A methodology and supporting techniques for the quantitative assessment of insider threats

Nicola Nostro, Andrea Ceccarelli, Andrea Bondavalli
University of Firenze, Viale Morgagni 65, Firenze, Italy
{nicola.nostro, andrea.ceccarelli, bondavalli}@unifi.it

Francesco Brancati
Resiltech S.r.l.
Piazza Nilde Iotti 25,
Pontedera (Pisa), Italy
francesco.brancati@resiltech.com

ABSTRACT
Security is a major challenge for today's companies, especially ICT ones which manages large scale cyber-critical systems. Amongst the multitude of attacks and threats to which a system is potentially exposed, there are insiders attackers i.e., users with legitimate access which abuse or misuse of their power, thus leading to unexpected security violation (e.g., acquire and disseminate sensitive information). These attacks are very difficult to detect and mitigate due to the nature of the attackers, which often are company's employees motivated by socio-economical reasons, and to the fact that attackers operate within their granted restrictions: it is a consequence that insiders attackers constitute an actual threat for ICT organizations. In this paper we present our ongoing work towards a methodology and supporting libraries and tools for insider threats assessment and mitigation. The ultimate objective is to quantitatively evaluate the possibility that a user will perform an attack, the severity of potential violations, the costs, and finally select the countermeasures. The methodology also includes a maintenance phase during which the assessment is updated on the basis of system evolution. The paper discusses future works towards the completion of our methodology.

Categories and Subject Descriptors
K.6.5: [**Computers and Education**]: Security and Protection: *authentication*, *unauthorized access*

K.6.m: [**Computers and Education**]: Miscellaneous: *security*

General Terms
security, standardization, verification.

Keywords
security; insider threats; risk assessment; attack path.

DISCCO '13, September 30 2013, Braga, Portugal

ACM 978-1-4503-2248-5/13/09…$15.00.
http://dx.doi.org/10.1145/2506155.2506158

1. INTRODUCTION
Today's ICT organizations are constantly facing the challenge of ensuring high degrees of security (and privacy). Security measures are attentively selected and maintained, mainly with the intent of protecting the organization from external threats. Several tools and solutions are available for this scope, for example firewalls. A lesser amount of solutions is instead available for mitigating threats coming from within the company, that is, from its own employees; these threats, that we refer to as *insider threats*, are most often mitigated almost exclusively through regulations and policies [6]. For example, insiders to an organization such as former, or newly fired employees or system administrators might abuse their privileges to conduct masquerading, data harvesting, or simply sabotage attacks. Although some intrusion detection systems offer insider threats capability, it is still very difficult to characterize all the threats, transform them into rules (or, in case of anomaly-based intrusion detection, instruct the detector to identify them as anomalies), and effectively detect intruders.

The problem of insider threats have been, and currently is, largely discussed in literature, because it is particularly challenging to identify insiders and mitigate the possible threats they pose to a system; we should consider that an insider attack may have socio-economical roots, and detection of false positive may have severe consequence on an organization (consider the impact of false accusations of insider threats on both the individual and the organization [7]). Mitigation may be composed of prevention (including deterrents as strict regulatory aspects, surveillance, legal implications), or detection methods and procedures that may help protecting the system.

It appears evident that protecting from insider threats requires a deep study on the socio-economical profiles of the users, their possible actions, and the impact of these actions on the system and on the life of the organization. This calls for a tailored *insider threats assessment* activity, which takes into account socio-economical aspects while identifying the attacks, their impact on the system and on the organization, and possible countermeasures. We aim to tackle this problem proposing a methodology for insider threats assessment and mitigation. This paper presents our ongoing work towards the methodology completion. The methodology presents the following features: i) it is tailored for the challenges posed by insider threats, ii) it is supported by a set of libraries and tools, iii) it takes into account socio-economical aspects, including a description of the profile of the attacker, iv) relies on model-based formalisms of the system and of the attack paths to quantitatively analyze threats and evaluate countermeasures. The methodology first defines the system requirements and the attackers profiles, then identifies the threats,

the attack paths and the potential countermeasures. The methodology also includes a maintenance phase during which self-reconfiguration facilities of the system are supported to update the assessment.

