Framing the Attacker in Organized Cybercrime

Muhammad Adnan Tariq, Joel Brynielsson, Henrik Artman
Royal Institute of Technology
SE-100 44 Stockholm, Sweden
Email: {tari, joel, artman}@kth.se

***Abstract*—When large values are at stake, the attacker and the attacker's motives cannot be easily modeled, since both the organization at stake and the possible attackers are unique and have complex motives. Hence, rather than using stereotypical attacker models, recent work proposes realistic profiling of the opponent by the use of user-centered design principles in form of the persona methodology.**

Today, cybercrime is often organized, i.e., attacks are planned and executed by an organization that has put together a tailor-made team consisting of the necessary skills for the task. The actual individuals taking part in the attack might not be aware of or interested in the overall organizational motives. Rather, taking motives behind espionage, fraud, etc., into account requires consideration of the attacking organization rather than the individuals. 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 motives in order to tackle organized cybercrime. The resulting framework presented in the paper 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.

***Index Terms*—Organized cybercrime; narrative; persona; intrigue sketch**

I. Introduction

How does one assess an organization's level of security? This can be discussed both in terms of a technical perspective, i.e., considering IT infrastructure, and from a user perspective incorporating more soft issues such as how people protect their information, usage patterns, etc. Ultimately, a high level of security with regard to all forms of intrusions is desirable, but this high level needs to be contrasted to users' needs: a high level of security may be perceived as a hassle resulting in the use of workarounds that are insecure. Another user issue to be considered is that different stakeholders and actors within an organization can have different perception and awareness when it comes to security, which can present security gaps for the security at large.

From a technical viewpoint, one is often focused on making technology as proof and secure as possible. A comprehensive effort has been made to achieve security through such technical means over the years. Mathematically sound cryptographic systems/protocols providing the most basic security services is an example, but when used by humans' the resulting level of security ranges from high to low depending on how it is being used in practice (password management, etc.) In this paper, we emphasize the human aspect of IT security as the most important and dictating feature to be considered in order for a system to provide good enough security. If a user is able to apply a security mechanism in an effective manner, then the mechanism can be considered to be more secure. Similarly, a very strong security policy may become cumbersome for users, which lead Saltzer and Schroeder [1] to propose the principle of being "psychologically acceptable" since then the user-centered design philosophy is gaining momentum. In 1996, the term user-centered security was introduced, which focuses on the need for security mechanisms, models and software to be usable [2]. For the user to be able to apply security in their day-to-day activities, they need to understand security in their own context of use. In [3] the author points to the need to understand user behavior in terms of security in order to improve the security of a system. Further, the author argues that phrasing the system security requirements in terms of user mental models can be beneficial, but that there is no framework that could be applied to achieve such goals. Moreover, Platt [4] emphasizes that every user has a "security budget" and when this budget is exceeded the end result is no security at all. Referring to the principle of least privileges, which suggest that the user should be given sufficient access to perform their day-to-day activities in a secure way, there is also a need for the user to be able to understand the implication of bypassing a security mechanism. The problem is twofold: lack of usability in the security mechanism itself and lack of user engagement due to not understanding the implications of bypassing a security mechanism.

From a user-centered perspective, one often reason about the problems people have with protecting information. Such problems can either be of the mundane kind, such as being unable to remember passwords and as a result writing them down or the users might be unaware of presenting information to the wrong persons. The lack of user involvement can lead to false assumptions about the security mechanism which could eventually lead to compromised/inadequate security, no matter how sophisticated the security mechanism is. As an example, Whitten and Tygar [5] 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, social engineering attacks aim to target the weakest link in the security chain: the users. Since the users are unable to understand the risk of disclosing certain information, this leads to failure of the security mechanism. In fact, emphasizing the human aspects it turns out that users are in most cases not well aware about the consequences of their actions which can lead to devastating results [6], [7]. Consequently, there is a need

978-0-7695-4782-4/12 $26.00 © 2012 IEEE
DOI 10.1109/EISIC.2012.48

for a framework to be used for enlightening the user/defender about the attacker perspective, 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 hard to find, harder to interview, and even harder to reveal. In this paper we follow-up on recent work [8] and propose a solution based on a methodology being highly appreciated within the practical user-centered design community—the persona methodology.

