TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing

Hubert Ritzdorf*, Karl Wüst*, Arthur Gervais†, Guillaume Felley‡, Srdjan Čapkun*
* Department of Computer Science, ETH Zurich, firstname.lastname@inf.ethz.ch
† Imperial College London, a.gervais@imperial.ac.uk
‡ Department of Computer Science, ETH Zurich, gfelley@student.ethz.ch

***Abstract*—An internet user wanting to share observed content is typically restricted to primitive techniques such as screenshots, web caches or share button-like solutions. These acclaimed proofs, however, are either trivial to falsify or require trust in centralized entities (e.g., search engine caches). This motivates the need for a seamless and standardized internet-wide non-repudiation mechanism, allowing users to share data from news sources, social websites or financial data feeds in a provably secure manner.**

Additionally, blockchain oracles that enable data-rich smart contracts typically rely on a trusted third party (e.g., TLSNotary or Intel SGX). A decentralized method to transfer web-based content into a permissionless blockchain without additional trusted third party would allow for smart contract applications to flourish.

In this work, we present TLS-N, the first TLS extension that provides secure non-repudiation and solves both of the mentioned challenges. TLS-N generates non-interactive proofs about the content of a TLS session that can be efficiently verified by third parties and blockchain based smart contracts. As such, TLS-N increases the accountability for content provided on the web and enables a practical and decentralized blockchain oracle for web content. TLS-N is compatible with TLS 1.3 and adds a minor overhead to a typical TLS session. When a proof is generated, parts of the TLS session (e.g., passwords, cookies) can be hidden for privacy reasons, while the remaining content can be verified.

I. Introduction

The overwhelming adoption of TLS [43] for most HTTP traffic has transformed the web into a more confidential and integrity protected communication platform. Despite TLS's adoption, an efficient, secure, privacy-preserving, non-interactive and seamless method to prove communication contents to a third party — i.e. a *standardized method for non-repudiation* — that does not require an additional trusted party is missing.

Such a non-repudiation solution and its proofs would allow more accountability in the web and aid the construction of decentralized blockchain oracles as we outline in the following.

Network and Distributed Systems Security (NDSS) Symposium 2018
18-21 February 2018, San Diego, CA, USA
ISBN 1-891562-49-5
http://dx.doi.org/10.14722/ndss.2018.23272
www.ndss-symposium.org

Interestingly, users are currently unable to prove to a third party the content they have observed on a particular website. One of the most popular methods for users to document and share content they watch on the Internet are *screenshots* that are trivial to falsify [21], [31]. A non-repudiation solution would remove the necessary trust towards a user that claims to have observed a given content. Further, currently trusted third parties, such as search engine caches or web archives could add non-repudiable proofs about the content they have observed and thus increase their credibility.

Furthermore, blockchain-based smart contracts [44] can significantly benefit from an efficient non-repudiation solution. If for example a stock market price API provides non-repudiable data, any user could submit verifiably valid stock price information to the blockchain (effectively creating a decentralized blockchain oracle). Because the blockchain-based smart contract verifies the validity of the provided data, peers would only need to trust the data provider, not the peers that actually transmit the data to the blockchain. Generally, this would allow to seamlessly connect real world events with a blockchain and as such enable new application scenarios for smart contracts. Note that existing blockchain oracles either rely on deprecated security protocols (e.g., TLS 1.1 for TLSNotary [42]) or introduce additional trusted third parties (e.g., TLSNotary and Intel SGX).

In this paper, we propose TLS-N, an extension of TLS that enables the seamless integration of non-repudiation between arbitrary parties within TLS. TLS-N allows the generation of privacy-preserving, non-repudiable, non-interactive proofs of the contents of a TLS session. Our solution takes into account the performance requirements of TLS, both in computation and memory to promote adoption and reduce the potential attack surface (e.g. against Denial-of-Service attacks). Our design supports various proof types, that can be shared with other parties, allowing them to verify the conversation contents.

The proof verification requires no additional security assumptions other than those of TLS, and we do not need an additional trusted third party. Furthermore, the security of TLS-protected content can be partially preserved using privacy protection. Privacy-protected content inside the proof is protected from dictionary attacks due to (undisclosed) salts with sufficiently high entropy. Salts for private content remain secret while other salts are included in the proof for verifiability. Note that any non-repudiation solution based on a higher layer (e.g., HTTP), would either require access to the long-term cryptographic TLS keys from the higher layer, violating the layer principle, or would require the deployment and

authentication of additional key material, thereby significantly increasing the complexity of the solution.

In TLS-N, by the definition of non-repudiation, message authentication and the identification of at least one TLS peer is guaranteed. We compare TLS-N to existing non-repudiation proposals and identify properties that non-repudiation solutions must possess for particular use cases.

We implement and evaluate TLS-N as an extension of the new TLS 1.3 standard. As such, we implement a TLS-N-enabled web server, web client, an Ethereum-based library for proof parsing and verification and finally an Ethereum-based oracle that uses TLS-N proofs. We also deploy the oracle inside the public Ethereum test network. The implementation details, the code and contract addresses can be found at https://tls-n.org, which itself has TLS-N enabled. Furthermore, users can use the website to generate and verify TLS-N proofs.

We find that our prototype implementation incurs an overhead of less than 1.5 milliseconds on existing TLS connections per HTTP request for responses of 10 KB or less, which is a realistic size for an API response. Verifying our proof examples in a smart contract costs between 0.5 and 8 USD due to the currently high gas price[1]. Prices depend on the proof size and signature type. Note that, once this proof is verified, it can be used by millions of blockchain users.

As a summary our contributions are as follows:

- We propose the first secure non-repudiation solution that captures privacy and performance requirements and can be seamlessly integrated with the TLS 1.3 standard [39]. Our solution does not add new security assumptions to those of TLS and does not rely on an additional trusted third party.
- We implement our extension for TLS 1.3 on top of Mozilla's NSS library [33] and create an Apache module supporting our extension. Our experimental evaluation shows that a typical proof size as well as the proof generation and verification times grow linear with the size of the data. The server side processing times are low with less than 1ms for 16 KB plaintext without privacy protection and less than 8ms for 16 KB plaintext with privacy protection.
- We provide an Ethereum-based library for TLS-N proof verification and parsing. TLS-N therefore acts as a practical decentralized blockchain oracle that does not require any additional trusted third party. Users can source data from any TLS-N-enabled content provider, submit it to the blockchain where the smart contract verifies the proof. Note that only the data provider needs to be trusted, and as such any client can submit a TLS-N proof to the smart contract. On our website, https://tls-n.org we also provide an example oracle that securely inserts bitcoin prices into the Ethereum blockchain based on an API from bitcoin.com.
- We provide a structured description of non-repudiation properties, possible attacks, requirements and use-cases for non-repudiation solutions.

[1]The gas price determines the conversion rate between gas and ether and therefore influences the transaction cost.

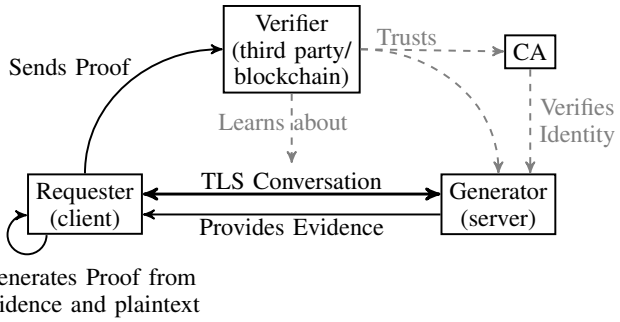


Fig. 1: Our view of non-repudiation. First, evidence generation (by generator), second proof generation (by requester), third proof verification (by verifier). Message originator and recipient might act as requester, generator or both.

The remainder of the paper is organized as follows. In Section II, we define the problem statement and motivate our TLS-based approach before presenting the design of our solution TLS-N in Section III. In Section IV, we perform its security analysis and evaluate it in Section V. We overview related work and contrast it to our solution in Section VI, while highlighting attacks on previous TLS-based work. We provide a discussion in Section VII, before concluding the paper in Section VIII.

II. Problem Statement

In this section we describe the main problem that we are trying to solve and we discuss relevant use cases and their requirements.

Broadly, we address the problem of non-repudiation in online interactions as seen in Figure 1. Given that such interactions are mainly protected using TLS [12], we focus on the provision of non-repudiation for services that run on top of TLS. TLS is the most widely used security protocol suite on the Internet and provides authentication, confidentiality, and integrity. Although it relies on public-key signatures for authentication, TLS protects message integrity and confidentiality of exchanged messages via shared secret keys that are established at the beginning of the session. Given this, TLS does not provide non-repudiation for the exchanged messages — clearly, a sender of the message can deny having sent the message, given that the Message Authentication Codes have been generated using a shared, symmetric key.

More precisely, we consider the following problem: *Can TLS be extended to provide a compact evidence allowing for efficient proof generation and verification so that the non-interactive proofs allow third parties to verify the TLS conversation contents.* [2]

In addition, since TLS peers might exchange privacy-sensitive content (e.g., login credentials, cookies or access tokens), the TLS extension should provide efficient, privacy-protection features to hide sensitive parts of the conversation from third parties.

[2]Here by extended we mean that a proper TLS Extension as specified in [39] can be created.

Based on previous work in the area, we consider the following non-repudiation types [20], [47], [1], [37]:

Non-repudiation of origin (NRO) provides proof that a message has originated from the specified originator. The evidence is provided by the originator and given the proof, the originator is not able to later deny having sent the message.

Non-repudiation of receipt (NRR) provides proof that a message was received by the specified recipient. The evidence is provided by the recipient and given the proof, the recipient is not able to later deny having received the message.