2. DEFINITION OF INSIDER THREAT

Talking of insider is often confusing, in literature there are different definitions of insiders, each of which, in general, has a negative meaning of the concept of insider. Although the question *"who is an insider?"* seems simple, a well established definition is still missing. Definition in [10], [11] suggests that an insider must be defined with respect to some set of rules that is part of a security policy:

"A trusted entity that is given the power to violate one or more rules in a given security policy... the insider threat occurs when a trusted entity abuses that power."

The CERT Program goes further by providing a definition of *malicious insider* [9]:

A malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria: i) has or had authorized access to an organization's network, system, or data; ii) has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

In [11] several possible uses of the term insider are listed, but still not exhaustive and potentially could be extended. In general, we can simply define an insider as *an entity that have been given the privileges to act within a specific environment.* What is of interest is the use of privileges (being it an abuse or misuse of privilege, or simply a mistake) in such a way that it constitutes a threat (being it malicious or accidental [7]) i.e., an *insider* threat.

3. STATE OF THE ART AND ADVANCEMENTS

A wide literature exists on the issue of the insider threats, although most of it is devoted to the description of techniques and methods useful to *prevent* insider attacks and to protect the system or the infrastructure. Examples are initiatives as restrict remote access and system administrator access, or inhibit the use of removable drives. Also works have been done to *predict* threatening insider activity, for example [14] presents a prediction model based on graph theory approaches, where alarms are raised when it is detected an increasing risk that users actions might lead to compromise systems resources.

Recent years have witnessed an increasing number of works devoted to research solutions for (early) *detection* of insider attacks [9], [7]. However, to the best of our knowledge, most of the proposed works have been devised for specific and well defined case studies, sometimes also requiring to introduce simplifying assumptions, and without offering good portability to different systems or environments.

In [1], the authors aim to detect masquerade attacks, where a user impersonates another user, by profiling user behaviors. To evaluate these attacks, UNIX command data were collected from a certain number of users and then the data were contaminated with masqueraders. The experiment was performed and compared with six masquerade detection techniques: Bayes one-step Markov, Hybrid multi-step Markov, IPAM, Uniqueness, Sequence-Match and Compression. In [2] an approach is pursued to predict financial fraud from insiders by considering: i) the audit data, gathered during the operation of the system, and ii) the human factor, as a qualitative aspects to integrate with the classic quantitative analysis of financial transactions. The works [3] and [4] focuses on the analysis of anomalous commands executed on data bases. In [3] a user profile has been generated according to a syntax-centric approach, that represents the structure of the SQL queries submitted by the users, in order to detect anomalous queries. Another approach which consider the RDBS as case study is in [4], where the approach is data-centric unlike the previous one. In this approach the anomalies are identified looking at the data that are retrieved following the user's request.

In [5] it is proposed a graph-based model of the system's basic network connectivity and access control mechanisms, to identify system vulnerabilities which can be exploited by a malicious insider in his attack. In [6], a study within an enterprise was conducted, during which analysts were monitored while performing analytical operations. Using Grounded Theory research method (Grounded Theory is defined as the discovery of theory from data systematically obtained from social research), the objective are: i) understand how security event analysis works, and ii) create an event-based model to analyze insider threats. This model shows how alerts and events created can be analyzed to determine if malicious insider behavior is present. This approach defines a process and a model to identify and characterize insider threats.

While great efforts have been devoted on the research of solutions to the thorny problem of the insider threat, few efforts have been made to identify and delineate a methodology for the *insider threats assessment*, comprising threats identification, (quantitative) evaluation and mitigation. A threat assessment process, generic and not limited to insider threat, is presented by NIST [12]. Although generic and largely applicable, it does not proposes methodologies and libraries to support and semi-automate the assessment process, nor to achieve a quantification of the dangerousness of each threat. While being compliant to the steps of the NIST process, we focus on insider threats assessment, aiming to define a methodology that is supported by libraries, techniques and tools. Note that external libraries or techniques as the threat models from [5] can still be used. An important challenge that we plan to address is related to the *maintenance* phase of the threat assessment process, to perform updates of the threat analysis smoothly and rapidly, in order to reflect the system evolution. This is especially intended for systems characterized by evolutionary and dynamic behavior, as for example Internet of Services, large-scale architectures, or cyber-critical infrastructures, in which traditional, pre-deployment Verification and Validation is inefficient and thus run-time verification [15] to cope with the changes in the system and its environment is required.

