Storytelling for Tackling Organized Cybercrime

Muhammad Adnan Tariq
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
tari@kth.se

Joel Brynielsson
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
joel@kth.se

Henrik Artman
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
artman@kth.se

Cybercrime is often organized, and the actual individuals that are perpetrating the different parts of the attack might not be aware of or interested in the overall organizational motives behind the attack. In this paper, based on interviews with IT security experts, we build on the attacker persona methodology and extend it with methodology to also handle organizational attacking motives in order to tackle organized cybercrime. The resulting framework extends the attacker persona methodology by also using narratives in order to assess the own organization's security. These narratives give rise to intrigue sketches involving any number of attacker personas which, hence, make it possible to take organized cybercrime into account.

Organized cybercrime, narrative, attacker persona, intrigue sketch

1. INTRODUCTION

From a user perspective, the problem of not being able to effectively apply security mechanisms is twofold: lack of usability in the security mechanism itself (Zurko and Simon 1996; Zurko 2005) and lack of user engagement due to not understanding the implications of bypassing a security mechanism (Platt 2006). As an example, Whitten and Tygar (1999) highlighted how users were unable to understand the security mechanism (PGP 5.0) which eventually lead to confidential data being sent in the clear. Similarly, users are in most cases not well aware about the consequences of their actions which can lead to devastating results (Adams and Sasse 1999; Fléchais and Sasse 2009).

Consequently, there is a need for a framework to be used for enlightening the user/defender about the attacker perspective (Brynielsson 2009), and enable them to specify security-centric requirements in their context of use. However, in order to do this one must have some representation of the threats and the actual actors who might pose the threat. Still, such criminal actors are likely to be hard to find and even harder to interview. In this paper we follow-up on recent work (Atzeni et al. 2011) and propose a solution based on the persona methodology.

2. ORGANIZATIONAL SECURITY ASSESSMENT

The elastic nature of the general and routine-like use of the term user as identified by Cooper (2004) is being acknowledged by many researchers and forms the basis for the use of personas in systems development. However, we argue that problems, and explicitly security problems, can be as elastic, especially in terms of assessing the organizational security. As an example, consider a situation where a user somehow downloaded a malicious file from the Internet. This whole activity points towards multiple factors which could have resulted in the download of that file. Such factors typically represent inadequacies with regard to, e.g., the security policy, the security mechanism, the user awareness, and so forth. The security problem in itself is elastic and depends not only on a single factor, but rather upon multiple factors. In this paper, a *narrative* is taken to be an indicator pointing towards such factors.

To further elaborate on the narrative property, consider the known analogy of the elephant and the six blind men. The blind men come across an elephant; by feeling different parts of the elephant each individual tries to describe what they perceive: they will all describe the elephant in various, and probably different, ways depending on if they have encountered the tail, the ears, the legs, the proboscis, or any other part of the elephant. This situation highlights that any complex and large problem being immediately perceived by an individual may elicit many different descriptions. In terms of an organization, the elephant represents the security-critical issues/problems, e.g., the download of a malicious file, and the blind men denote the different stakeholders. The perceptions of these stakeholders are the narratives, and each stakeholder might be able to describe an event or activity using a number of narratives. The narrative provides us with potential causes of an event, and with multiple people providing their narratives it becomes easier to identify overall security holes. Of course, the most predominant cause of the security issue will have an overlapping effect among the collected narratives. This overlapping between narratives will identify the major loop holes, and the collection of narratives will incorporate factors which one individual was unable to identify. Thus, the collection of narratives encompasses multiple factors and provides insight into the cause of the security problem from different angles.

