Social Threats Modelling with *i**

Lin Liu[1], Eric Yu[2], Gul Jabeen[1]

[1]School of Software, Tsinghua University, Beijing, China
[2]School of Information, University of Toronto, Toronto, Canada
linliu@tsinghua.edu.cn,
eric.yu@utoronto.ca,
gul.jabeen@kiu.edu.pk

Abstract Security incidents lead to loss or disruptions of an organisation's operations, services or functions, or reductions in the quality of the expected services. For any security incident, there is an individual or a group of attackers, conducting the attack action, towards one or many victims. The two sides are played by social actors, with certain social positions, protecting or obstructing a given operations, services functions with certain techniques. In this paper, we propose a meta-model that aims to capture the act of attackers and the counter-act of the victims using social concepts in *i**. Such act vs. counteract, attack vs. protection situation is inherently socio-technical. By compensating existing tactical analytic frameworks on security, an important dimension of the problem space is tackled, which leads to the identification of effective solutions systematically that are otherwise by coincidence.

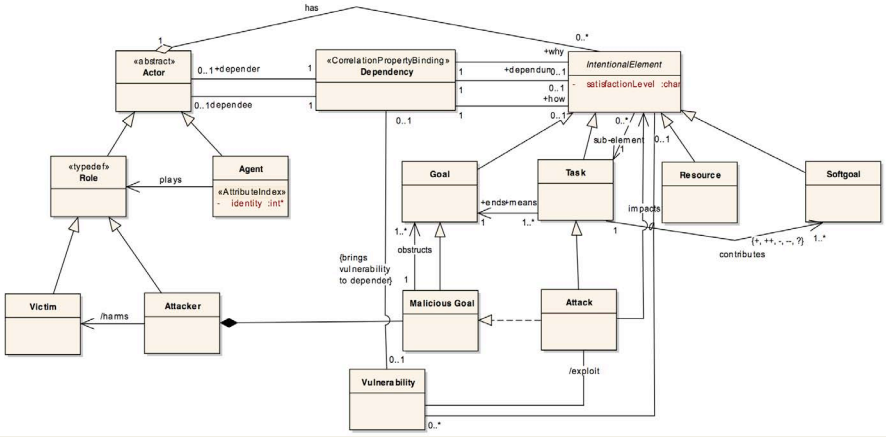
Keywords: security, requirements, modeling, UML profile, *i** framework

1 Introduction

In the cybercrime research, the subject of attackers and their motivations are studies in depth [11]. Security threat modelling is a socio-technical problem, where the social aspects are often neglected in the literature [3]. Security is a critical non-functional requirements that *i** can help model and yield interesting reasoning results [1]. This includes the elicitation of the social relations involved in the problem domain, the identification of vulnerable dependencies, the potential attacks violating committed social contracts, the possible counter-measures that can partially or fully disable potential threats. Many techniques were proposed for dealing with security requirements, including scenario-based approaches [13], UML-based approaches[12], and goal-oriented approaches [7, 8] that are treating security requirements as anti-goals or obstacles [6], or abuse frames [4] or security taxonomies[2], ontologies [10] and patterns [9]. Each of these approaches covers a different aspect of security requirements modelling, amongst which *i** covers the social strategic angle that complements existing approaches.

This paper revisits the social modelling concepts in *i**, and proposes a meta-model and examines its expressiveness when dealing with the general threats use cases. Its sufficiency as standard threats modelling language is examined and possible future direction is discussed. A model as such adopts meta-model concepts such as: role, agent, actor, and security modelling concepts are: attacker, victim. Actor is the first class concept in the social modelling of security. There are two subclasses of actor, one is role, which covers the abstract behavioral patterns in a given domain; the other one is agent, which covers the concrete physical entities related to real systems context, who plays roles in different setting. There are two types of roles we are concerned about in the security setting, one is the attacker, and the other is the victim of attacks. An attacker usually has malicious goals or intents. Malicious goal is a subclass of goal, which obstructs at least one other goal. Attacks are means to realise malicious goals, which is defined as a task in *i**. It means that an attack is composed of a certain procedure, may require certain resource, sub-goal, sub-task, or

softgoal. It is made successful as an attacker finds a viable way through the social dependency network of "role-playing", "task-decomposition", "means-ends" and "contribution" links. A social vulnerability is defined as a subclass of dependency, which brings vulnerability to a depender as the attacks are propagated through vulnerable dependencies.