4. OUR METHODOLOGY IN SIX STEPS

The objective of this work is to provide an incisive, clear and supported methodology to handle those systems, and related risk assessment processes, where the insider threat issue could be relevant. Especially the proposed methodology will be independent from the type of system.

In the following subsections 4.1 to 4.6 we provide a brief presentation of the proposed methodology, pointing out the description of six key iterative phases around which the

methodology has been developed. Compliance with NIST risk assessment procedure is not shown for brevity, but can be easily proven intuitive. The specialization of the proposed methodology on a real case study will be given in the later sections of the paper.

4.1 System under analysis

A *system* is characterized by a number of resources (e.g., services, computers, removable drives, etc.), one or more communication networks, and users, which can use the system or in general interact with it. In addition, new features of the system can be integrated over time, due to the evolution of technologies, and the update of system specification.

In the characterization of a system we can therefore talk of macro-components which constitute the overall architecture. A system can thus be seen as the set of *n* macro-components. A functional description of the system in some form, from textual requirements to semi-formal language, can be provided and used here. Although precise requirements and a model of the system is preferable (especially as input for the successive phases of our methodology), restrictions on the description method and level of details are not provided, because we are aware that in practise a threats assessment may incur while the system requirements definition is still ongoing (although this may call for additional iterations of the procedure).

4.2 Insiders

The second phase of the methodology consists in profiling potential insiders, determining their dangerousness to the system and their key attributes. This is organized in two steps.

In first step, which follows from system requirements, all possible users involved in the system under analysis are identified.

In the second step their potential attributes as insiders are defined. To perform this task more efficiently and raise evidence of the completeness of the assessment procedure, we propose a predefined library of insiders. We refer to the attributes presented in [8], where a detailed threat agent library (TAL) has been provided, which constitute a consistent reference library describing the human agents involved in IT systems and that could pose threats to such kind of systems, although not limited to insider threats. The idea is *not* to represent specific individuals, but instead the library is intended to create a taxonomy of specific attributes useful to uniquely identify the users/insiders.

Specifically, the attributes defined are eight and they are described in the following specialized for insider threats [8]:

Intent. Whether the insider intends to cause harm. Insiders fall into two categories based on their intent: *Hostile* and *Non-Hostile*.

Access. Defines the extent of the insider's access to the company's assets. There are two options: *Internal* or *External*.

Outcome. Defines the insider's primary goal, that is, what the insider tries to accomplish with a typical attack. Possible outcomes are: *Acquisition/Theft*, *Business Advantage*, *Damage*, *Embarrassment*, *Technical Advantage*, etc.

Limits. Legal and ethical limits that may constrain the insider, e.g., the extent to which the insider may be prepared to break the law. Options are: *Code of Conduct*, when the insiders follow both the applicable laws and an additional code of conduct accepted within a profession or an exchange of goods or services; *Legal*, the insiders act within the limits of applicable laws; *Extra-legal, minor*, the insiders may break the law in relatively minor, non-violent ways, such as minor vandalism or trespass, e.g., activist; *Extra-legal, major*, insiders take no account of the law and may engage in felonious behavior resulting in significant financial impact or extreme violence, e.g., members of organized crime.

Resource. Defines the organizational level at which an insider typically works, which in turn determines the resources available to that insider for use in an attack. Options are: *Individual*, insider acts independently; *Club*, members interact on a social and volunteer basis; *Contest*, participants interact together for a very short period of time and perhaps in anonymous way with the objective to achieve a single goal; *Team*, a well organized group with a leader, typically motivated by a specific goal and organized around that goal. *Organization*, a larger and better resourced than a Team. *Government*, controls public assets and functions within a jurisdiction, it is very well resourced and persists long term.

Skill Level. The special training or expertise an insider typically possesses. Options are: *None*, *Minimal*, *Operational*, *Adept*.

Objective. The action that the insider intends to take in order to achieve a desired outcome. Options are: *copy*, *destroy*, *injure*, *take possession*, *don't care*.

Visibility. The extent to which the insider intends to conceal or reveal his or her identity. Options are: *overt*, *covert*, *clandestine*, *don't care*.