Non-repudiation of conversation (NRC) provides a proof of a total order of messages sent and received by a party. Intuitively, NRC specifies the conversation and the party's role in it, from the perspective of its system. The specified party is not able to later deny a claim of having sent and received the message in the conversation or the order of messages within the conversation.

Note, that non-repudiation of conversation (NRC) implies non-repudiation of origin (NRO) for all sent messages within the conversation and non-repudiation of receipt (NRR) for all received messages. Therefore, NRC is a stronger proof than NRR or NRO. To highlight the difference between NRO and NRC consider the following example. A web service returns the current stock price for a requested ticker symbol, e.g. for the request `EXAMPLE` the response is $10. Non-repudiation of origin would ensure that the web service answered $10. The answer by itself, however, is not useful without the context of the conversation. Non-repudiation of conversation would ensure that the web service answered $10 after being queried for `EXAMPLE`.

Apart from the non-repudiation type we also consider the following properties of a non-repudiation solution. These properties are motivated by different use cases, as we will show in Table I.

Order-Preserving: A total order of messages between the TLS peers can be determined based on the proof.

Request-Response Binding: A TLS conversation might include multiple requests and responses. This property ensures a binding between requests and responses based on the proof. This is important as protocols such as HTTP/1.x do not reference the request in the response, e.g. they contain no request ID.

Time: Based on the proof the content creation time (as seen by the peers) can be identified.

Privacy Protecting: Privacy sensitive content (e.g., passwords or cookies) transmitted in a TLS session can be efficiently hidden in the proof.

Possible use cases that would benefit from a non-repudiation solution are (cf. Table I) (i) Document Submission Systems (e.g., HotCRP) and (ii) Public Data Feeds, e.g. for stock exchange rates and currency exchange rates [45], [36]. Verifiable, public data feeds are essential for the further development and expansion of blockchain-based smart contract applications [44]. Given such a feed, public data can be securely inserted into the blockchain: a smart contract can, on submission of data including a proof, verify the proof and then store the verified data on the blockchain. Any other contract can use such blockchain-based information. This disintermediation removes the need for an additional third party acting as an oracle [46], [26]. Further use cases are (iii) Web Archives [2], [38] for web content or deleted social media content [14], and (iv) proving misbehaviour in P2P networks [34], [16].

	Evidence				Privacy		
Use Cases	Non-repudiation Type	Order-Preserving	Request-Response B.	Time	Protecting Sensitive I.	Protection Granularity	Usability
Document Submission	NRR	●	●	●	●	Bytes	●
Public Data Feed	NRC	◐	●	●	-	-	-
Web Archive	NRC	◐	●	●	-	-	-
Misbehaviour in P2P	NRC	◐	●	◐	◐	Bytes	●

TABLE I: For the use cases presented here, non-repudiation of conversation NRC is the most commonly required one. We also find that most use cases require request-response binding and timing information. Additionally, some use cases require privacy protection (e.g., hiding of access tokens or passwords). ● = required property, ◐ = partially required property, - = non-required property.

A. Previous Work and its Limitations

Here, we briefly motivate why existing work is insufficient and motivate our TLS-based design. For a more extensive discussion, please refer to Section VI.

Our design is TLS-based as this comes with multiple key advantages. TLS is ubiquitous. Based on the layer approach, many applications can benefit from a TLS-based solution. TLS provides extension support, allowing for incremental deployment as our extension is backwards compatible. We can reuse existing, cryptographic primitives of TLS reducing development and maintenance overhead. Additionally, most TLS deployments are based on a few cryptographic libraries simplifying standardization. Finally, TLS already uses an established public-key infrastructure (PKI) necessary for authentication.

1) Existing TLS-based solutions: Existing TLS-based solutions do not provide secure non-repudiation, as we will show in Section VI-B. In particular, none of the solutions provides NRC. We present attacks against all existing solutions and conclude that none of them has all the required security properties.

2) (Existing) Application Layer solutions: Non-repudiation can also be managed on the application layer. However, as we will explain in Section VI-B, application layer solutions come with multiple drawbacks. One drawback is that each of the application layer solutions has to provide a separate non-repudiation implementation resulting in many presumably poorly maintained implementations. Therefore, we think that the TLS layer should provide non-repudiation, because it already provides a frequently-used layer offering confidentiality and authentication to all kinds of applications. Furthermore, application layer solutions need their own authentication

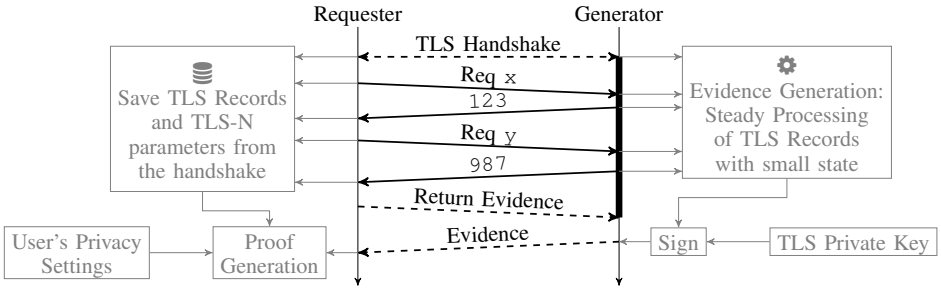


Fig. 2: Simplied Overview of TLS-N: The TLS conversation proceeds as usual. During the conversation the generator continually processes sent and received TLS records, thereby keeping only a small state. The requester stores all TLS records for the proof generation. The TLS-N-specific "Return Evidence" message closes the Evidence Window (shown as bold part of the time axis), which determines the evidence-relevant records. Upon receiving the message, the generator signs the evidence, which the requester uses to generate the proof according to the user's privacy settings.

scheme, while a TLS-based solution can reuse the existing PKI. Finally, in a design as ours, the application layer still retains full flexibility, as it decides what will be included in the proof.

To the best of our knowledge, there are currently no fully worked-out application layer solutions that would cover the relevant protocols that run on top of TLS. However, even if an application layer solutions would be built, this wouldn't devalue TLS-N, since to compare, one needs to design, build and evaluate both. TLS-N explores the TLS layer approach whereas we hope that application layer system might be explored in future work so that the two can be properly compared.

3) Other existing solutions: There are other solutions providing similar properties, such as TLSnotary [42] and Town Crier [46] that we will discuss in Section VI-C. While TLSnotary only works for older TLS versions and requires trust in a third party, Town Crier is a specific solution for smart contracts that requires a third party with special hardware and trust in the attestation service.

Our design, overcomes the shortcomings of previous work, requires no special hardware, no trusted third party and provides a general and portable solution for secure non-repudiation that reuses existing TLS primitives. We describe our design in the following section.

III. Our Design: TLS-N

Throughout this paper, we consider the following three parties: *(i)* the requester (typically a client machine), *(ii)* the generator (typically a web server) and *(iii)* the verifier (third party or smart contract), as seen in Figure 1. Our design, called TLS-N, provides generator-signed evidence about the TLS conversation to the requester, who can then construct a (redacted) proof. The design is similar to content extraction signatures [40] and redactable signatures [22], which have not been used in combination with TLS. We provide a comparison to these schemes in Section VI.

Figure 2 shows the evidence and proof generation between requester and generator. Initially, they establish a TLS connection and negotiate the TLS-N parameters in the handshake. During the TLS session, the generator keeps a small TLS-N state that is updated using all the sent and received TLS records [3]. This state contains a hash value incorporating all previous records, an ordering vector and a timestamp from the beginning of the session.

Once the requester asks for the evidence, the evidence window that defines which records will be included in the evidence closes. Note, that in TLS-N and in contrast to previous work the evidence window begins right after the handshake. To compute the evidence, the generator signs its TLS-N state using its private key. Together with the saved records, this evidence allows the requester to produce non-repudiable proofs for the entire conversation or for a subset of it.

Therefore, the requester retains full control what is included in the proof. To protect sensitive TLS content, the requester can hide entire records or chunks thereof. Note, that most client applications, e.g. browsers or email clients, are aware what content parts are sensitive, e.g., they know where passwords are used and how they are sent. Furthermore, TLS-N proofs can be further redacted if a sensitive piece of information was missed initially.

The generator is oblivious to what the requester considers sensitive and is not involved in the proof generation. By checking the proof, a verifier learns the disclosed content of the TLS session in a non-repudiable manner. We only make standard TLS assumptions, such that both requester and verifier trust the certificates to correctly identify the generator.

A. Parameter Negotiation

TLS sessions begin with the handshake during which settings such as the cipher suite are negotiated. If the requester wants to use TLS-N, it includes a TLS-N extension into the handshake. Here, the requester also specifies its preferences for the TLS-N settings. To hide sensitive content, the requester can chose between: *record-level* and *chunk-level granularity*. While chunk-level granularity is more precise it also has a higher computational overhead. In case of chunk-level granularity the requester can also select the chunk size. Again a smaller granularity leads to a higher computational overhead.

[3] In TLS, protocol messages including application data are sent in records.

Essentially, record-level granularity allows efficient proofs for public data, e.g. in a web archive, or for conversations where entire records can be censored. It represents the most efficient design, as the conversation has to be parsed record-by-record.

The generator can reject or accept the TLS-N settings by including a corresponding response in its handshake message. To ensure that TLS-N cannot be abused for Denial-of-Service attacks, the generator can also enforce the use of a TLS client puzzle [35].

B. Evidence Generation

In this Section, we outline how the generator (server) produces the evidence in TLS-N. We discuss the evidence window, the provided evidence and provided auxiliary information to aid proof generation.