1) For ALL x in Actor, y in Resource, z in Attack,
   Role-Play (Attacker, x) AND HAS-ACCESS(x, y) AND COMMIT(x, z)
   => Exist x' in Actor, Role-Play(Victim, x') AND LOSS (x', y, z);
2) For ALL x in Actor, y in Resource, WithinBoundary(x, y) => HAS-ACCESS(x, y);
3) For ALL x in Actor, y, y' in Resource, WithinBoundary(x, y) AND ISA(y, y')
   => WithinBoundary(x, y') ;
4) For ALL x, x' in Actor, y in Resource, WithinBoundary(x, y) AND (ISA(x, x') OR IS-Part-Of(x, x'))
   => WithinBoundary(x', y)
5) For ALL x in Actor, z in Attack, COMMIT(x, z) => WithinBoundary(x, z)

Fig. 1. Meta-model and formalisms of cyber security from an actor's viewpoint

2 Threat Modeling Use Case I: Corporate Information Security

We use two threats modelling use cases to examine the modelling capability of the above meta-model.

Here is a description of the first one: A multi-national company with multiple datacenters, office facilities, and international business activity. Offices and data centers are located in the US, Europe, APAC. Some facilities are in countries with conflict of interests. Employees include citizens across all locations. Some data centers are hosted by a co-location provider with external security staff. Turnover of staff is within normal ranges. There are active use of contractors and other external partners, and a large number of deployed security systems, sensors. Information Security systems includes: Access control through directory, but large number of services that are not integrated; Basic endpoint security systems for most servers and laptops; Firewalls; Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Security Information and Event Management (SIEM); Systems monitoring; Physical Security systems. Basic physical access control: Video monitoring of sensitive areas; Intrusion detection; Commercial fire alarms and suppression; Notification/alerting for critical events (through SMS, email, etc.) On call staff includes skeletal 24/7-support team, some on-call staff for escalation, External guards.

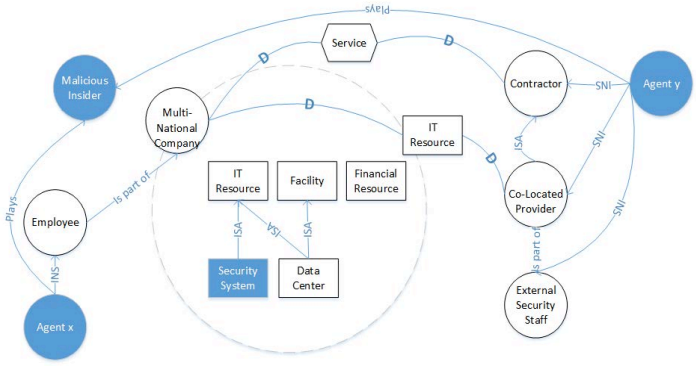


Fig. 2. Modelling Actors and Assets in the Problem Context

As the *i** model in Fig. 2 shows, actors are used to represent the different players in the problem setting, in this particular scenario, we are interested in understanding the security situations of the multi-national company with certain assets that is considered valuable and requires protection. There are five types of actors defined: the multi-national company under discussion, its employee, who is connected with the company with "is-part-of" link. There are also contractors, who are not considered as part of the company, but are relied upon on certain services. When some data centers are hosted by some co-located provider, these provider are actually subclasses of contractors, who may hire external security Staff. Assets are represented as resources, internal resources are owned by the company, so we use actor boundary to indicate such ownership relationship. External resources are not owned, but are dependums that linked to the actual owner or provider. A variety of potential attack scenarios can be played out against the company by attackers, including external and internal attacks. While there is a reasonable security program in place, the company is not able to ensure full in-depth security across all systems and assets for the following reasons. In these scenarios the following strategies are employed:

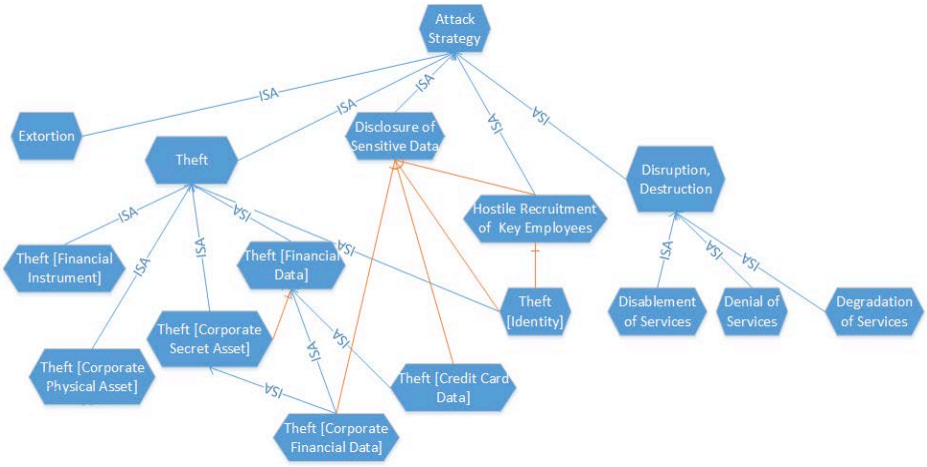


Fig. 3. Modelling Attack Strategies using Class Hierarchy and Task Decomposition

Potential adversaries may include: Cyber criminals, including organized crime (domestic and foreign); Competitors; Malicious Insiders: Disgruntled employees and contractors; Hostile Investors: Potential corporate or individual acquirers of company; Nation state adversaries (unlikely, unless company engages in critical infrastructure or national defense, etc.); Terrorist Organizations. Combating cyber threats will call for a classification that exploits the very foundation of crime itself - motivation. Until attack is seen from the view of motivation for the criminals themselves, efforts to battle it will