The remainder of this paper is structured as follows. In Section II, relevant background regarding the persona methodology is given. Then, Section III discusses organizational security assessment in general and the organized cybercrime threat in particular. The undertaken methodology is then described in Section IV, followed by a presentation of the resulting personas in Section V. Section VI then proposes and defines a persona-inspired framework which ultimately serves to estimate the overall cybercrime threat. Lastly, Section VII wraps up the paper with some concluding remarks.

II. Personas as a Way to Present Users to Security Designers

Personas is a method for highlighting end users and their needs of a system [9]. A persona is an aggregated character description representing a group of users with similar usage patterns and goals. It is meant to hinder an elastic notion of the end user and help the systems design team to focus on a particular user who, in turn, represents a cluster of consumer needs. It is common to describe several personas for a project, where one persona is the primary persona with goals that should never be compromised. Each persona is described as a short description of a fictive person with name, photo/sketch, age, slogan, a usage scenario, goals, and needs. All descriptive aspects should be coherent and not contest general conceptions of the actual or prospective users. The method is supposed to be based on thorough research of actual usage, and is used to understand and focus on user requirements to communicate these requirements among different stakeholders in a design project. In essence, it is a tool that can be used to capture the user behavior, goals, motivations, and attitude towards a given software product. In the area of human-computer interaction this methodology has been used to aid designers to design towards end users when actual or prospective users are absent. Also, Pruitt and Grudin [10] argue that personas are remarkable in terms of creating a common ground for communication within the organization or the systems development project. Moreover, personas can be used as a tool for educational purposes, especially from the organizational perspective [11].

The use of personas as a methodology has, however, not been thoroughly researched. In addition, it has been rejected by some people since it can be used to replace direct user participation [12], [13]. Others argue that this is its actual strength since actual user involvement in the design work can be perceived as a hinder rather than as a help due to real users might having idiosyncratic demands which is not always shared within a larger group of users [9], [10], [12], [14], [15]. In other cases it might be impossible to involve users because they are unknown or do not have the required time to engage whole-heartily in the project. For this paper, personas are relevant as attackers are generally not known at a personal basis and do not lend themselves to be involved in designing systems which will prevent attacks. When designing against intruders or attackers it might be relevant to have a shared and clear idea of the prospect of the user one is designing against. 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. In [8] this has been dealt with by developing personas by using assumptions of their character. In this paper we introduce the concept of narratives, or storytelling, which puts personas in a general context where motives and goals are based on the situation and surrounding, rather than solely on individual goals. This is in line with Quesenbery who claims that, "the power of storytelling may be the single most important reason why personas work" [15]. According to her, storytelling is an intrinsic part of being human, and we are prone to listen to and learn from narratives. Also, [12] theorize that the underlying psychological reason for the success of personas is a theory of mind in terms of being alert to stories.

A. Assumption and Attacker Personas

Empirical data collection to develop personas is a critical factor. Cooper's [9] persona methodology focuses on acquiring first hand data by observing users though workshops, focus groups and interviews, whereas Pruitt and Grudin [10] argue that developing persona in such a manner is time-consuming and sometimes not feasible. The alternative to this approach is the assumption personas, in which expert opinions regarding a targeted group of users are used rather than observing groups of users. Assumption personas are developed at the start prior to the design phase. The hypothetical perception of the target group of users is captured in the assumption personas. The idea of using assumption personas has been perceived as a quick way to develop and present one's assumption about a specific group of users.