In our solution, the evidence collection starts immediately after the TLS handshake. This has two main benefits. One is to prevent Content Omission Attacks (cf. Section VI-B1c) and the other is that TLS-N then does not require an explicit "Collect Evidence" message (proposed by related work [5]). In TLS-N, the evidence window ends as soon the generator receives a "Return Evidence" message.

1) Order of records: The generation of the evidence is non-trivial as the requester and generator might observe a different order of records. We label the i-th requester and generator records r_i and g_i respectively. If both peers simultaneously send records r_0 and g_0, each peer will observe its sent record before observing its received record, resulting in two different orders: (r_0, g_0) and (g_0, r_0). Note, however, that the two peers have identical partial orders over records generated by one peer, i.e., they observe the same order for all $\{r_i\}$ and for all $\{g_i\}$.

Based on their partial orders, both peers have to agree on a total order. In TLS-N the generator determines the total order of records, as it generates the evidence. To inform the requester about the chosen total order, the generator uses an *ordering vector*. As both peers have the same partial order over $\{r_i\}$ and $\{g_i\}$, the ordering vector is a bit vector encoding the interleaving of $\{r_i\}$ and $\{g_i\}$. In the ordering vector, a 0 corresponds to a record sent by the requester (r_i) and a 1 to a record sent by the generator (g_i). An ordering vector of $(1, 0, 0, 1)$ results in the total record order of (g_0, r_0, r_1, g_1).

2) Commitments: To allow chunk-level censoring of sensitive information during proof generation, each record of length l_r is split into fixed-sized chunks of the negotiated chunk size l_c. We construct hiding and binding commitments for each of the chunks using a commitment scheme `C()` that takes a chunk and a pseudo-random value, called salt, as input. As the chunk might have low entropy the pseudo-random salt is used to protect the hiding property of the commitment against brute-force attacks.

3) Merkle Tree Generation: To efficiently include commitments in the proof, we construct a Merkle Tree [30] over the commitments, as shown in Figure 3a. The root hashes of the Merkle trees h_i are generated from the children hash values, the length of the record l_r and the originator information O_i. O_i is the i-th element of the ordering vector. We assume that `H()` provides a binding commitment scheme, i.e., is a collision-resistant hash function. To reuse secure, existing TLS primitives we use the hash function negotiated in the cipher suite (typically SHA-256) as `H()`.

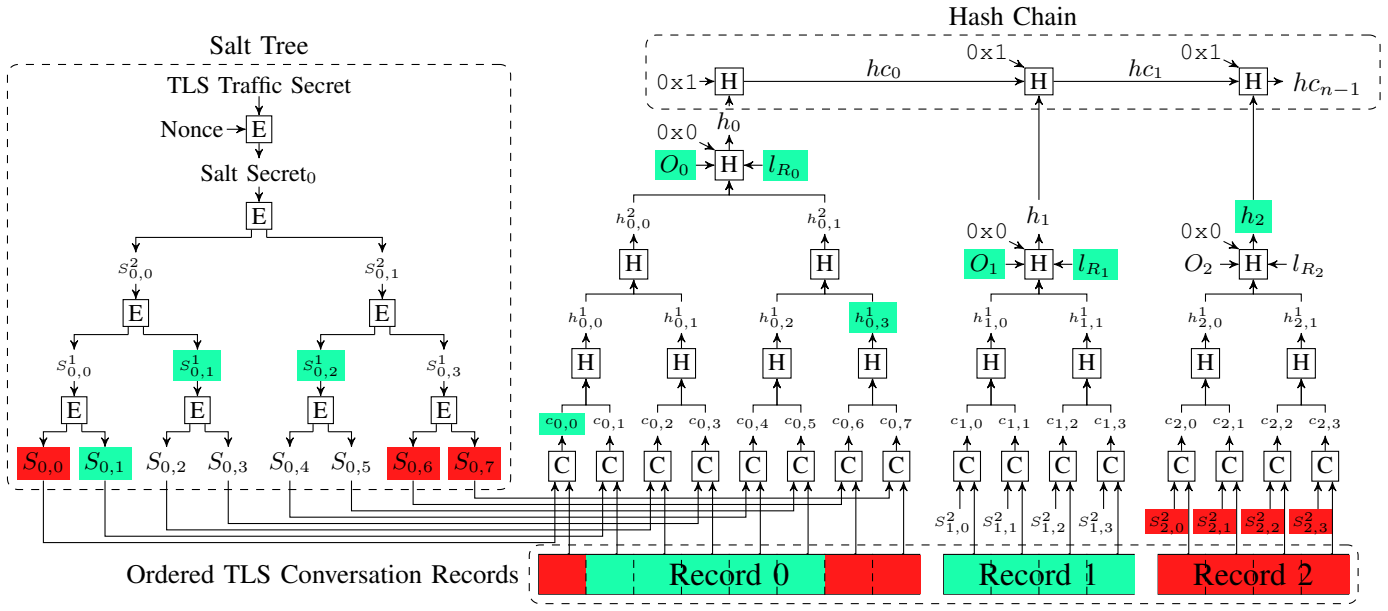
The records' root hashes h_i are combined in a hash chain (hc_i), with hc_{n-1} being the final hash chain state. Using a hash chain ensures a very small storage overhead per TLS session, namely only a single hash value. The hash chain uses markers (`0x0`, `0x1`) to prevent second preimage attacks, as explained in Section IV-C. A hash chain allows the server to keep a constant-size state while the TLS session is alive, namely the last hash chain element. A tree, in comparison, would require a state which grows logarithmically in the session size. Therefore, we chose a hash chain to minimize the memory overhead and the associated DoS risk.

4) Salt Tree Generation: To create hiding commitments using `C()` we need independent, random values S_{i_r,i_c}, called salts, for record i_r and chunk i_c. To achieve hiding, the outputs S_{i_R,i_c} and $S_{i'_R,i'_c}$ have to be independent, if $i_R \neq i'_R \vee i_c \neq i'_c$. Additionally, to reduce proof sizes we need efficient disclosure of salts for non-sensitive chunks. Therefore, we use a *salt tree* based on the function `E()` to derive the salt values. By using a salt tree, to censor a single chunk, only a logarithmic number of salts need to be revealed in the proof. `E()` is a variable-length output pseudorandom function that takes a pseudorandom key, (possibly empty) context information and the output length as inputs. `E()` leaks no information about its key.

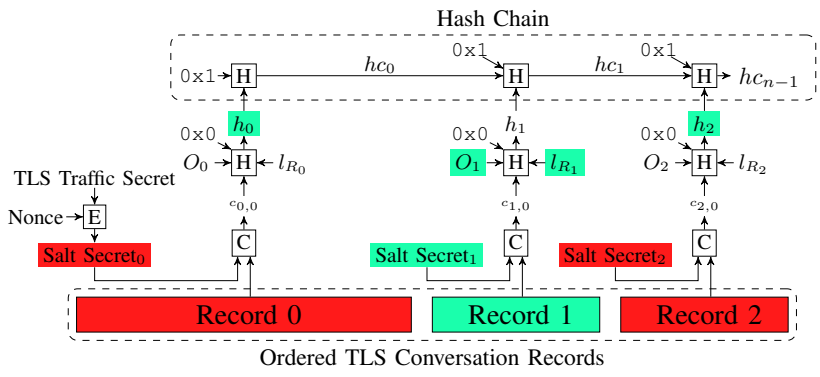
The salt tree is computed as follows (cf. Figure 3a): Initially, for each record R_i composed of c chunks, a unique salt secret is derived from the TLS traffic secret using a record-based nonce. This ensures the generation of a pseudo-random and independent salt secret as explained in Section IV-C. The derived salt secret is further expanded using `E()` to generate the salt tree. In the salt tree, each output of `E()` is truncated to length $2l_s$ and split into two bitstrings of length l_s, e.g., $S^2_{0,0}$ and $S^2_{0,1}$ in Figure 3a. Until the salt tree has c leaves and thus is large enough to supply a unique salt for every chunk of the record, this process is repeated, i.e. each intermediate secret $S^d_{i,j}$ at depth d is used as an input to `E()` and the output is split again to produce the values $S^{d-1}_{i,2j}$ and $S^{d-1}_{i,2j+1}$. The leaves of this tree are then used as salts. In TLS 1.3, `HKDF-Expand-Label` is used as `E()` [39], [23].

5) Chunk-level granularity vs. Record-level granularity: In Figures 3a and 3b we show the overall evidence generation based on the content for chunk-level and record-level granularity. For chunk-level granularity we combine the salt tree with the commitments, the Merkle tree and the hash chain. On the other hand for record-level commitments, we only generate a single commitment per record and therefore do not need a salt or Merkle tree. In short, for record-level granularity, each record is handled as a single chunk. In both cases we generate the overall hash chain result hc_{n-1} that is subsequently signed.

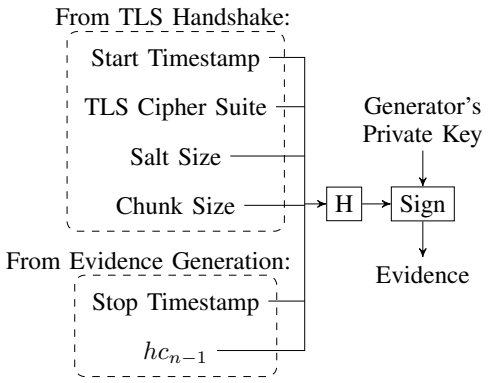
6) Providing Trustworthy Timing Information: To provide trustworthy timing information and protect against the Time Shifting attack (cf. Section VI-B1a), our design employs two generator-produced timestamps: one timestamp taken during the TLS handshake and one timestamp taken during evidence generation, i.e. at the beginning and the end of the evidence window. As both timestamps are included in the evidence, the



(a) Evidence Generation with chunk-level granularity. The left side shows the salt tree for record 0. The other salt trees are omitted due to space constraints. Commitments are generated for each chunk using a salt tree leaf (i.e. a salt). To reduce the proof size, a Merkle tree is computed over the commitments. The Merkle roots are combined using a hash chain, as the hash chain only requires a small state.