not yield their full promise. Cyber criminals are driven by time-honored motivations. Spotting these motivations could be an essential key to find a holistic solution. Not much research has looked into this important aspect of threats classification. Main Strategies in the example case are:

- Identity Theft: the attacker attacks the end user systems or the corporate assets to obtain the identities of primarily the end users.
- Financial Data Theft: the attackers obtain sensitive financial information about end-users or other entities from corporate assets.
- Extortion/Ransom: the attacker obtains the ability to affect corporate assets negatively (e.g. through denial, destruction, disruption, degradation, distortion, data exfiltration, etc.) and blackmail the company. The company pays a ransom to avoid negative consequences.
- Money/Financial Instrument Theft: this is traditional direct theft of money, or similar financial instruments that can immediately be sold.

Role of the Malicious Insider is that the insider is simply an agent assisting the main actors in executing their attacks. The insider may be motivated by any reason. For the case of money theft, the malicious insider can be a main actor. Possible queries can be answered based on the model in Fig. 4:

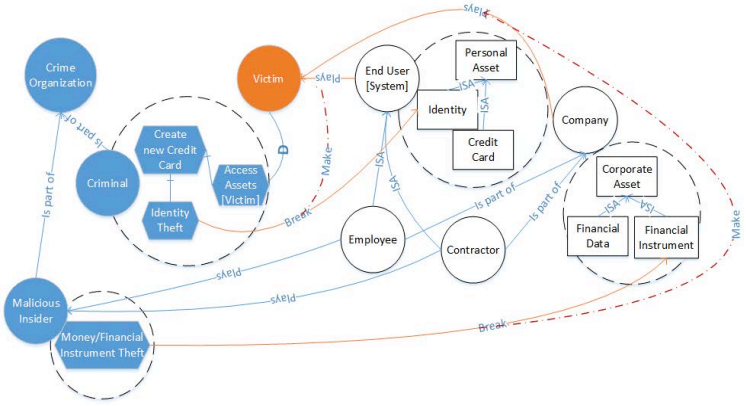


Fig. 4. Strategic Rationale Modelling of the Attackers in Financial Gain Scenario

An Example Query to the formalism in Fig.1 is:
Given x, x' in Actor, z in Attack,
if Role-Play (Attacker, x) AND HAS-ACCESS(x, Identity(x')) AND COMMIT(x, z)

What will happen? By applying rule 1, 2, 5, we can derive the following result:
Role-Play(Victim, x') AND { For All y in Resource, WithinBoundary(x', y) => LOSS(x', y, z)}.

3 Threat Modeling Use Case II: Ransomware Modelling

A ransomware is the new form of cybercrime, which victimizes Internet users by hijacking user files, deleting files from the system, encrypting files and demanding payment in exchange for the decryption key. Ransomware always tries to grab control over the victim's files or computer until the victim agrees to the attacker's demands. It searches different file extension such as .txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, etc. It encrypts the data file of the user by using malicious code. The malicious code should be deleted after encrypting the files. Then it hides the files of system, and generates static pop up menus in to the system that cannot be removed from the system. The ransomware propagates itself in to the system by email spam, or by web files downloading, or via external devices. It is only detected

when a user is not able to access his files, or when a user gets messages informing him that his data has been encrypted. So far, there is no perfect mechanism to build a perfect system to detect ransomware. A system can be easily targeted if it is already attacked by any malware. The following are the main vulnerabilities in user system: careless browsing, browser weaknesses, no up to date antivirus protection, download unknown email attachments, pop up menu is enabled. We use i* models to capture the above scenario in Fig. 5 below.