4.3 Insider Threats

The third phase is the identification and description of possible threats which the system could be vulnerable to. This activity is of critical relevance because it allows to identify the damages that can be done on the system and the potential consequences. Through this phase it is possible to define the threats that need to be addressed with higher priority. It is important to note that we are not interested on the motivations that lead an insider to put into practice an attack.

For example, the potential threats which a generic system may be subject are: installation of improper software/apps (e.g., viruses, Trojans, spyware, backdoors, key loggers, logic bombs, etc.); improper data operations (e.g., data removal, exporting data, producing fake data, data modification, etc.); managing of user profiles (e.g., creation of fake users). The list is long and most likely system-dependent; a library of threats, expanding the list above mentioned, will be prepared, matched to the identified users type and attributes (e.g., insider attacker motivations or experience), and maintained.

4.4 Attack paths

This phase has the objective to identify the path(s) exploitable by the insider to realize the threat(s) and achieve the goal.

Several approaches exist and are very useful for determining what threats exist in a system and how to deal with them, e.g., attack trees [18], attack graphs [19], privilege graphs [20], ADVISE [17]. The latter extends the concept of attack graph by considering different attack goals, attack preferences of specific attackers, and creating customizable models to produce quantitative analyses based on specific metric of interest.

Regardless of the adopted approach, the capability to build an attack path, match it to a system model, and consequently to evaluate quantitatively the success rate and effects of the attack is

of paramount importance, as it allows for example to get information on the probability of occurrence of an attack.

The identification of the overall set of attack paths is a critical step, especially if we think of *unknown* paths. Many insiders, abusing of their privileges, are able to set up unexpected attack paths, that are unknown w.r.t. the presented set of attack paths [22]. Said this, the activity of discovering the unknown paths is strongly linked to a monitoring activity of the system, with a careful management of the known access paths into the system.

4.5 Countermeasures selection

This phase consists in the selection of the proper countermeasure(s), in order to avoid or mitigate the identified threat(s). Again, a defined library which lists the countermeasures for determined attacks can be used to support the countermeasures identification and selection.

Introduction of such countermeasures necessarily require to re-assess the system, improved with the countermeasure, to verify that the threat is mitigated and give evidence of the security improvement. In case a model of the system and of the countermeasure is available, these can be integrated with the attack path of Section 4.4.

4.6 Iteration and Update

It is well known that today's large scale systems and infrastructures are subject to changes and evolutions; this can require to iterate the phases of the methodology in order to align the assessment outcomes to the most recent status of the system. To semi-automate this procedure, this require to: i) collect feedbacks from the field about system status, ii) use those feedback to understand the evolution of the system, its users, and possible changes of system requirements, iii) update the insider threats library and the attack paths, and iv) perform the quantitative analysis. This will ultimately lead to define new countermeasures to be applied. In this paper this step is not discussed further to allow more space to a first basic definition of the methodology.

5. METHODOLOGY APPLICATION

We apply our methodology to a compact but concrete case study. For this purpose we consider our ongoing work in the context of the Secure! project. We point out that the sixth phase is currently not considered, because the Secure! project is still in its design phase; consequently the assessment will cover phases 1 to 5.

5.1 System under analysis

Secure! [13] is a system whose objectives are: i) prevent crisis as terrorist acts, vandalism, sabotage, and ii) support crisis management (e.g., in case of environmental catastrophes, human sabotages, and authorized or not-authorized demonstrations). The Secure! system will be able to integrate several heterogeneous information (audio, video, images, text) originated from different sources, including social networks (e.g., Facebook, Twitter, Flickr), emergency numbers, surveillance camera, telecommunication network, and data provided by the Secure! users on field through a Secure! application for mobile devices (anyone can be a Secure! user, after downloading the application). The Secure! system includes instruments to semi-automatically correlate, query and analyze the data, supporting both the intervention of crisis management teams, and a-posteriori forensic analysis. Secure! can run on cloud system, which is particularly involved for the big-data management. Secure! is subject to severe security and privacy requirements. In fact, in order to have users trust the Secure! system and to make it acceptable to the community, it is mandatory to provide guarantees that users authorized to work with the data collected do not compromise, counterfeit, steal or even unnecessarily query them, or do not abuse of the data correlation and data search capacity behind what is strictly necessary for their work. This calls for an attentive evaluation of insider threats. Secure! project started recently, therefore the description is currently only textual [13], and the architectural description using the MDA approach is ongoing.