2.1. Organized cybercrime and personas

Recent trends in the IT security landscape suggest that organized cybercrime has become part of the everyday cyber landscape with criminal groups using cybercrime to achieve their goals (McCusker 2006; Choo and Smith 2008). Moreover, McCombie and Pieprzyk (2010) suggest that there are cases where groups of cybercriminals have used extortion, black-mailing, and online fraud to achieve their desired goal. To map such an organization into a persona is a challenge due to the inadequacy of observable data about organizational culture, environment, hierarchical structure, communication, etc. Furthermore, the persona methodology is designed towards convergence of a group of individuals with more or less similar motivations, goals, skills, behavior, etc., into a single personification. To overcome these issues, the persona methodology needs to be extended to provide insight into such critical issues. However, there has been work carried out to capture the group or organizational aspect of persona (Giboin 2011; Judge et al. 2012; Matthews et al. 2011), but personification of a group of attackers has its limitation mainly due to the secret nature of such organizations.

3. FRAMEWORK

In this section we present our framework, which is an attempt to highlight the organizational security threats while extending the persona methodology. The framework comprises 1) narratives, 2) attacker personas (including scenarios), 3) intrigue sketches, and 4) plots. Narratives have already been discussed while this section serves to describe attacker personas, intrigue sketches and plots.

3.1. Attacker personas

Personas is a method for highlighting end users and their needs of a system (Cooper 2004). Since personas can be used to replace direct user participation its usefulness has been questioned by some people (Grudin 2006; Portigal 2008). However, others argue that this is its actual strength since actual user involvement in the design can be perceived as a hinder due to idiosyncratic demands of the real users (Cooper 2004; Grudin 2006). By representing the attackers as personas we can get an understanding of the complex ways attackers might work. This introduces problems as we cannot interview actual attackers. Atzeni et al. (2011) have dealt with this problem by using assumptions of their character while collecting data from sources such as attacker taxonomies, profiling, and knowledge elicitation workshops. However, Tariq et al. (2012) argue that the personas should be context independent as security is not a single context problem: in fact, each security issue has multiple contexts, especially in terms of organizations. De-attaching the context from the attacker personas gives the flexibility to use attacker personas in multiple contexts. That is, we do not argue against a context bound framework but argue against an attacker persona that is bound to specific contexts or specific systems. Rather, we perceive attacker personas as a collection of threats to an organization.

Scenarios are part of the persona methodology and are used to describe the sequential activities that a user undertakes to reach a specific goal. We have used the concept of scenarios, as discussed by Quesenbery (2006), and applied it in terms of attacker activities, i.e., we have developed a set of small stories which emphasize how a specific attacker in the past has attacked several organizations to achieve their goal. However, these stories do not provide a detailed step by step approach to describe an attack, but rather provides a high-level description of the attack. The aim of using the scenarios is to provide a basic understanding of how an actual attacker could operate and which weaknesses that might be exploited by the attacker. This information is particularly helpful while analyzing the narratives and relating them with the attacker personas. Hence, the idea of presenting this information is to provide a guideline so that the narrative can be related to the personas and scenarios while developing *intrigue sketches*, which will be discussed further in the following section.

3.2. Intrigue sketches

Before we define the intrigue sketch it is necessary to understand why we need intrigue sketches. As discussed in Section 3.1, our personas are context independent so in order to put them in an organizational context we need to relate them to organizational-specific narratives. In practice, this process consists of a systematic interpretation of the narrative in terms of attacker personas. The interpretation can mainly be carried out by someone who has a good understanding of IT security, and thus the security analyst is part of the process. This interpretation of a narrative in terms of personas enables one to understand the problem identified by the narrative from an IT security viewpoint. Also, taking this attacker perspective could help determining the overall motivations and goals behind an attack, which might lead to identifying organized cybercrime activity by looking at multiple intrigue sketches, which will be discussed further below.