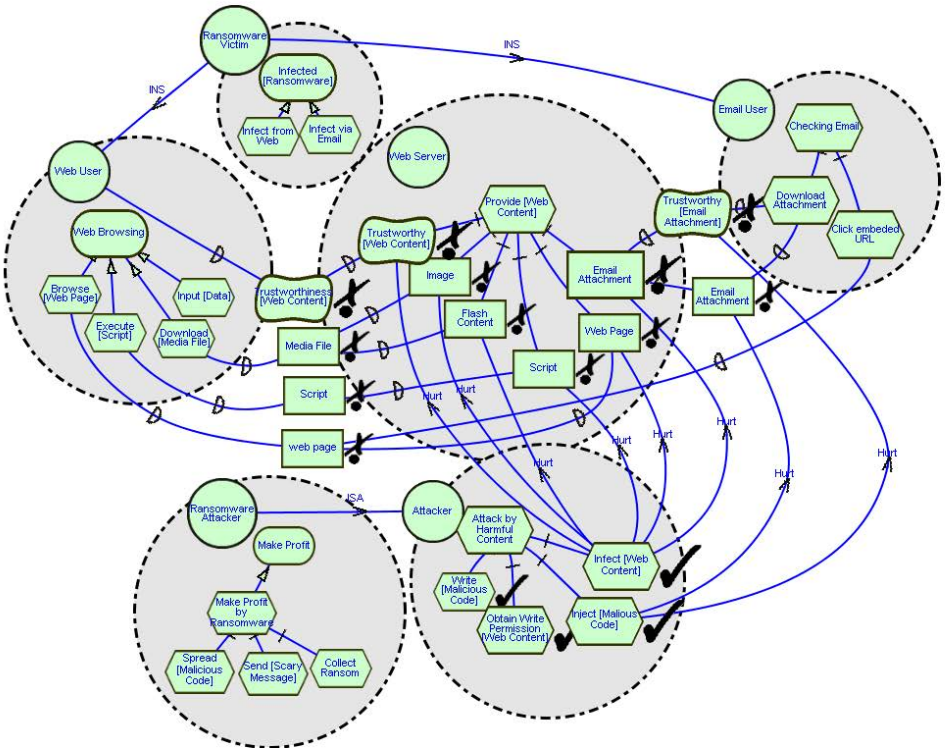


Fig. 5. Strategic Rationale Modelling of the Attackers in Ransomware (Partial)

4 Discussions

From the modelling examples above, we conclude that in order to describe the different threats with different causes and impacts, a context model of the attack is needed, which involves social modeling of the attack, especially for intentional attacks. In order to limit the negative impact of the incident, we need to identify vulnerabilities in the social infrastructure, and to take actions to prevent threats from happening in future, or to reduce potential loss of a current one, or to recover from a past event, where a social modelling approach will help work out a viable solution from the social dependency perspective. It includes: building and evaluating social dependency relationships network at the macro level, and select the best personal/organization for a certain social role at the micro level. This can be turned into a social modeling profile of UML with built-in reasoning abilities. It can further implemented as managerial guidelines or information systems functionalities.

Acknowledgments. Partial Financial support by Natural Science Foundation of China project (no. 61432020) is acknowledged.

References

[1] Elahi G, Yu E, Zannone N. A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations[C]//International Conference on Conceptual Modeling. Springer Berlin Heidelberg, 2009: 99-114.

[2] Firesmith D G. A taxonomy of security-related requirements[C]//International Workshop on High Assurance Systems (RHAS'05). 2005.

[3] Myagmar S, Lee A J, Yurcik W. Threat modeling as a basis for security requirements[C]//Symposium on requirements engineering for information security (SREIS). 2005, 2005: 1-8.

[4] Lin L, Nuseibeh B, Ince D, et al. Using abuse frames to bound the scope of security problems[C]//Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International. IEEE, 2004: 354-355.

[5] Souza V E S, Mylopoulos J. Monitoring and diagnosing malicious attacks with autonomic software[C]//International Conference on Conceptual Modeling. Springer Berlin Heidelberg, 2009: 84-98.

[6] Van Lamsweerde A. Elaborating security requirements by construction of intentional anti-models[C]//Proceedings of the 26th International Conference on Software Engineering. IEEE Computer Society, 2004: 148-157.

[7] Li T, Horkoff J, Paja E, et al. Analyzing Attack Strategies Through Anti-goal Refinement[C]//IFIP Working Conference on The Practice of Enterprise Modeling. Springer International Publishing, 2015: 75-90.

[8] Dalpiaz F, Paja E, Giorgini P. Security Requirements Engineering: Designing Secure Socio-Technical Systems[M]. MIT Press, 2016.

[9] Schumacher M, Fernandez-Buglioni E, Hybertson D, et al. Security Patterns: Integrating security and systems engineering[M]. John Wiley & Sons, 2013.

[10] Souag, Amina, Camille Salinesi, and Isabelle Comyn-Wattiau. "Ontologies for security requirements: A literature survey and classification." International Conference on Advanced Information Systems Engineering. Springer Berlin Heidelberg, 2012.

[11] Gordon S, Ford R. On the definition and classification of cybercrime[J]. Journal in Computer Virology, 2006, 2(1): 13-20.

[12] Jürjens J. Secure systems development with UML[M]. Springer Science & Business Media, 2005.

[13] Sindre, G., Opdahl, A.L.: Eliciting security requirements with misuse cases. Requirements Engineering 10(1) (2005) 34–44.