5.2 Insiders

A taxonomy of users physically or logically involved within the system has already been organized in six plausible groups of users and is described below [13].

Operator. A Secure! user who works in the security field, e.g., trained firefighter, or rescue personnel.

Human Sensor. Any citizen voluntarily registered to the Secure! platform in order to cooperate using the Secure! application.

Domain expert. Represents an expert in the homeland security field, e.g., a police officer or a component of national intelligence.

Unknown user. A citizen who is not registered to the platform, but interacting, even unconsciously, with the system, e.g., by social media, blog, etc. This user is in general very little expert of Secure!.

System expert. A special user which can access the system in order to install and configure the various components of Secure!.

System Administrator (SA hereafter)**.** A special user which has remote and local access to Secure! in order to perform maintenance tasks, removal, exports and drop of data, managing user profiles, etc. Moreover, the SA is in charge of managing emergency situations in which the system is undergoing maintenance, or under cyber-attacks, etc.

Given the dimension of the Secure! system, more than one user belongs to the same group, e.g., there are different SAs; also, one user can belong to multiple groups. For illustrative purposes, we apply our methodology to one of the above insiders, that is the SA. According to the eight attributes defined in Section 4.2, in this step we can provide a preliminary matching Attributes-Values, showed in Table 1, which will be refined during the next *Insider threats* phase. In fact, the values assigned to the attributes could vary based on the threat to be considered.

Table 1. Preliminary matching attributes-values.

Attribute	Value
Intent	Hostile/Non Hostile
Access	Internal
Outcome/Goal	Acquisition/Theft, Embarrassment, Damage
Limits	Code of Conduct, Legal, Extra-legal
Resources	Individual, Team, Contest
Minimum Skills	Operational
Objective	Copy
Visibility	Clandestine

5.3 Insider threats

In the context of the Secure! project, we can identify a number of threats of different type of severity, which are related to the actions performed by the insiders. This phase of the methodology

aims at identifying all threats whose impact, in case of successful attack, is intolerable in terms of economic losses, image, damages to the infrastructures and/or to the environment, and so on.

Within Secure!, for example, *human sensors* could use their own Secure! application in order to provide, intentionally, fake information to the system, causing delay on supporting operations on field. System expert, as the SA, could install and improperly configure components on the Secure! system.

For brevity, in this work we consider the SA, who can potentially realize a consistent number of threats with respect to the others insiders. Specifically, thanks to its privileges, he could install malicious software/code, create backdoors, disable system logs and anti-virus, create new users or change users' privileges, install remote network tools, plant logic bombs [16], perform operation on data base in order to have Secure! creating erroneous reports, modify, delete, and steal data.

The basic idea is to list all the possible threats of interest and try to associate them to the previously identified insiders, as sketched in Table 2 which shows a portion of the SA row.

In the rest of the paper, among the mentioned threats, we concentrate on the *improper data management* which the SA could realize for personal purposes e.g., collecting information about movements of the police teams and or export sensitive data to sell or to use for personal purposes; delete useful information about the current or past critical event to hide or cope something/someone.

Based on the insider under analysis and the threat of interest, we can refine the previous Table 1 and we obtain Table 3.

Table 2. Mapping insiders to threats.

	Threats			
Insiders	Send fake info	Disable system logs	Improper data management	Improper user management
System Administrator	NO	YES	YES	YES

Table 3. Refined matching attributes-values.

Attribute	**Value**
Intent	Hostile
Access	Internal
Outcome/Goal	Acquisition/Theft
Limits	Legal
Resources	Individual
Minimum Skills	Operational
Objective	Copy
Visibility	Clandestine

5.4 Attack paths

To achieve his attack goal, that is the theft of sensitive data, the SA will perform the following steps.

First of all, the SA logs into the system. This action can be performed both within the company, and from remote. Then the SA accesses the data base in order to execute his data queries or even dump the database. After that he can copy the obtained data to a different file, or to an external drive, or he can send them by e-mail or simply print them. These simple actions can be performed by any user with the same privileges of the generic SA. Said this, it is easy to see that the SA could create one or more false SA or even he could give SA privileges to another user (e.g., operator, system expert) behind his back, and exploit the new insider's account and privileges to achieve its attack goal, preventing being identified. In order to assess the identified insider threats, both quantitative and qualitative formalism can be used to model the attack paths.