(b) Evidence Generation with record-level granularity. Salt tree or Merkle trees are not computed, as each record is just one one chunk. Record-level granularity has a significantly smaller computational overhead for all involved parties, but also provides less flexibility for privacy protection. For non-sensitive records, the complete plaintext and the salt secret is included in the proof.



(c) Final step of the evidence generation. Negotiated parameters from the TLS Handshake are included to protect their integrity. Out of the evidence generation the timestamp and final hash chain value are used. The evidence hash is signed with the private key.

Fig. 3: Evidence Generation based on the ordered TLS records using expansion function `E()`, commitment scheme `C()` and hash function `H()`. O_i gives the originator information and l_{R_i} is the length of record i. The record-based hashes h_i are input to a hash chain, whose result is the final hash value hc_{n-1} that will be signed by the generator. Sensitive content is marked red and is hidden in the proof while all green elements are included in the proof. Accordingly, we also color the salts in red and green. Red salts will not be disclosed and thereby provide a protection against dictionary attacks. Note, that the decision about included content is made by the requester during proof generation. We only provide the colors here for completeness.

verifier can detect proofs resulting from long TLS sessions and Time Shifting attacks.

As seen in Figure 3c, the evidence consists of the final hash hc_{n-1}, the two timestamps, the chunk size l_c, the salt size l_s and the TLS cipher suite negotiated for this session. When the evidence is requested, it is hashed and signed with the generator's private key. Our design limits the generator's computational overhead as it mostly computes hashes and only provides one signature. The evidence is sent to the requester together with the ordering vector. The requester can use the evidence to construct a variety of different proofs as we will show in the following section.

C. Proof Generation And Verification

A central benefit of performing non-repudiation over TLS is that we can reuse the already deployed public-key infrastructure (PKI). The signed evidence and its authentication can therefore be verified by third parties. However, third parties only possess the trusted root certificates and miss intermediate certificates required to verify the certificate chain. To allow third-party verification, the requester saves the certificate chain of the TLS connection and includes it in the proof.

Therefore, a proof contains these global parameters: timestamps for start and end, the negotiated salt size and chunk size, the number of records, the evidence signature, and optionally the certificate chain.

For every record, a proof node is included with the following information: type of proof node (e.g. hash chain element, plain text etc.), in case the proof node contains hidden data: hashes and salts and their respective locations in the Merkle and salt tree; in case the proof node contains plaintext data: plaintext length and plaintext data, and the originator information.

For proof generation, the requester uses the n records, the salt secrets, the evidence provided by the generator, the ordering vector, and the certificate chain. Based on these, the requester can generate different kinds of proofs. Here, we give some representative examples.

1) Proving NRO or NRR: As explained in Section II, NRC implies non-repudiation of origin (NRO) and non-repudiation of receipt (NRR). Therefore, we can also prove these for one or multiple messages of the conversation. A NRO-proof or NRR-proof for a record i, contains the following: plain text of record i, salt secret i, O_i, hc_{i-1}, $h_{i+1}, \ldots, h_n$, the evidence and the certificate chain.

During proof verification the verifier uses the plain text of record i, its salt secret, the cipher suite and O_i to build the Merkle tree and salt tree, and compute h_i as in Figure 3a. Using the hash chain value hc_{i-1} and the computed h_i the verifier can compute hc_i and using the $h_{i+1}, \ldots, h_n$ the verifier can complete the hash chain and compute hc_{n-1}. Then, the verifier checks the evidence, by verifying the signature using the certificate chain and comparing its hc_{n-1} to the provided hc_{n-1}. Finally, the verifier checks the timestamps based on the application-specific requirements, e.g., testing whether they are too far apart or from a wrong date.

2) Privacy-preserving, browser-based NRC proof: In this scenario, the browser acts as the requester and a web server as generator. The browser is configured to consider all passwords and cookies sensitive and remove them from the proof, while the web server is unaware of these privacy settings. To hide only the passwords the browser requests evidence with chunk-level granularity. The web server generates the evidence as shown in Figure 3a.

For the proof generation the browser proceeds as follows: For every record i *without* sensitive information, the browser includes its plaintext, its salt secret and O_i. For every record i *with* sensitive information, the browser proceeds as in Figure 3a. All plaintext of all non-sensitive chunks are included with their salts $S_{i,j}$. For chunks with sensitive content the browser includes their commitment and keeps their salt values secret. Thereby, dictionary attacks are infeasible even if the content has low entropy. If subsequent chunks are sensitive or non-sensitive the browser includes higher level-nodes from the Merkle tree and the salt tree respectively. Therefore, only $O(\log(c))$ nodes have to be included and the proof size is reduced. Additionally, the proof contains the evidence, and the certificate chain.

During proof verification the verifier uses the proof to regenerate the same evidence as in Figure 3a. For records *without* sensitive content it constructs the Merkle Tree and salt tree, for records *with* sensitive content it constructs the partial Merkle Tree based on the provided plaintext, commitments and hashes. Thereby, the verifier obtains all root hashes h_i, constructs the hash chain and hc_{n-1}. As before the verifier also checks the evidence based on the certificate chain and validates the timestamps.

IV. Security Analysis

In this section we present the security analysis of TLS-N. We start by introducing our system and attacker model.

1) Trust assumptions: For the purpose of this paper, we make the following trust assumptions. First, we assume that the used cryptographic primitives such as digital signatures and cryptographic hash functions are secure. We need `H()` to produce a binding and hiding commitment. Note, that the hiding property of hash functions has neither been proven nor rejected. Second, we assume the existence of a Public Key Infrastructure (PKI) that correctly binds entities to the public keys used in TLS, i.e. we inherit the trust assumptions of TLS when used with certificates. Hence, both requester and verifier trust the generator's identity. Note, that we assume public keys to be unique which they might not always be [19]. Third, we assume that private keys used by the generator are not leaked to the adversary and that the generator will not sign arbitrary statements. In any non-repudiation solution relying on digital signatures, incorrect use of the private key compromises the security of the scheme. We consider concrete solutions to the problem of revoked or leaked private keys to be out of the scope of this work (a non-repudiable statement could be included in a blockchain together with a consecutive Online Certificate Status Protocol (OCSP) response to proof the validity at creation time). Fourth, we assume that TLS connections are not intercepted, e.g. by some middle box. Finally, the verifier trusts the generator to produce accurate content and timestamps.

A. Security Properties

For the security analysis, we adopt the security definition of Content Extraction Signature [40] . The extended security definitions and proofs had to be omitted due to space constraints. Please find the complete version under https://tls-n.org.

Property P_0 , is the adapted CES-Unforgeability stating that a valid proof can only be produced for a conversation that is a subconversation of a conversation signed in a proof. Here, we substitute the documents in the definition of CES-Unforgeability with the conversations.

Property P_1 is the adapted CES-Privacy, stating that a proof leaks no information about hidden parts.

Property P_2 : The proof reveals the structure of hidden data. Records with hidden chunks are distinguishable from records without hidden chunks and conversations with missing records are distinguishable from complete conversations.

Property P_3 : For every non-hidden record, the originator is known.

Property P_4 : The timestamps inside the proof provide tight upper and lower bounds on the generator's time during the conversation.

B. Adversarial Model

We assume a computationally-bounded adversary that can take one of two roles. Either the adversary acts as requester trying to generate proofs that lead the verifier to wrong conclusions about the conversation (violating P_0, P_2, P_3 or P_4). Or the adversary acts as a verifier trying to learn hidden data (violating P_1).

Either way, the adversary is allowed to interact with the generator, request evidence for different conversations and inspect proofs published by other users. Furthermore, in accordance to the TLS threat model, on the network the adversary acts as described in the Dolev-Yao Model [13]. In section VI-B1, we detail attacks on existing solutions under this adversarial model.

C. Security Sketch for TLS-N

In this section we provide a brief security analysis of TLS-N. The full analysis and the proofs had to be omitted due to space constraints, but is available at https://tls-n.org.

For Property P_0, the unforgeability of the signature scheme and the collision resistance of `H()`, ensure that the additional data (parameters and timestamps) and the hash chain output are unforgeable. The unforgeability of the hash chain inputs, namely the Merkle hashes, reduces to the collision resistance of `H()`. Given all these, the CES-Unforgeability is satisfied for each records according to the proof provided by Steinfeld et al. [40] as records are almost identical to documents and as the differences are irrelevant for the proof.

For Property P_1 we need to prove that the commitments do not leak any information and that the TLS traffic secret is not revealed, which together with the adversarial network capabilities would disclose hidden data. The hiding property of `C()` is sufficient for the first part given that the salts are pseudorandom and independent. Salts are pseudorandom due to the properties of `E()` and independent as for each record they are derived from an independent salt secret. The TLS traffic secret is not leaked as it is only input to `E()`, which due to its properties does not leak it.

A hidden chunk is observable due to the definition of a record and its length is known due its position, the chunk size and the record size. If the first record of a conversation is not included the proof must start with a hash chain node of the type `H(0x1,`hc_{i-1}`,`h_i`)` instead of `H(0x1,`h_0`)`, which together satisfies property P_2.

As the records include originator information that is unforgeable due to P_0, P_3 is satisfied. And as the timestamps are likewise unforgeable and are taken at the beginning and the end of the evidence window, tight bounds can be provided on the generator's time, fulfilling P_4.