Atzeni et al. [8] have presented attacker personas. They argue that the notions of anti-persona and assumption persona can be used to depict users for whom the system is not being developed for. In the case of attacker personas, Atzeni et al. [8] argue that empirical data collection directly from the user is not feasible. Instead, existing data sources such as taxonomies, profiling and knowledge elicitation workshops about the targeted group of users can act as an alternative. Considering IT security from an attack versus defend viewpoint is a common way to study threats [16], [17], and can provide insightful information about the attackers such as how they carry out attacks, which weaknesses they target the most, the skill of the attacker in terms of the way an attack is carried out, etc. Such data concerning different categories of attackers can be acquired from IT security professionals using quantitative and/or qualitative means. The obtained behavioral

characteristics can then be further incorporated into attacker personas.

The assumption personas presented by Atzeni et al. [8] are context bound. Using such context specific attacker personas means that one needs to develop multiple personas for a single context and for the case of multiple contexts then for each context one should have multiple personas. The problem is that security is not a single context problem: in fact, each security issue has multiple contexts, especially in terms of organizations. It is critical to develop context specific personas when the aim is to design the system for the user but here we are developing personas to design against the general intruders who actually would be able to attack any system. De-attaching the context from the attacker personas gives us the flexibility to use our attacker personas in multiple contexts. That is, we do not argue against a context bound framework but we 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, and in this paper we, in line with [15], present attacker personas in a dynamic and narrative structure. Still, before we can develop a general framework methodology for this effort we need to have an idea of organized cybercrime as a second possible caveat with regard to the persona methodology, which is usually focused on individual needs and behaviors rather than organized team behavior.

III. Security Assessment in Organizations

The elastic nature of the general and routine-like use of the term user as identified by Cooper [9] 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. To further elaborate on the idea, let us consider an example where an employee in an organization somehow downloads a malicious file/code. This activity points towards a number of factors which could eventually 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 complex and depends not only on a single factor, but rather upon multiple factors. In this paper, the gathering of narratives serves to provide basic data for understanding such underlying factors.

A. The Narrative Property

In order to further elaborate on the narrative property, let us 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 and the blind men denote the different stakeholders in the organization. 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. A major issue is, however, how one should connect different narratives with actual attackers. This is where persona becomes a resource.

B. Organized Cybercrime and Personas

Recent trends in the IT security landscape suggest that organized cybercrime has become a part of the everyday cyber landscape with conventional criminal groups using cybercrime to achieve their goals [18]. Choo and Smith [19] categorize organized cybercriminals into three categories:

1) conventional organized criminals who want to improve their criminal activities using cyberspace,
2) online cybercrime groups that mainly do their activities online, and
3) ideologically/politically motivated individuals that want to make use of the cyberspace for their particular interest.

Moreover, McCombie and Pieprzyk [20] suggest that the cyber landscape provides ample opportunity for organized criminals. Further, the case studies and the references provided in their article emphasize that there are cases where groups of cybercriminals have used extortion, blackmailing, and online fraud to achieve their desired goal. Hence, we assume that there exist groups of IT criminals operating on the Internet where the attackers are specialized and need to be described using a specific set of motivations, skills and goals. To map such an organization into a persona is a challenge due to the inadequacy of observable data about organizational culture, environment, hierarchal 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 [21], [22], but personification of a group of attackers has its limitation mainly due to the secret nature of such organizations.

To acquire good enough security it is critical that organizational security issues are not looked upon as a single-factor

problem rather than being multidimensional by nature. The persona methodology, contrary to its typical usage, can be used to design systems against the attacker by incorporating the attacker perspective. The narratives are a way to provide a multidimensional perspective on the security issues in an organization whereas the attacker personas are a way to relate different narratives with each other from an attacker perspective. The attacker personas will provide a different perspective on the narratives, aiding in identifying overlapping narratives and providing a mechanism to understand the motives and the goals behind a security problem or an attack. However, to achieve such benefits from the personas there is a need to develop attacker personas that are generic in nature, and thus can be applied in several contexts.

In the following we present the development of a framework for eliciting narratives and connecting to general attacker personas. The framework and the methodological procedure is intended to help organizations to become better equipped to assess and be prepared to act against perceived threats. The framework is based on both theoretical argumentation and a minor empirical survey.