For example, to perform quantitative evaluation, the ADVISE modeling formalism [17] is here proposed. ADVISE is a formalism for security evaluation that extends attack graphs and takes into account the attack behavior and proficiencies of different attack profiles.

It is important to point out that to be able to perform a *quantitative* security analysis using ADVISE, a mapping between the TAL library and ADVISE profiles must be provided, also assigning numerical values, and ultimately a mapping from ADVISE to the system description. We want make it clear that this mapping is currently unavailable, and it will be devoted to future works. Merely to give a simple example of the ADVISE attack execution graph, describing how an insider can realize the considered threat, we propose the structure in Figure 1. We briefly describe the meaning of the graphical notation: the rectangular boxes represent the attack steps; the squares are the access domain; the circles are the knowledge items and finally the ovals represent the attack goal. More details on the formalism and graphical notation can be found in [17]. Since this is a preliminary work towards a methodology for quantitative assessment of insider threats, we refer to future works for analyses results preferring to provide a better description of the methodology.

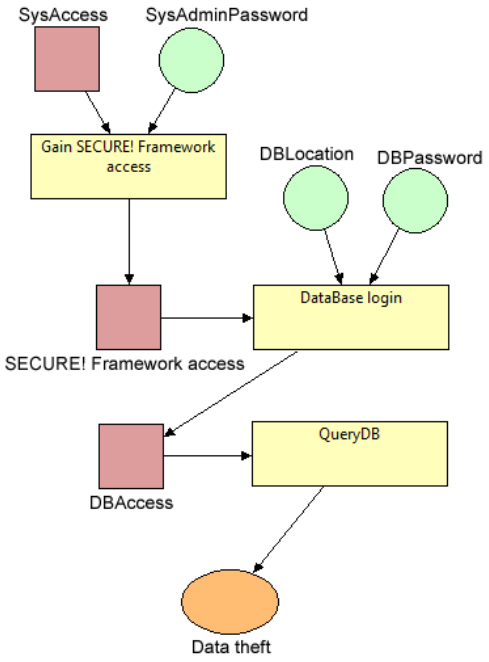

Figure 1. ADVISE attack execution graph for Data Theft.

5.5 Countermeasures selection

The individual actions which constitute the graph in Figure 1 are legitimate; it is their sequence and semantics that constitute the attack. Countermeasures, being them preventive, deterrent, or a-posteriori, must be imposed. At this stage we are not willing to determine which solution is best for Secure!, but instead we simply propose countermeasures from the state of the art that are suitable for this threat.

What we aim to prevent is the export of the sensitive data outside the company. Possible countermeasures are:

- avoid the use of other programs during the action of reporting (e.g., word processor application);
- avoid the use of external data storage;
- avoid to log into the system during holiday days or outside the office hours;
- allow printing reports only in specific printers;
- query monitoring as in [3] and [4] can identify anomalous query of the database.

Selecting one or more among the proposed countermeasures and implementing them properly in the original model, allows to re-evaluate the security of the Secure! system with respect to the considered attack.

6. CONCLUSIONS AND FUTURE WORKS

Increasing attention is being paid to insider threats and attacks. Several techniques exists to avoid or detect the risk that a legitimate user abuses of its authority in the system usage. However, we identified a lack in the definition of a methodology and related supports for the systematic investigation and quantitative assessment of insider threats. This paper presents our work towards the identification of such methodology.

Our future work is mainly targeted to realize our approach in the Secure! case study, addressing the open points that were mentioned in the course of the paper. In particular, some expected challenges that we will face are the following. First, define a method which supports the creation, usage and maintenance of the threats library, using both a taxonomy and an ontology. Second, identify an approach to support the selection of the input parameters that characterize the attack path. These inputs are required to understand the costs and dangerousness of an attack; note that these vary from a system to another. Third, verify compliance of the procedure with standards, and integrate the threats assessment methodology with risk assessment processes from standards. Fourth, define solutions for evolutionary system, where the definition of insiders, the constructions of the insider threats and of the attack paths, and the execution of the model should be performed at run-time, possibly automatically, and on the basis of feedback collected from the field.