V. Implementation and Evaluation

In this section we describe our TLS-N implementation, its deployment and its evaluation using real-world as well as synthetic traffic. The code for our implementation and further details can be found at https://tls-n.org.

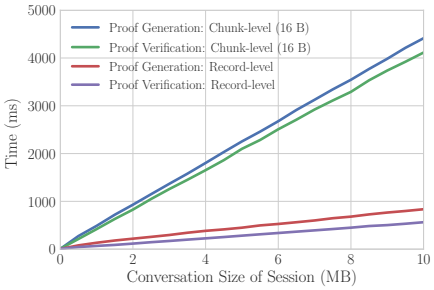
A. Implementation

For our implementation, we extend the Network Security Services (NSS) library [33] provided by the Mozilla Foundation. We chose the NSS library for its support of TLS 1.3 and because it can be used on the client side, e.g., in Mozilla Firefox, and on the server side, e.g., through the mod_nss Apache module [9], [10]. We implement TLS-N as an extension in NSS and deploy it in a real-world setting using an adapted version of mod_nss and Apache running on an Amazon EC2 node. Our unoptimized NSS extension uses roughly 2400 lines of C code.

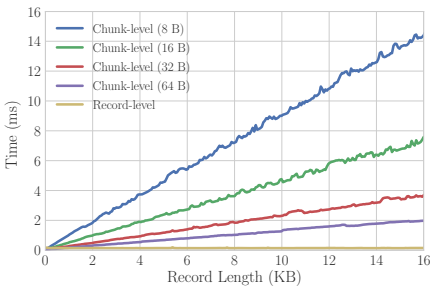
We extend TLS so that the requester application can enable the TLS-N extension. The peers negotiate the usage of TLS-N during the handshake. We use a 16-byte salt size, in order to preserve the 128-bit confidentiality protection of TLS [12]. Unless otherwise stated, we also use a 16-byte chunk size, as Figure 4b shows that it provides a good trade-off between granularity and efficiency. For `H()` our implementation uses the hash function of the chosen cipher suite and for `E()` we use the `HKDF-Expand-Label` function with specific labels for salt secret and salt tree generation. `HKDF-Expand-Label` is already used for these properties [39]. As nonce for the salt secret generation, we use the TLS per-record nonce [4], which is guaranteed to be unique in combination with the traffic secret [39]. For `C()` we use the same function as for `H()`, as we assume that modern hash functions with sufficiently large salts provide a hiding commitment. To reduce the proof size we use TLS certificates using elliptic curve cryptography, namely secp256r1. Overall, we completely reuse cryptographic primitives that are already present in TLS.

Our extension then constructs a proof according to the settings of the requester application, which provides regular expressions for sensitive content that is then hidden in the proof. Finally, the proof is returned to the requester application. The requester application can store the proof and send it to

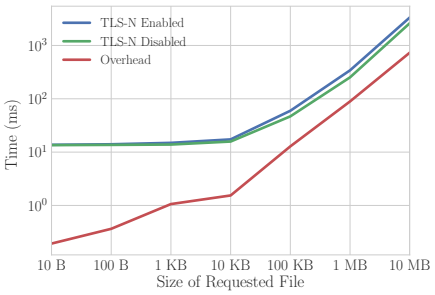
[4] In TLS 1.3 the per-record nonce is a bi-directional record counter. [39]



(a) Proof generation and proof verification times for random, simulated TLS sessions. Such proofs without hidden data are the worst case for the proof verification. We observe a linear scaling for both times. Each result is averaged over 20 repetitions.



(b) Average processing time for one record depending on its size. Time includes building salt and Merkle tree. Chunk-granularity with sizes ranging from 8 to 64 bytes is compared to record-level granularity. 16 KB is the largest NSS-supported record size.



(c) Average time from sending one HTTP request until the requested file is received with and without our TLS-N extension running on an Apache webserver. We find that TLS-N is usable, even for bigger files. Each result is averaged over 100 measurements.

Fig. 4: Performance Evaluation for our implemented extension of TLS-N on client and server side.

		Conversation Size			
		1 KB		10 KB	
		secp256r1	secp256k1	secp256r1	secp256k1
Costs	Basic Gas	119,758		737,159	
	Total Gas	1,284,723	131,286	1,938,872	782,219
	Ether	0.0257	0.0026	0.0388	0.0156
	USD	5.2198	0.5334	7.8776	3.1782

TABLE II: Gas costs for validating public, record-level proofs within our Ethereum smart contract based on the conversation size and the elliptic curve. The basic gas cost is intrinsic for a transaction of that size. Gas and ether prices taken as of August 1st 2017.

verifiers. Verifiers can use our library extension to determine the validity of a proof, which includes the necessary salt tree and Merkle tree computations as well as the signature check and the verification of the included certificate chain.

B. Blockchain Implementation and Evaluation

To show that the proof verification can be performed by a blockchain-based smart contract, we provide an Ethereum [44] implementation of the proof verification procedure in our TLS-N solidity library, which is available at https://tls-n.org. The library parses the proof, computes the hashes, and performs a signature verification. The library contains 45 lines of solidity code. The unoptimized secp256r1 signature verification has 168 lines. We measure the cost of these operations in gas, Ethereum's currency for computational tasks.

Table II shows the respective gas costs in ether and USD (at the time of writing), depending on the conversation size (the cumulative length of all records) and the elliptic curve used in the evidence signature. We also show the basic gas cost that results from the size of a transaction [44]. We show two elliptic curves, because no elliptic curve is supported by major TLS implementations and Ethereum (TLS implementations mostly support secp256r1 while Ethereum uses secp256k1). The costs differ greatly for the signature schemes, because Ethereum's support for secp256k1 [4]. We had to implement verification for secp256r1 on top of Ethereum, resulting in a verification cost around 1.2 million gas per signature verification. Overall, we observe, that the proof validation costs are dominated by the basic gas cost and cost for signature verification, whereas our design only adds a marginal cost.

Another issue is the certificate chain verification within the blockchain. To the best of our knowledge, there is no blockchain-based system to verify TLS signatures based on the web-PKI. We, therefore, suggest that the verifying smart contract knows the generator's (e.g. the content provider's) public key so that it can omit the certificate chain verification. Our smart contract library supports this functionality and our website allows the generation of (blockchain-specific) proofs without the certificate chain. Essentially, the public key is thereby pinned inside the smart contract, which, however, might allow this pinning to be updated. Once the smart contract has verified the proof, it knows that the conversation is authentic and can act immediately, e.g. perform a matching payout, save the content or save a content hash in order to avoid future verifications.

Given our smart contract implementation, TLS-N allows to connect web-based content from any TLS-N-enabled content provider such that any smart contract can operate on the provided, non-repudiable data. Note that the requester is not required to be trusted, and as such any requester can submit a TLS-N proof to the smart contract. Therefore, clients can even use web services, such as at https://tls-n.org, to generate proofs. On the project website we also provide an example oracle using our library. The oracle accepts proofs from the bitcoin.com-API [27] to securely insert bitcoin prices into the blockchain.

C. Evaluation

In the following we evaluate the performance of our implemented TLS extension using real world examples and synthetic examples to test its scalability, as shown in Table III and Figure 4.

1) Real-world Examples: We evaluate the performance of TLS-N for real-world examples by replaying recorded HTTP connections of web services, such as the Twitter API, Facebook

API, YAHOO! API and a Google Search (cf. Table III). Since the network latency is irrelevant for the proof size and the processing times, we locally replay the recorded traffic between a Lenovo X220 laptop and a server with an Intel Core i7.

We first study the time we deem most critical, the server's processing time during the TLS connection. For conversation sizes below 6 KB the server has a total processing time of less than 3.5 ms. After processing all the records during the connection, the server's final step of the evidence generation is independent of the conversation size. For chunk-level proofs, we filter all cookies, passwords and authentication tokens, but we also show an unfiltered record-level proof, namely archiving a Wikipedia page, which is significantly more efficient given the conversation size.

2) Performance Projections: In Figure 4a, we study the scalability of proof generation and verification using synthetically generated proofs. For each size, we create random conversations consisting of 2000-byte records. We observe that the proof generation and verification times scale linearly in the conversation size. Regarding the proof verification, Figure 4a shows the worst-case scenario, as the proofs contain no hidden data and as such all salt and Merkle tree nodes have to be computed. We observe that proofs with record-level granularity are significantly efficient, as Merkle and salt trees only have a single node.

In Figure 4b, we find that server processing times scale linearly in the record size. We plot the average server side processing time for a single record depending on the record length and the chunk size. Bigger chunk sizes require less computation, but have a coarse-grained privacy protection. Along this trend, record-level granularity is by far the most efficient solution.

3) Latency Overhead: To estimate the real-world overhead of a complete HTTP request, we measure the overhead of our implementation on the latency of HTTP requests to an Apache server running on an Amazon AWS c4.large instance. In each request, the client requests a file of a size between 10 and 10^7 bytes (in powers of 10). For each file size, the average time from sending the request until the file is received is plotted in Figure 4c. Again, we use a chunk size of 16 B. We observe that as long as the whole file can be sent in a single record (i.e. its size is smaller than 16 KB), the latency of TLS 1.3 without TLS-N remains below 10 milliseconds. For larger files the overhead increases but remains below one second for 10MB files. Even though our implementation is neither optimized or parallelized, i.e. the overhead could still be reduced, the overhead appears tolerable. Additionally, recall that this was achieved with a relatively small chunk size of 16 B.

VI. Solution Space and Related Work

In the following we summarize existing solutions and their limitations, provide insights on possible strawman solutions and compare their applicability to the use-cases from Section II and which properties they satisfy.