The intrigue sketches make use of narratives, security analysts and attacker personas with scenarios. Both the narrative and the attacker personas have some attributes in common which are mainly goals, motivations, and skills. The narrative incorporates these aspects from the respondent perspective, e.g., how a certain event took place, which critical asset was targeted, and so forth. Similarly, each persona contains a set of goals, motivations, and skills. When these attributes, derived from a narrative and the corresponding attacker personas, are related with each other by a security analyst/expert the result is an intrigue sketch. The intrigue sketch holds information about the relevant attacker or attackers, possible attack procedure (derived from the corresponding attacker persona scenario), motivations, and goals. The intrigue sketch development process can be seen as a way to combine the attacker perspective (personas with scenarios), the respondent perspective (narrative) and the security perspective (the security analyst) in order to understanding the multidimensional aspects of security. For the development of the overall framework, it should also be emphasized that each intrigue sketch will contain at least one persona, but can of course contain more depending on the narrative. To make sense of the intrigue sketches in terms of the organizational perspective, each intrigue sketch should be classified mainly on the basis of the attacker's goals and in some cases the combination of both goals and motivations. This classification of the intrigue sketches will prove necessary in the next phase of the framework, which is the creation of *plots*.

3.3. Plots

The plot is the last part of the framework, which describes the overall security of the organization by relating intrigue sketches with the existing security practices being used by the organization. Each intrigue sketch can be related with the existing security practices of the organization either individually or collectively to point out threats to the organization. However, using intrigue sketches individually may result in ignoring the multidimensional aspect of security. On the other hand, however, there could be a case where the intrigue sketch represents an isolated attacker's activities. In such case, the plot will comprise of a single intrigue sketch related with the organizational practices to identify potential threats. A collective usage of the intrigue sketches will provide a holistic view of the organizational security. To achieve this it is critical that the intrigue sketches are specified so that it is easy to identify the overlapping among them. This problem is solved by the specification of intrigue sketches in terms of goals and motivations, as mentioned earlier. The intrigue sketches can be related by using a combination of both goals and motivations, e.g., attackers who are trying to steal critical information and are ideologically motivated can be clustered together, etc.

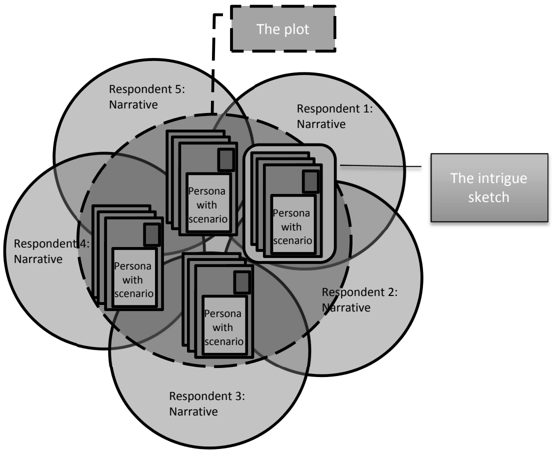

Figure 1: *The complete framework consists of different narratives that are collected from the respondents in the organization, which are then being related with attacker personas with scenarios in order to develop intrigue sketches, which are finally brought together with existing organizational practices to develop the overall plot.*

Once the intrigue sketches have been synthesized they can be related to existing organizational practices, which will result in an assessment of the existing security practices of the organization and eventually identify threats that the organization might face. However, it should be mentioned that the number of plots will depend upon the number of intrigue sketch syntheses, i.e., the intrigue sketches might result in one espionage synthesis and one mafia synthesis which, when related with the organizational practices, will yield two different plots since they represent two separate kinds of attacks. To finally tackle the organized cybercrime threat, the attacker personas can be related from an organized cybercrime perspective based on their goals and motivations to find out whether the attacker personas represent individual attackers or are part of an organized criminal activity. To summarize, see Figure 1 where the framework constituents have been put in perspective to each other.