IV. Methodology

In order to collect empirical data and insight about the multidimensional aspect of security and using narratives/storytelling as communication medium to propagate security issues we conducted a short exploratory survey in which we asked the respondents about their point of view on IT security. The questions had two parts. First, a question was asked in order to point out differences between the higher management vis-à-vis IT system designers/developers with regard to understanding of IT security issues within an organization, aiming towards the multidimensional perspective of security issues. The second part dealt with storytelling, i.e., the respondents' thoughts about storytelling and whether it can be used as a communication medium for fostering consistent understanding of the IT security challenges and issues across the organization. We asked these questions to a total of six individuals. The questions were e-mailed to the respondents, and 5 out of 6 respondents sent their responses via e-mail while one chose to answer through a telephonic conversation. The targeted group consisted of IT professionals having a background in IT security. Three of them were working in the organization as software developers/designers, one was working in software testing, and two were providing security consultancy. The respondents were mainly working in large organizations having more than 100 employees.

The next methodological step focused on the representation of the attackers in the form of personas. To accomplish this, identifying resources for acquiring data was the first thing to do. In a related article, Faily and Fléchais [23] use threat taxonomies as the major source of information, which is relevant for their context of use. However, we argue that there are multiple sources of data that can be used to develop attacker personas. Especially, there exists a comprehensive body of knowledge with regard to understanding the attacker perspective, and during our literature review we came across multiple multidisciplinary sources of attacker data. The data collected for the development of attacker personas has been taken from a combination of ethnographic studies, psychological studies of attackers, and IT security literature. The multidisciplinary nature of the literature shed light on the attackers from different perspectives such as attackers' behavior, motivation, social and cultural aspects and goals, etc. Furthermore, there are several accounts of attackers which have been documented within IT security literature, mostly regarding the convicted attackers, which provide information about profiling of attackers and their skills [24], [25], [26], [27], [28].

The categorization of the attackers was carried out based on their motivations. There is plenty of IT security literature available that sheds light on this aspect and provides a comprehensive classification of attackers [29], [30], [31]. The classification of attackers within the security literature consists of a rather stereotypical technical skill description, and differ only in that an attacker with similar skills is described using different names in different sources, e.g., an attacker who has the very basic skills is referred to as a script kiddie, novice, newbie, etc., depending on the source.

The identified sources were used to develop sketched personas of the attacker. The personas created provided a brief history of the attacker's goals, motivations, and relevant skills. To further refine the persona we developed scenarios to highlight inconsistencies. Additionally, we used hypothetical scenarios to test the personas in different conditions, and to understand how these generic personas can be used in a given context.

V. Results

This section summarizes the results that were collected as part of our exploratory survey with the aim of understanding the elastic nature of IT security problems in an organization. Moreover, we present the attacker personas which are used to represent the attackers in a narrative structure. The attacker personas are currently six in number and have been made as a proof of concept for the case of developing attacker personas that are context independent.

A. Survey

Analyzing the survey responses, the respondents agreed to the fact that there is a difference when it comes to understanding IT security. They highlighted that sometimes the higher management in the organization considers security from a more abstract perspective while the developer or the system designer have a more technical understanding of IT security. The first question, "Do you think there is a gap between the higher management understanding of the IT security (in general) and your thinking of IT security while designing/developing the system?," was aimed at understanding the difference between the higher management and the system developers. One of the respondents did not agree that there is such a difference and meant that everyone has a more or less

similar understanding, but due to lack of communication the understanding of IT security is different with regard to one's viewpoints:

> I do not think there is gap between management and the developer to understand IT security. Managers need to describe in detail to their developers how they want the system should work. It's up to the developers how they implement it.

Similarly, one respondent argued that this difference in understanding is natural since both the higher management and the software developers have different roles in the organization.

> There is a definite gap of understanding. The higher management decisions are driven by business goals. If designing security becomes a hurdle, security is often appended in the end giving a sense of security. As a designer of a system, our goals of incorporating security are purely technical and are driven by overall application security.