A. Related Approaches

In this section, we overview approaches that are related to our design and describe their properties.

Content Extraction Signatures [40] aim to solve a similar problem. Given a signed document, different parts can be extracted while the signature remains valid and is still verifiable by third parties. Content Extraction Signatures consist of a "PseudoRandom Generator with Seed Extraction" corresponding to our salt tree and use merkle trees based on commitments. As they are only designed for a single document, the document length is included in the signature. We include the record length and the originator information in the Merkle root node.

Redactable Signatures [22] as proposed by Johnson et al., are also design-related. Their GGM tree [15] corresponds to our salt tree and they use a Merkle tree, however without commitments. However, they do not include the overall document length in the proof so that a verifier cannot observe how much data was "redacted", if it was "redacted" at the end of the document. Also, their solution requires a marker in every Merkle tree node which is less efficient.

Further additions to redactable signatures provide transparency [6], [24]. These signatures aim to prevent any inference attacks as they hide the structural information of the data. Some schemes even make it impossible for the verifier to observe a redaction. In our work, we intentionally reveal the fact that data was hidden and its structural information (P_2). Previously motivated [22], we provide our motivation for this design through the Content Hiding Attack.

Another related solution, Sanitizable Signatures [7], can be generated by a signer using its private key. They also include the public key of a designated sanitizer and a division into blocks and admissible. These admissible blocks can later be changed by the sanitizer. However, in our design there shouldn't be a designated sanitizer. To simplify adoption and deployment, any generator-accepted peer can act as requester.

Authenticated Data Structures [32], [11] achieve a similar goal as our design. An untrusted party extracts or computes a result based on a signed construct so that the result correctness can be verified by a third party. However, authenticated data structures are more aimed at data outsourcing, e.g. for databases.

B. Existing and Strawman TLS Solutions

In this section, we look at other solutions to provide non-repudiation through TLS and present attacks according to our adversarial definition in Section IV. The solutions and their provided properties are summarized in Table IV.

TLS Sign is a proposed extension [17] for TLS 1.1. TLS Sign defines a new sub-protocol (or content type) for TLS called TLSSignOnOff (in addition to the three already existing: Handshake, Application data, and Alert). Both, client and server can use the TLSSignOnOff messages to notify their peer that they will start or stop transmitting signed data, i.e., the sub-protocol is used to specify the evidence window. In the evidence window, each record is hashed, and a signature over this hash is generated. When the stop signal is triggered, the generator gathers all hash signature pairs and sends them to the requester as evidence.

			Server side during TLS session			Client side, Offline				
			Online	Upon Request						
Use Case	Conversation Size (B)	Number of Records	TLS-N Processing Time (ms)	Evidence Size (B)	Evidence Generation Time (ms)	Proof Type	Proof Size^{+} (B)	Proof Generation Time (ms)	Proof Verification Time (ms)	Hidden Data, e.g., cookies (B)
Twitter API	5,320	3	3.223	84	0.404	Chunk	5,668	9.491	10.345	348
Facebook API	3,187	4	2.041	84	0.394	Chunk	3,629	8.410	9.734	224
YAHOO! API	2,038	4	1.376	84	0.395	Chunk	2,676	8.721	10.032	182
Oanda API	935	2	0.662	84	0.397	Chunk	1,414	6.320	8.767	161
Google Search*	549,530	424	283.162	84	0.398	Chunk	552,180	357.411	231.934	10,001
Wikipedia Archive	585,136	218	11.418	84	0.339	Record	589,924	20.949	20.662	0

TABLE III: Use case evaluation: For each use case we give its sizes, total, server-side processing time during the session, the evidence generation time (performed upon request) and the client-side times for proof generation and verification. We highlight the only additional latency during the TLS session. Times are averaged over 20 repetitions. When applicable, the chunk size was 16 B. *The Google Search includes many records due to auto-completion.$^{+}$ The proof size includes the conversation size.

	Evidence				Privacy/Leakage		
Solutions	Non-Repudiation	Order-Preserving	Request-Response B.	Time	Protecting Sensitive I.	Protection Granularity	Usability
TLS Sign	NRO	-	-	-	●	Record	◐
TLS Evidence	NRO, NRR	◐	-	◐	●	Record	◐
MAC Chaining	-	-	-	-	-	n/a	-
One Signature	NRC	●	●	●	-	n/a	●
Our Solution	NRC	●	●	●	●	Bytes	●

TABLE IV: Provided properties satisfied by the different solutions. ● = provided property, ◐ = partially provided property, - = not provided property.

The development of TLS Sign had stopped before a final version was released; thus this extension is incomplete. TLS Sign's design presents following disadvantages: TLS Sign is inefficient, because it requires one asymmetric signature per record within the evidence window. TLS Sign is vulnerable to content reordering and content omission attacks. Therefore, TLS Sign only provides NRO and no timing information or message ordering.

TLS Evidence is a TLS extension [5]. Similar to TLS Sign, the client expresses his intent to use TLS Evidence in the TLS extension field. TLS evidence uses a set of new alert messages to be transmitted in the existing alert protocol to define the evidence window. The requester sends an alert message and waits (i.e. he is not allowed to send any messages) for the responding alert. After exchanging these alerts, the evidence window is open until one of the peers sends an alert, triggering a corresponding reply. Then, the peers exchange their certificates and generate the following evidence: a signature over a timestamp, a hash over all sent messages, a hash over all received messages and a hash of the handshake.

TLS evidence has several limitations. First, for human-centered use cases it is unclear when to start and stop the evidence collection.Second, since TLS evidence provides a signature over the hash of all sent and the hash of all received messages, it only provides a partial order within the sent and the received messages. However, the total order between sent and received messages is not preserved. Therefore, TLS Evidence is vulnerable to the content reordering attack, as seen in Figure 5. Because the evidence window can be opened after some content has already been transmitted, TLS Evidence is also vulnerable to the content omission attack. Finally, as the included timestamp is the time of evidence generation, a time shifting attack is possible. Therefore, TLS Evidence only provides NRO, NRR, a partial order and upper time bound.

MAC Chaining was described in the IETF mailing list [25] as combining the already-used Message Authentication Codes (MACs) of individual records to a MAC over the complete communication. MAC Chaining suggests including the MAC of the previous record into the current record and thereby chaining the MAC properties. Finally, to provide the evidence the last MAC of the communication is signed to verify the whole stream with very small overhead. Two variants of MAC Chaining are proposed that either verify only one side or both sides of the communication.

However, in TLS 1.3 a proof for MAC Chaining would have to include the TLS traffic secrets used for authenticated encryption (AEAD) [29] to allow the verification of individual MACs. Given such a proof, including the TLS traffic secrets, the signature of the last MAC and the conversation content, the adversary can create proofs with different conversation content. In short, the unforgeability of P_0 is violated. This is because AEAD authentication tags, for all cipher suites available in TLS 1.3 [39], are not considered collision resistant if the key is known to the adversary. We therefore conclude that MAC Chaining provides *no non-repudiation* as proofs can be forged given an existing proof.

Signing the complete TLS session from the beginning of the handshake until one party closes the connection would be one of the simplest solutions to provide non-repudiation. The evidence window would thereby cover the complete connection. Similar to previous work, such an extension would require the inclusion in the handshake and an additional evidence message at the end of the session.The evidence would be order-preserving. However, this solution requires the requester to store all records in order to be able to compute the final signature and would necessarily result in a big proof size. Finally, such a non-repudiation service offers no privacy protection. In contrast our record-level approach has comparably low computational costs, while being more efficient and providing

record-level privacy protection.

Signing content at the application layer could be another non-repudiation solution, as one could argue that such a functionality should not be handled at the TLS layer. Two parties can exchange signed content on the application layer by explicitly requesting to sign data, or employ already existing protocols such as OpenPGP [8]. Application layer non-repudiation however suffers from several disadvantages. First, regarding reusability, an application layer solution would only support a particular protocol/application. Having a TLS layer solution, however, enables any TLS-based application to benefit from non-repudiation. Second, an application layer solution would require that private keys are exposed to the application layer, contradicting the principle of minimum exposure and that the TLS layer is responsible of managing the cryptographic keys.

There are existing solutions providing additional authentication for REST-ful HTTP as studied and extended by Lo Iacono et al. [28]. However, these solutions include different HTTP headers, would have to be extended for future headers and provide authentication only. A TLS-based non-repudiation solution includes all of the HTTP traffic and allows the proof contents to be chosen during proof generation. Finally, in contrast to the existing solutions, TLS-based non-repudiation solves the problem of public key authentication by leveraging the already established web-PKI. Using the existing PKI from the application layer would require the exposure of private keys.

As explained in the previous section, earlier works are vulnerable to a number of attacks and do not achieve all of the desirable properties. Furthermore, they don't easily allow the specification of the evidence window and, therefore, limit usability. The protection of sensitive information moreover is only feasible on a record granularity which is impractical for most applications (e.g., stock market API).

1) Attacks on Existing TLS Solutions: In this section we present attacks against existing TLS solutions apart from the already explained attack on MAC Chaining.

a) Time Shifting Attack: In Section II we described why proofs should contain timing information. However, an adversary acting as requester can manipulate time information included in the proof. The possible kind of manipulation depends the kind of timing information included in the proof.

If a single timestamp is included, the adversary can manipulate the connection according to its type. If the proof generation time is included, the adversary can request the information at time t, then keep the connection open for a time duration Δt and finally request the proof at time $t' = t + \Delta t$. Note that Δt may be substantial as TLS connections can be long lived. Therefore, the proof contains timestamp t' for content requested at time t. Even if Δt is only in the order of minutes, this could have big impacts for data feeds such as stock prices or currency exchange rates. Thus, if such attacks are possible, the timing information is not trustworthy, violating P_4.

b) Content Reordering Attack: As our system makes no assumptions about the higher level protocol, we must assume that there are cases where the order of messages is important. In particular, the verifier should be able to identify the message order from the perspective of the generator, i.e. the relative order of sent and received messages.

