim.eu/

ERCIM Programme for PhD Education

The ERCIM Programme for PhD Education (EPPE) is a new mobility programme for cooperation in PhD education among ERCIM members. The goal is to add a European international dimension to PhD education by crossing national, scientific and institutional borders.

With experience from the successful ERCIM postdoctoral Fellowship Programme, the EPPE reduces administrative and formal obstacles for PhD students, supervisors and institutions when establishing cooperation.

Objectives

- Improve the quality of PhD education.
- Exploit complementary qualities of institutes and universities.
- Facilitate research cooperation among institutions and candidates.
- Disseminate research results from EU funded research.
- Make ERCIM institutions more attractive in recruiting good candidates.

Principles

- The EPPE provides added value to programmes already run by ERCIM members. Participation is on voluntary basis. .
- The cooperation can result in a single or a double degree.
- Candidates have a Home Institution and a Host Institution.
- ERCIM provides templates for cooperation agreements dealing with scientific supervision, costs, IPR, evaluation, and other matters.
- The programme is efficiently operated and simple to use. It provides a safe and legal platform. The rules, documents and information system permits supervisors and students to easily establish a cooperation.
- Through the ERCIM, members can raise awareness of their PhD programs and call for candidates, and the students will benefit from enhanced visiblity of their theses work.

How it works in practice

A set of contract templates and guidelines is available for members on request.

Please contact:
Emma Lière, ERCIM Office
+33 4 9238 7574
emma.liere@ercim.eu

W3C Web & Virtual Reality Workshop

Mountain View, CA, USA,
19-20 October 2016

Improvements in hardware and software capabilities have resulted in a renewed interest in virtual reality experiences. Many of these improved capabilities are available in modern browsers via the Open Web Platform, and thus make the Web a promising ecosystem to create, distribute and enjoy virtual reality applications and services.

W3C is organizing a workshop to look at the intersection of Web and Virtual Reality technologies. The workshop aims at sharing experiences between practitioners in the field, discuss existing gaps in the Web platform that make some Virtual Reality use cases difficult or impossible in browsers today, and explore which future standards are needed to pave the way for the Web to be one of the major VR platforms.

The event is hosted by Samsung. People internested in participation can submit a statement or expression of interest until 16 September 2016.

Link:
https://www.w3.org/2016/06/vr-workshop/

ERCIM Membership

After having successfully grown to become one of the most recognized ICT Societies in Europe, ERCIM has opened membership to multiple member institutes per country. By joining ERCIM, your research institution or university can directly participate in ERCIM's activities and contribute to the ERCIM members' common objectives to play a leading role in Information and Communication Technology in Europe:

- Building a Europe-wide, open network of centres of excellence in ICT and Applied Mathematics;
- Excelling in research and acting as a bridge for ICT applications;
- Being internationally recognised both as a major representative organisation in its field and as a portal giving access to all relevant ICT research groups in Europe;
- Liaising with other international organisations in its field;
- Promoting cooperation in research, technology transfer, innovation and training.

About ERCIM

ERCIM – the European Research Consortium for Informatics and Mathematics – aims to foster collaborative work within the European research community and to increase cooperation with European industry. Founded in 1998, ERCIM currently includes 21 leading research establishments from 18 European countries. Encompassing over 10 000 researchers and engineers, ERCIM is able to undertake consultancy, development and educational projects on any subject related to its field of activity.

ERCIM members are centres of excellence across Europe. ERCIM is internationally recognized as a major representative organization in its field. ERCIM provides access to all major Information Communication Technology research groups in Europe and has established an extensive program in the fields of science, strategy, human capital and outreach. ERCIM publishes ERCIM News, a quarterly high quality magazine and delivers annually the Cor Baayen Award to outstanding young researchers in computer science or applied mathematics. ERCIM also hosts the European branch of the World Wide Web Consortium (W3C).