Hence, the feedback from the survey re-enforce the idea described in Section III regarding several perceptions of the same issue due to the organization being a complex entity and every user in the organization having a different perception. The higher management in the organization has a different understanding of the security problems whereas the designers have a more technical understanding of security. This difference in understanding mainly stems from the particular role of an individual in the organization.

With regard to the second question, "What do you think of using techniques such as storytelling to communicate IT security problems across the organization?," the survey responses were varying. According to one respondent the idea is interesting but should be used in combination with other methods to increase its effectiveness:

> Storytelling is good technique in which user can tell his needs, problems etc in a simple language. And the expert can draw design on based on story. However this is one of the technique and is not sufficient to communicate security related problems across organization. Different techniques can be merged along with storytelling.

In another case the respondent argued that newspapers can be an alternative mechanism which could be used to create awareness during the weekly meeting where recent threats and issues of concern to the organization are discussed:

> Recent news about IT-Security problems in Meetings, Seminars.

Yet another respondent argued that this technique could be useful in terms of known security threats or attacks but would not be effective in case of new types of threats. The remaining respondents were positive to the use of storytelling and suggested that this method could be used to create awareness as well as during the design and development phase of a product.

Fig. 1. Each attacker persona contains goals, motivations, skills, and a scenario that are specific for the persona in question.

B. Presentation of Personas

Based on the acquired data, we have developed a total of six attacker personas according to Figure 1, namely the ideologically motivated, the botnet developer, the bragger, the insider, the spy, and the financially motivated attacker. The personas are developed to represent the most common set of motivations of an attacker according to IT security literature such as ideological, financial, political, revenge, and so on. One could develop any number of attacker personas based on their specific requirements but for a proof of concept, we have developed six attacker personas and to exemplify, we will briefly present three of these below. Each persona has been given a distinct name and picture, representing the fictional character. Moreover, each persona has been associated with goals, motivations, attitudes and skills. The personas are developed to depict the generic perception of the attackers and are not designed to serve any specific organization or context. The skills and attitudes are high-level in nature and are based on literature. This collection of personas depicts several threats to an organization. Relevance of these personas in terms of organizational context can be judged based on their motivations and high level goals described within the personas. The skill sections in each persona represent the capability of an attacker, and how these skills can be used to carry out an attack is presented in the persona-specific scenario.

To further elaborate on the scenarios that are part of each persona, these are part of the persona methodology and are used to describe the sequential activities that a user undertakes to reach a specific goal. The aim of the scenarios is to aid the system designers in understanding the user activities and requirements while developing a system. We have used the concept of scenarios, as discussed by Quesenbery [15], 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. This information is also derived from the IT security literature as discussed in Section II.

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 it 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 Section VI. These personas act as a tool to question the existing security practices applied by the organization at a higher level, and provides a multidimensional view of threats that an organization can face. The scenarios coupled with the attacker personas provide a much detailed analysis of the attacker perspective, providing a generic understanding of how the attacker operates.

Martin represents the set of attackers which are ideologically motivated. The persona starts with a brief historical account of Martin, depicting how he started to develop his skills within the area of IT security and what motivated Martin to become an ideological attacker. Furthermore, a brief set of skills are also expressed in the persona to highlight high-level understanding of the type of attacks Martin can perform. Martin's skills range from social engineering to developing specialized tools or scripts to infiltrate an organization. The Martin persona also includes the set of goals which he is trying to pursue and what he would achieve if a successful attack on the organization is carried out.

The next attacker persona is *Kevin*, which represents the group of attackers who are financially motivated. The persona starts with a brief background, representing a brief world-view of the attacker. The attacker has chosen cybercrime as a way of living and finds criminal activities on the Internet very profitable. The persona also sheds some light on the underground hacking circle where he has contacts. From his large array of hacking skills, social engineering attacks are of most interest since he finds them easy to exploit. Kevin is represented in the persona as a "gun for hire" and can be used by anyone, e.g., the mafia, terrorist organizations, spies, and others.