If the adversary can perform a partial content reordering or the content order is not clear from the proof, unforgeability is violated. The scheme cannot prove non-repudiation of conversation (NRC) as the context is unclear. An example relevant for TLS Sign and TLS Evidence is shown in Figure 5.

c) Content Omission Attack: If the adversary acts as the requester and if the evidence window does not start right after the TLS handshake, i.e., the non-repudiation service allows omission of content as in TLS Sign or TLS Evidence, P_2 is violated. Figure 6 shows a scenario where the adversary requests a resource `x` before opening the evidence window, immediately requesting another resource `y` and closing the evidence window. Now, only two records are in the evidence window: the request for `y` and the response for `x`.

If the upper-level protocol does not supply any resource identifier in the response, as is the case for HTTP 1.x, it appears to a verifier that `x` was the legitimate response to the request for `y`. Therefore such non-repudiation services provide no request-response binding and cannot provide a NRC.

d) Content Hiding Attack: In this attack the adversary hides important communication content of variable-length protocols by abusing the privacy protection features. In particular, the adversary hides a part of the communication, e.g. a complete request, in order to trick the verifier. An example is shown in Figure 7.

In Figure 7 we assume a simple protocol with three message types: authentication with a password (Auth), requests with an identifier (Req) and responses. As passwords, identifiers and responses can be of variable length, all messages are terminated with a special character ($\backslash 0$).

The adversary first starts evidence collection, then authenticates, sends two requests for resources `x` and `y` and then requests the evidence so that only the response for `x` will be included in the evidence. If the non-repudiation service allows the protection of information, the adversary hides the password along with the request for `x` (up until the terminating character). The verifier observes the authentication with a hidden password, a request for `y` and the response `123`. The verifier therefore incorrectly assumes that `123` is the correct response for resource `y`, even though it is `987`.

The adversary can send authentication and first request within the same TLS record, so that the verifier cannot use TLS metadata to determine whether an extra request was sent.

C. Orthogonal Solutions

In the following, we describe orthogonal solutions that offer evidence of TLS sessions using a trusted third party, e.g., TLSnotary [42] and Town Crier [46].

1) TLSnotary: TLSnotary [42] provides a service that allows a third party auditor to attest a TLS connection between a server and a client. If the client follows a particular protocol with a third party auditor, while initiating a connection to a server, the third party auditor is able to claim with certainty that the client provided data that originated from the server. TLSnotary modifies the TLS handshake protocol on the client

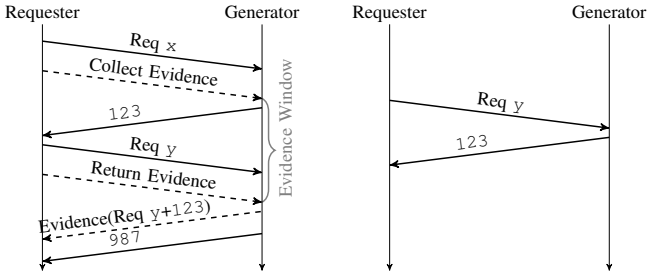


Fig. 5: Content Reordering Attack: The left figure shows the original and the right figure the signed conversation. Due to content reordering, the response `123` seems to belong to request `y`, which is incorrect.

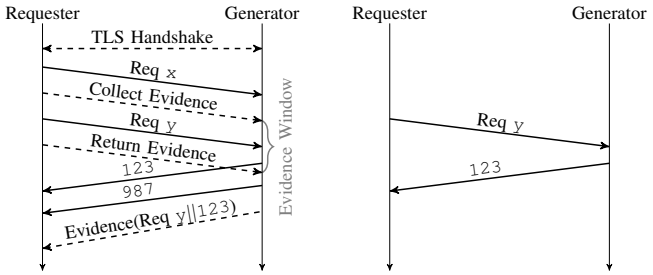


Fig. 6: Content Omission Attack: The left figure shows the original and the right figure the signed conversation. Since context is missing in the signed conversation, the response `123` appears to belong to request `y` which is incorrect.

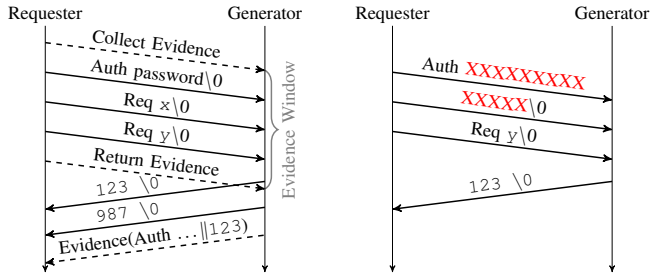


Fig. 7: Content Hiding Attack: The left figure shows the original and the right figure the signed and redacted conversation. The verifier can not determine whether a long password was used or an additional request took place.

side by leveraging particular properties of TLS 1.0 and TLS 1.1. The modified protocol prevents the client from learning the TLS key material that would allow the client to authenticate traffic from the server. More specifically, the client is not able to generate the server MAC key, only the third party auditor is capable of doing so, effectively preventing the client from crafting traffic that seemingly originates from the server. After the client provided a hash of the traffic, the third-party auditor releases the TLS server MAC key. The client can then verify the message authentication.

a) TLSnotary Limitations: Although TLSnotary provides the capability of notarizing TLS connections, it comes with several limitations and security issues.

First, TLSnotary is only supported up to TLS 1.1. The properties that are used by TLSnotary were removed in versions 1.2 and 1.3. TLS 1.1 and below are considered less secure than current TLS versions. Second, TLSnotary uses and can only use the hash functions MD5 and SHA-1, both of which can be considered deprecated [41]. Third, TLSnotary only supports the RSA key exchange, which does not provide forward secrecy. Last, TLSnotary requires trust in a third party in most use cases, e.g. if the evidence should be publicly verifiable. If the verifier takes the role of the auditor in the protocol, a trusted third party is not required. However, in that case, the verifier needs to take part in the interactive protocol, i.e. evidence of a past session cannot be provided.

2) Town Crier: Town Crier [46] allows disintermediation through the Intel SGX technology. Town Crier can provide publicly verifiable data feeds based on the contents of a TLS session, but it can also do more as it has computational resources and allows further confidentiality. In order to provide verifiable data feeds for smart contracts (e.g. on the Ethereum blockchain [44]), the core of Town Crier runs in an SGX enclave and can thus provide attestation that the correct code was executed. Town Crier then forwards information that was provided by an HTTPS website to a smart contract on the blockchain.

a) Town Crier Limitations: Similarly to TLSnotary, Town Crier requires a trusted third party, i.e., a client of the service needs to trust Intel since the attestation relies on the security of Intel SGX. In contrast to TLSnotary, Town Crier always requires the trusted third party and requires correct SGX attestation.

VII. Discussion

In the following we discuss observations and possible avenues for future work. Our solution is not directly applicable to Datagram TLS (DTLS) that is based on UDP. The DTLS extension remains as a challenge. Moreover, because TLS 1.3 provides simplified resumption features, TLS-N could be extended to support TLS session resumption.

A. Validity or Expiry of Proof

A proof should only by considered valid as long as all involved TLS certificates are neither outdated nor revoked. In order to retrospectively understand the time of validity of a proof, either the generator or the validator could make use of a timestamping service attesting the existence of the proof. Besides a centralized service, a cryptographic hash of the proof could also be submitted to a blockchain, effectively timestamping the first occurence of the proof and reducing the trust into a single entity.

B. Variable-sized chunking

Our current solution provides fixed-size chunking which is generally applicable, but which might not represent the most efficient solution for the privacy protection of certain applications. Cookies or access tokens (e.g. an OAuth bearer token [18]) are typically stored in the HTTP header. In a

hypothetical HTTP mode, TLS-N could support variable-sized chunking, where one chunk could represent one HTTP header. The privacy protection of one header would therefore be more efficient.

C. SNARKs for extended Proofs

In some cases, it may be desirable for a requester to provide a more fine grained proof. For example, if a higher-level protocol is used that contains large sections of sensitive variable length data, an attacker could succeed with a content hiding attack (cf. Section VI-B1d). In such cases, the proof will no longer convince a verifier of its validity. Therefore, a requester can extend the TLS-N proof with a zk-SNARK [3]. Such a proof could e.g. prove that the hidden content matches some regular expression, i.e. that no non-sensitive content is censored that is required for the correct semantic meaning of the provided data.

Additionally, a prover can extend a TLS-N proof with a zk-SNARK to prove some statement about the sensitive data. For example, if a party requires proof of sufficient funds, a prover can provide a TLS-N proof of his bank statement but censor his actual bank account balance. He can then provide a zk-SNARK stating that his balance is above some threshold value. Since the TLS-N proof contains a signature of the bank, the verifier is convinced of the origin of the bank account information but since the sensitive content is hidden, he does not receive any unnecessary information.

D. Applicability to future TLS versions

As we have argued through this paper, previous are insufficient as they rely on specific features of outdated TLS versions. This raises questions about the future applicability of TLS-N. We clearly cannot predict the future development of TLS. However, in contrast to TLSnotary that relied on very specific algorithms, TLS-N uses the generic security primitives of TLS 1.3 and does not depend on their exact implementation. As an example, TLS-N works with any strong cryptographic hash function.