> **“Through a long history of successful research collaborations in projects and working groups and a highly-selective mobility programme, ERCIM has managed to become the premier network of ICT research institutions in Europe. ERCIM has a consistent presence in European Community funded research programmes conducting and promoting high-end research with European and global impact. It has a strong position in advising at the research policy level and contributes significantly to the shaping of EC framework programmes. ERCIM provides a unique pool of research resources within Europe fostering both the career development of young researchers and the synergies among established groups. Membership is a privilege.”**
>
> ***Dimitris Plexousakis, ICS-FORTH***

Benefits of Membership

Institutions, as members of ERCIM AISBL, benefit from:

- International recognition as a leading centre for ICT R&D. ERCIM, a European-wide network of centres of excellence in ICT, is internationally recognised as a major representative organisation in its field;
- More influence on European and national government R&D strategy in ICT. ERCIM members team up to speak with a common voice and produce strategic reports to shape the European research agenda;
- Privileged access to standardisation bodies, such as the W3C which is hosted by ERCIM as to other bodies with which ERCIM has also established strategic cooperation. These include ETSI, the European Mathematical Society and Informatics Europe;
- Invitations to join projects of strategic importance;
- Establishing personal contacts among executives of leading European research institutes during the bi-annual ERCIM meetings;
- Invitations to join committees and boards developing ICT strategy nationally and internationally;
- Excellent networking possibilities with more than 10.000 high-quality research colleagues across Europe. ERCIM’s mobility activities, such as the fellowship programme, leverages scientific cooperation and excellence;
- Professional development of staff including international recognition;
- Publicity through the ERCIM website and ERCIM News, the widely read quarterly magazine.

How to Become a Member

- Prospective members must be outstanding research institutions (including universities) within their country;
- Applicants shall address a request accompanied by short description to the ERCIM Office. The description must contain:
  - Name and address of the institute;
  - Short description of the institute’s activities;
  - Staff (full time equivalent) relevant to ERCIM’s fields of activity;
  - Number of European projects currently involved in;
  - Name of the representative and the alternate.
- Membership applications will be reviewed by an internal board and may include an on-site visit;
- The decision on admission of new members is made by the General Assembly of the Association, in accordance with the procedure defined in the Bylaws (http://kwz.me/U7), and notified in writing by the Secretary to the applicant;
- Admission becomes effective upon payment of the appropriate membership fee in each year of membership;
- Membership is renewable as long as the criteria for excellence in research and an active participation in the ERCIM community, cooperating for excellence, are met.

Interested in joining ERCIM?
Please contact:

ERCIM Office
2004 route des Lucioles, BP 93
06902 Sophia Antipolis Cedex
Tel: +33 4 92 38 50 10
Email: contact@ercim.eu
http://www.ercim.eu

ERCIM
European Research Consortium
for Informatics and Mathematics

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

Consiglio Nazionale delle Ricerche
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1, 56124 Pisa, Italy
http://www.iit.cnr.it/

Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
http://www.cwi.nl/

Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
http://www.fnr.lu/

FWO
Egmontstraat 5
B-1000 Brussels, Belgium
http://www.fwo.be/

F.R.S.-FNRS
rue d'Egmont 5
B-1000 Brussels, Belgium
http://www.fnrs.be/

Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
http://www.ics.forth.gr/

Fraunhofer ICT Group
Anna-Louisa-Karsch-Str. 2
10178 Berlin, Germany
http://www.iuk.fraunhofer.de/

INESC
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal

Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
http://www.inria.fr/

I.S.I. – Industrial Systems Institute
Patras Science Park building
Platani, Patras, Greece, GR-26504
http://www.isi.gr/

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
http://www.sba-research.org/

SICS Swedish ICT
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

Spanish Research Consortium for Informatics and Mathematics
D3301, Facultad de Informática, Universidad Politécnica de Madrid
28660 Boadilla del Monte, Madrid, Spain,
http://www.sparcim.es/

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
http://www.sztaki.hu/

University of Cyprus
P.O. Box 20537
1678 Nicosia, Cyprus
http://www.cs.ucy.ac.cy/

University of Southampton
University Road
Southampton SO17 1BJ, United Kingdom
http://www.southampton.ac.uk/

Universty of Warsaw
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warsaw, Poland
http://www.mimuw.edu.pl/

Universty of Wroclaw
Institute of Computer Science
Joliot-Curie 15, 50–383 Wroclaw, Poland
http://www.ii.uni.wroc.pl/

VTT Technical Research Centre of Finland Ltd
PO Box 1000
FIN-02044 VTT, Finland
http://www.vttresearch.com

Subscribe to ERCIM News and order back copies at http://ercim-news.ercim.eu/