Thomas is the persona representing botnet developers, i.e., a persona performing non-targeted attacks. This persona represents attackers who develop botnets by first hacking into organizations and later using their infrastructure for attacking third party networks. The Thomas persona describes why the organization is of interest and how he can benefit from the organizational infrastructure without having a direct motivation for attacking the organization in itself. Thomas's major motivation is financial and he works in collaboration with other attackers. The Thomas persona is specifically designed to address the non-targeted attacks on an organization, and how someone who might not be directly interested in hacking into critical assets of an organization still can pose an indirect threat.

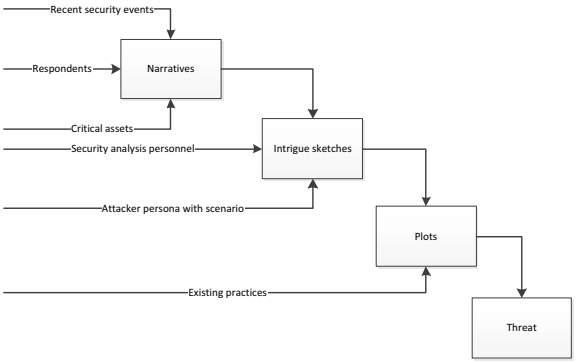

Fig. 2. The complete flow diagram of the framework starts with the collection of narratives which are derived from respondents in terms of critical assets and security related events. Narratives and attacker personas with scenarios are then used by a security analyst to develop intrigue sketches. These intrigue sketches are further related with each other and with existing security practices in order to develop a small number of plots to be considered for identifying the overall threat.

VI. 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 four parts, namely:

1) narratives,
2) attacker personas (including scenarios),
3) intrigue sketches,
4) plots.

In the preceding sections, narratives and attacker personas have already been discussed. Henceforth, this section serves to describe intrigue sketches and plots.

A. Intrigue Sketches

Before we define the intrigue sketch it is necessary to understand why we need intrigue sketches. As discussed in Section II, our personas/scenarios are context independent so in order to put them in an organizational context we need to relate them to organizational-specific narratives and therefore we have introduced the term intrigue sketch. The aim of the intrigue sketches is to provide a mapping such that the attacker and the IT security perspective can be related in a context specified by the user through the narrative. 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 a 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 can further lead to identifying organized cybercrime activity by looking at multiple intrigue sketches, which will be discussed further below.

As shown in Figure 2, the intrigue sketches make use of narratives, security analysts and attacker personas with scenar-

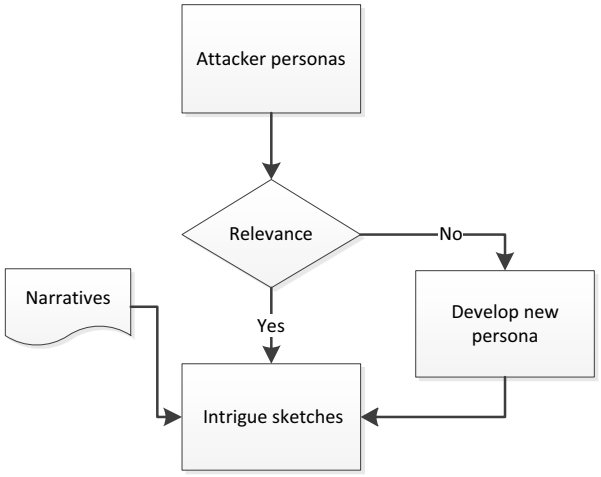

Fig. 3. The intrigue sketch development process relates a narrative with one or several attacker personas. If the narratives cannot be described using the existing persona set, then new attacker personas must be developed so that a narrative has a minimum of one attacker persona assigned to it.

ios. 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. As depicted in Figure 3, 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. Moreover, new personas can be developed for the case when the existing personas do not tackle the problems identified by the narrative.