4. CONCLUSIONS

We have presented a framework to be used for understanding the IT security environment in an organization. The framework highlights possible inconsistency in terms of understanding the requirements and expectations from an organizational perspective. Also, the framework is an effort to assess the organizational security from multiple perspectives by extending the persona methodology. We have presented attacker personas such that they are context independent and are used to incorporate the organized cybercrime perspective. The major contribution is the intrigue sketch which is the combination of a respondent's narrative, generic attacker personas and a security specialist's assessment. The intrigue sketch sets a scene for the possibility to frame one or several attackers in a specific situation.

REFERENCES

Adams, A. and M. A. Sasse (1999, December). Users are not the enemy. *Communications of the ACM*, 42(12), pp. 40–46.

Atzeni, A., C. Cameroni, S. Faily, J. Lyle, and I. Fléchais (2011, August). Here's Johnny: a methodology for developing attacker personas. In *Proceedings of the Sixth International Conference on Availability, Reliability and Security (ARES 2011)*, Vienna, Austria, pp. 722–727.

Brynielsson, J. (2009, March). An information assurance curriculum for commanding officers using hands-on experiments. *ACM SIGCSE Bulletin*, 41(1), pp. 236–240.

Choo, K.-K. R. and R. G. Smith (2008, June). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology*, 3(1), pp. 37–59.

Cooper, A. (2004). *The Inmates Are Running the Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity* (2 ed.). Indianapolis, IN: Sams Publishing.

Fléchais, I. and M. A. Sasse (2009, April). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human-Computer Studies*, 67(4), pp. 281–296.

Giboin, A. (2011, February). From individual personas to collective personas. In *Proceedings of the Fourth International Conference on Advances in Computer-Human Interactions (ACHI 2011)*, Guadeloupe, France, pp. 132–135.

Grudin, J. (2006). Why personas work: The psychological evidence. In J. Pruitt and T. Adlin (Eds.), *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*, San Francisco, CA: Morgan Kaufmann. Chapter 12, pp. 642–663.

Judge, T., T. Matthews, and S. Whittaker (2012, May). Comparing collaboration and individual personas for the design and evaluation of collaboration software. In *Proceedings of the 30th Conference on Human Factors in Computing Systems (CHI 2012)*, Austin, TX, pp. 1997–2000.

Matthews, T., S. Whittaker, T. Moran, and S. Yuen (2011, May). Collaboration personas: A new approach to designing workplace collaboration tools. In *Proceedings of the 29th Conference on Human Factors in Computing Systems (CHI 2011)*, Vancouver, Canada, pp. 2247–2256.

McCombie, S. and J. Pieprzyk (2010, July). Winning the phishing war: A strategy for Australia. In *Proceedings of the Second Cybercrime and Trustworthy Computing Workshop (CTC 2010)*, Ballarat, Australia, pp. 79–86.

McCusker, R. (2006, December). Transnational organised cyber crime: distinguishing threat from reality. *Crime, Law and Social Change*, 46(4–5), pp. 257–273.

Platt, D. S. (2006). *Why Software Sucks... and what you can do about it.* Boston, MA: Addison-Wesley.

Portigal, S. (2008, January–February). True tales: Persona non grata. *interactions*, 15(1), pp. 72–73.

Quesenbery, W. (2006). Storytelling and narrative. In J. Pruitt and T. Adlin (Eds.), *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*, San Francisco, CA: Morgan Kaufmann. Chapter 9, pp. 520–554.

Tariq, M. A., J. Brynielsson, and H. Artman (2012, August). Framing the attacker in organized cybercrime. In *Proceedings of the IEEE European Intelligence and Security Informatics Conference 2012 (EISIC 2012)*, Odense, Denmark.

Whitten, A. and J. D. Tygar (1999, August). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, Washington, DC, pp. 169–183.

Zurko, M. E. (2005, December). User-centered security: Stepping up to the grand challenge. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005)*, Tucson, AZ, pp. 187–200.

Zurko, M. E. and R. T. Simon (1996, September). User-centered security. In *Proceedings of the 1996 New Security Paradigms Workshop (NSPW'96)*, Lake Arrowhead, CA, pp. 27–33.