VIII. Conclusion

In this paper we present TLS-N, the first efficient and privacy-preserving TLS extension that provides non-repudiation of a TLS conversation based on content extraction signatures. Our flexible, parametrized design allows the trade-off between efficiency and privacy, being especially efficient if privacy is not required. No trusted third party or trusted hardware is required while the security assumptions of TLS are inherited and TLS primitives are reused.

Our real-world evaluation including recorded traffic and an Apache Server module demonstrate the usability. For smaller requests, such as API calls, the extra latency is less than 1.5 ms. This secure and efficient non-repudiation solution for TLS will enable parties to provably share the vast amounts of content accessible through TLS — and thus provide disintermediation leading to more trustworthy and decentralized services.

In the future we plan to provide an RFC for TLS-N and also aim to resolve the issue of certificate chain verification on the blockchain. Furthermore, we plan to demonstrate how TLS-N can be used to generate proofs for complex websites whose content is transferred through multiple, parallel TLS connections.

Acknowledgment

In addition to the peer reviewers, the authors would like to thank the following people in no particular order for their assistance in this project: Manu Drijvers, Malte Göller, Kari Kostiainen and Simon Meier.

This work was partially supported by the Zurich Information Security & Privacy Center (ZISC).

References

[1] I. J. 1, "ISO/IEC 13888-1:2009," 2009, Information technology - Security techniques - Non-repudiation - Part 1: General.

[2] I. Archive, "Wayback machine," https://archive.org/web/, 2017, accessed: 2017-05-19.

[3] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, *SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 90–108. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40084-1{_}6

[4] A. Beregszaszi, "Ethereum ecverify," 2016, https://gist.github.com/axic/5b33912c6f61ae6fd96d6c4a47afde6d.

[5] M. Brown and R. Housley, "Transport layer security (tls) evidence extensions," Working Draft, IETF Secretariat, Internet-Draft draft-housley-evidence-extns-01, November 2006, https://tools.ietf.org/html/draft-housley-evidence-extns-01. [Online]. Available: https://tools.ietf.org/html/draft-housley-evidence-extns-01

[6] C. Brzuska, H. Busch, O. Dagdelen, M. Fischlin, M. Franz, S. Katzenbeisser, M. Manulis, C. Onete, A. Peter, B. Poettering, and D. Schröder, "Redactable signatures for tree-structured data: Definitions and constructions," in *Proceedings of the 8th International Conference on Applied Cryptography and Network Security*, ser. ACNS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 87–104. [Online]. Available: http://dl.acm.org/citation.cfm?id=1894302.1894310

[7] C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schröder, and F. Volk, *Security of Sanitizable Signatures Revisited*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 317–336.

[8] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "Openpgp message format," Tech. Rep., 2007.

[9] Christian Heimes, "mod_nss," 2017, Available from: https://pagure.io/mod_nss.

[10] ——, "mod_nss branch TLS 1.3," 2017, https://pagure.io/fork/cheimes/mod_nss/branch/tls13.

[11] P. T. Devanbu, M. Gertz, C. U. Martel, and S. G. Stubblebine, "Authentic third-party data publication," in *Proceedings of the IFIP TC11/ WG11.3 Fourteenth Annual Working Conference on Database Security: Data and Application Security, Development and Directions*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2001, pp. 101–112. [Online]. Available: http://dl.acm.org/citation.cfm?id=646118.758638

[12] T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug. 2008. [Online]. Available: https://rfc-editor.org/rfc/rfc5246.txt

[13] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theor.*, vol. 29, no. 2, pp. 198–208, Sep. 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.1983.1056650

[14] M. Fang, "Former Trump Adviser Roger Stone Admits Collusion With WikiLeaks, Then Deletes It," 2017, Available from: http://www.huffingtonpost.com/entry/roger-stone-donald-trump-julian-assange_us_58bc24cae4b0d2821b4ec16c.

[15] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, no. 4, pp. 792–807, Aug. 1986. [Online]. Available: http://doi.acm.org/10.1145/6490.6503

[16] A. Haeberlen, P. Kouznetsov, and P. Druschel, "Peerreview: Practical accountability for distributed systems," in *ACM SIGOPS operating systems review*, vol. 41, no. 6. ACM, 2007, pp. 175–188.

[17] I. Hajjeh and M. Badra, "TLS Sign," Working Draft, IETF Secretariat, Internet-Draft draft-hajjeh-tls-sign-04, December 2007, https://tools.ietf.org/html/draft-hajjeh-tls-sign-04. [Online]. Available: https://tools.ietf.org/html/draft-hajjeh-tls-sign-04

[18] D. Hardt, "The oauth 2.0 authorization framework," Internet Requests for Comments, RFC Editor, RFC 6749, October 2012, http://www.rfc-editor.org/rfc/rfc6749.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt

[19] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your ps and qs: Detection of widespread weak keys in network devices," in *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. Bellevue, WA: USENIX, 2012, pp. 205–220. [Online]. Available: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger

[20] S. Herda, "Non-repudiation: Constituting evidence and proof in digital cooperation," *Computer Standards & Interfaces*, vol. 17, no. 1, pp. 69 – 79, 1995. [Online]. Available: http://www.sciencedirect.com/science/article/pii/092054899400044H

[21] S. S. Imitator, "Fake Twitter Tweet," 2017, http://simitator.com/generator/twitter/tweet.

[22] R. Johnson, D. Molnar, D. X. Song, and D. Wagner, "Homomorphic signature schemes," in *Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology*, ser. CT-RSA '02. London, UK, UK: Springer-Verlag, 2002, pp. 244–262. [Online]. Available: http://dl.acm.org/citation.cfm?id=646140.680938

[23] H. Krawczyk, *Cryptographic Extraction and Key Derivation: The HKDF Scheme*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 631–648. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14623-7_34

[24] A. Kundu and E. Bertino, "Structural signatures for tree data structures," *Proc. VLDB Endow.*, vol. 1, no. 1, pp. 138–150, Aug. 2008. [Online]. Available: http://dx.doi.org/10.14778/1453856.1453876

[25] S. Lerner, "Renegotiation and TLSNotary," IETF TLS mailing list, 2015, Available from: https://mailarchive.ietf.org/arch/msg/tls/8ZK37bSWPvHf0p0X9nFzVAoT-04.

[26] O. Limited, "Oraclize - blockchain oracle service, enabling data-rich smart contracts," http://www.oraclize.it, 2017, accessed: 2017-05-19.

[27] S. B. LLC, "Bitcoin.com composite price index (bcx) — documentation," 2017, https://index.bitcoin.com/.

[28] L. Lo Iacono and H. V. Nguyen, *Authentication Scheme for REST*. Cham: Springer International Publishing, 2015, pp. 113–128. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-19210-9_8

[29] D. McGrew, "An interface and algorithms for authenticated encryption," Internet Requests for Comments, RFC Editor, RFC 5116, January 2008, http://www.rfc-editor.org/rfc/rfc5116.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5116.txt

[30] R. C. Merkle, *A Digital Signature Based on a Conventional Encryption Function*, 1988.

[31] G. Mezzofiore, "All the reasons why that james comey's 'pee tape' tweet is fake," 2017, http://mashable.com/2017/05/10/james-comey-fake-tweet-pee-tape-debunk/.

[32] A. Miller, M. Hicks, J. Katz, and E. Shi, "Authenticated data structures, generically," *SIGPLAN Not.*, vol. 49, no. 1, pp. 411–423, Jan. 2014. [Online]. Available: http://doi.acm.org/10.1145/2578855.2535851

[33] Mozilla, "Network Security Services," 2017, Available from: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS.

[34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[35] E. Nygren, S. Erb, A. Biryukov, D. Khovratovich, and A. Juels, "TLS Client Puzzles Extension," Internet Engineering Task Force, Tech. Rep., Dec. 2016. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-nygren-tls-client-puzzles-02

[36] OANDA, "Exchange Rate API for Businesses and Corporates," https://www.oanda.com/solutions-for-business/feed.html, 2017, accessed: 2017-05-19.

[37] J. A. Onieva, J. Lopez, and J. Zhou, *Secure Multi-Party Non-Repudiation Protocols and Applications*, ser. Advances in Information Security. Springer, 2009, vol. 43. [Online]. Available: http://dx.doi.org/10.1007/978-0-387-75630-1

[38] B. Palmer, "Did Bernie Sanders really dare Trump to send protesters? It's not on Twitter. Deleted or hoax?" 2016, Available from: http://bit.ly/1MgB9Ol.

[39] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-tls-tls13-18, October 2016, https://tools.ietf.org/html/draft-ietf-tls-tls13-18. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-tls13-18

[40] R. Steinfeld, L. Bull, and Y. Zheng, "Content extraction signatures," in *Proceedings of the 4th International Conference Seoul on Information Security and Cryptology*, ser. ICISC '01. London, UK, UK: Springer-Verlag, 2002, pp. 285–304. [Online]. Available: http://dl.acm.org/citation.cfm?id=646283.687991

[41] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full sha-1," 2017, https://shattered.io/static/shattered.pdf.

[42] TLSnotary, "TLSnotary - a mechanism for independently audited https sessions," 2014, available from: https://tlsnotary.org/TLSNotary.pdf.

[43] Trustworthy Internet Movement, "SSL Pulse," 2017, Available from: https://www.trustworthyinternet.org/ssl-pulse/.

[44] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014.

[45] XE, "XE Currency Data Feed," http://www.xe.com/datafeed/, 2017, accessed: 2017-05-19.

[46] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 270–282. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978326

[47] J. Zhou and D. Gollmann, "Evidence and non-repudiation," *Journal of Network and Computer Applications*, vol. 20, no. 3, pp. 267 – 281, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804597900564