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. Similarly, each narrative will have at least a single corresponding intrigue sketch. 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. As shall be seen, this classification of the intrigue sketches will prove necessary in the next phase of the framework, which is the plot creation.

B. 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.

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. Moreover, each attack represents a threat to an organization and thus each plot will yield a single threat. To finally tackle the organized cybercrime threat, the attacker personas that were listed during the intrigue sketch development activity are used. 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 attackers which are individual actors or are part of an organized criminal activity. To summarize and to get an overview of the framework, see Figure 4 where the framework constituents have been put in perspective relative to each other.

VII. Conclusions

In this paper we have presented a framework which is to be used to understand the existing IT security environment in an organization. The framework highlights possible inconsistency in terms of understanding the IT security specific requirements and expectations from the organizational perspective. Also, the framework is an effort to assess the organizational security from multiple perspectives by extending the persona methodology. A small amount of empirical data was collected from individuals working as developers and designers within different organizations. Most agreed that using storytelling to communicate organizational-specific threats (in terms of IT security) is a good idea and some further suggested that these stories can be used as a tool to elicit security-specific requirements as well. We have also presented attacker per-

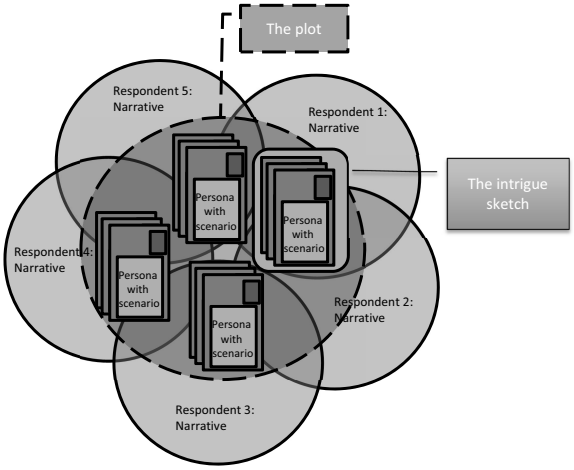

Fig. 4. The complete framework consists of different narratives that are collected from the respondents in the organization, which are then being related with attacker personas with scenarios in order to develop intrigue sketches, which are finally brought together with existing organizational practices to develop the overall plot.

sonas 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. In the future, we aim at 1) assessing the validity of the framework by collecting empirical data from IT security specialists, and 2) applying the framework at a selected organization in order to evaluate its practical usefulness.

REFERENCES

[1] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[2] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of the 1996 workshop on New security paradigms*, ser. NSPW'96. New York, NY: ACM, 1996, pp. 27–33.

[3] M. E. Zurko, "User-centered security: Stepping up to the grand challenge," in *Proceedings of the 21st Annual Computer Security Applications Conference*, ser. ACSAC'05. Washington, DC: IEEE Computer Society, 2005, pp. 187–202.

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

[5] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th conference on USENIX Security Symposium*, ser. SSYM'99. Berkeley, CA: USENIX Association, 1999.

[6] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[7] I. Fléchais and M. A. Sasse, "Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science," *International Journal of Human-Computer Studies*, vol. 67, no. 4, pp. 281–296, Apr. 2009.

[8] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Fléchais, "Here's Johnny: A methodology for developing attacker personas," in *Sixth International Conference on Availability, Reliability and Security (ARES)*, Aug. 2011, pp. 722–727.

[9] A. Cooper, *The Inmates Are Running the Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity*. Sams Publishing, 2004.

[10] J. Pruitt and J. Grudin, "Personas: Practice and theory," in *Proceedings of the 2003 conference on Designing for user experiences*, ser. DUX'03. New York, NY: ACM, 2003, pp. 1–15.

[11] E. Markensten and H. Artman, "Procuring a usable system using unemployed personas," in *Proceedings of the third Nordic conference on Human-computer interaction*, ser. NordiCHI'04. New York, NY: ACM, 2004, pp. 13–22.

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

[13] S. Portigal, "True tales: Persona non grata," *interactions*, vol. 15, no. 1, pp. 72–73, Jan.–Feb. 2008.

[14] J. Grudin and J. Pruitt, "Personas, participatory design and product development: An infrastructure for engagement," in *Proceedings of the 7th Biennial Participatory Design Conference (PDC 2002)*, 2002, pp. 144–161.

[15] W. Quesenbery, "Storytelling and narrative," in *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*, J. Pruitt and T. Adlin, Eds. San Francisco, CA: Morgan Kaufmann, 2006, ch. 9, pp. 520–554.

[16] J. Brynielsson, "An information assurance curriculum for commanding officers using hands-on experiments," *ACM SIGCSE Bulletin*, vol. 41, no. 1, pp. 236–240, Mar. 2009.

[17] S. Cooper, C. Nickell, V. Piotrowski, B. Oldfield, A. Abdallah, M. Bishop, B. Caelli, M. Dark, E. K. Hawthorne, L. Hoffman, L. C. Pérez, C. Pfleeger, R. Raines, C. Schou, and J. Brynielsson, "An exploration of the current state of information assurance education," *ACM SIGCSE Bulletin*, vol. 41, no. 4, pp. 109–125, Dec. 2009.

[18] R. McCusker, "Transnational organised cyber crime: distinguishing threat from reality," *Crime, Law and Social Change*, vol. 46, pp. 257–273, 2006.

[19] K.-K. R. Choo and R. G. Smith, "Criminal exploitation of online systems by organised crime groups," *Asian Journal of Criminology*, vol. 3, pp. 37–59, 2008.

[20] S. McCombie and J. Pieprzyk, "Winning the phishing war: A strategy for Australia," in *Second Cybercrime and Trustworthy Computing Workshop (CTC 2010)*, Jul. 2010, pp. 79–86.

[21] M. Kuniavsky, "Extending a Technique: Group Personas," http://www.boxesandarrows.com/view/extending_a_technique_group_personas/, 2004, [Online; accessed 10-April-2012].

[22] A. Giboin, "From individual personas to collective personas," in *Proceedings of the Fourth International Conference on Advances in Computer-Human Interactions (ACHI 2011)*, Feb. 2011, pp. 132–135.

[23] S. Faily and I. Fléchais, "Barry is not the weakest link: Eliciting secure system requirements with personas," in *Proceedings of the 24th BCS Conference on Human Computer Interaction (HCI 2010)*, ser. BCS'10. Swinton, UK: British Computer Society, 2010, pp. 124–132.

[24] P. Shachaf and N. Hara, "Beyond vandalism: Wikipedia trolls," *Journal of Information Science*, vol. 36, no. 3, pp. 357–370, Jun. 2010.

[25] M. Kilger, O. Arkin, and J. Stutzman, "Profiling," in *Know Your Enemy: Learning about Security Threats*, 2nd ed., L. Spitzner, Ed. San Francisco, CA: Addison-Wesley, 2004, ch. 16, pp. 505–556.

[26] R. Barber, "Hackers profiled—who are they and what are their motivations?" *Computer Fraud & Security*, vol. 2001, no. 2, pp. 14–17, Feb. 2001.

[27] E. D. Shaw, "The role of behavioral research and profiling in malicious cyber insider investigations," *Digital Investigation*, vol. 3, no. 1, pp. 20–31, Mar. 2006.

[28] I. Enrici, M. Ancilli, and A. Lioy, "A psychological approach to information technology security," in *Proceedings of the 3rd International Conference on Human System Interaction*, May 2010, pp. 459–466.

[29] M. Rounds and N. Pendgraft, "Diversity in network attacker motivation: A literature review," in *Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE'09)*, vol. 3, Aug. 2009, pp. 319–323.

[30] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation*, vol. 3, no. 2, pp. 97–102, Jun. 2006.

[31] D. E. Denning, *Information Warfare and Security*. Boston, MA: Addison-Wesley, 1999.