7. ACKNOWLEDGMENTS

This work has been partially supported by the European Project FP7-2012-324334-CECRIS (CErtification of CRItical Systems), the Regional Project POR-CREO 2007-2013 Secure!, and the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research.

8. REFERENCES

[1] M. Schonlau, W. Dumouchel, W. Ju, A. Karr, M. Theus, and Y. Vardi, "Computer intrusion: Detecting masquerades," *Statistical Science*, 16(1):58–74, 2001.

[2] S. Hoyer, H. Zakhariya, T. Sandner, and M.H. Breitner, "Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit," In *Proc. of the 45th Hawaii Int. Conf. on System Sciences* (HICSS '12). IEEE Computer Society, Washington, DC, USA, pp. 2382,2391, 4-7 Jan. 2012.

[3] A. Kamra, E. Terzi, and E. Bertino, "Detecting anomalous access patterns in relational databases," *The VLDB Journal* 17, 5, pp. 1063-1077, 2008.

[4] S. Mathew, M. Petropoulos, H. Q. Ngo, and S. Upadhyaya., "A data-centric approach to insider attack detection in database systems," In *Proc. of the 13th Int. Conf. on Recent advances in intrusion detection* (RAID'10), S. Jha, R. Sommer, and C. Kreibich (Eds.). Springer-Verlag, Berlin, Heidelberg, pp. 382-401, 2010.

[5] C. Ramkumar. A. Iyer, H.Q. Ngo, and S. Upadhyaya, "Towards a theory of insider threat assessment," *Proc. of the Int. Conf. on Dependable Systems and Networks* pp. 108-117, 2005.

[6] G. Doss, and G. Tejay, "Developing insider attack detection model: a grounded approach," *IEEE Int. Conf. on Intelligence and Security Informatics, 2009*, pp. 107,112.

[7] J. Hunker and C. W. Probst, "Insiders and Insider Threats - An Overview of Definitions and Mitigation Techniques," in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 2, n. 1, pp. 4-27, 2011.

[8] T. Casey, "Threat Agent Library Helps Identify Information Security Risks," Intel White Paper, September 2007, Retrieved April 24, 2013 from http://communities.intel.com/docs/DOC-1151.

[9] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn, "*Common Sense Guide to Mitigating Insider Threats,*" 4th Edition (CMU/SEI-2012-TR-012), 2012. Retrieved April 24, 2013, from the Software Engineering Institute, Carnegie Mellon University website: http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

[10] M. Bishop. "Insider is relative," In *Proc. of 2005 Workshop on New Security Paradigms* (NSPW). ACM, New York, NY, USA, pp. 77-78 Lake Arrowhead, CA, October 20-23, 2005.

[11] M. Bishop, S. Engle, S. Peisert, S. Whalen, and C. Gates, "We have met the enemy and he is us," In *Proc. of the 2008 Workshop on New Security Paradigms* (NSPW). ACM, New York, NY, USA, pp. 1-12, 2008.

[12] NIST, "Guide for conducting risk assessment," Sept. 2012.

[13] Secure! project, "D1.1 Requirements specification," May 2013, http://secure.eng.it.

[14] Q. Althebyan, "Design and analysis of knowledge-base centric insider threat models," Ph.D. Dissertation. University of Arkansas, Fayetteville, AR, USA, 2008.

[15] J. Rushby, "Runtime certification," In Runtime Verification, Martin Leucker (Ed.). Lecture Notes In Computer Science, Vol. 5289. Springer-Verlag, Berlin, Heidelberg 21-35.

[16] M. Keeney and E. Kowalski. "Insider threat study: Computer system sabotage in critical infrastructure sectors." May 2005.

[17] E. LeMay, M. Ford, K. Keefe, W.H. Sanders, C. Muehrcke, "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)", 8th Int. Conf. on Quantitative Evaluation of Systems (QEST), 2011, 191-200.

[18] B. Schneier, Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, 2004.

[19] O. M. Sheyner, "Scenario graphs and attack graphs," Ph.D. dissertation, Carnegie Mellon Univ., Pittsburgh, PA, 2004.

[20] M. Dacier and Y. Deswarte, "Privilege graph: An extension to the typed access matrix model," *Proc. of the 3rd European Symposium on Research in Computer Security (ESORICS '94)*. London, UK: Springer-Verlag, 1994, pp. 319-334.

[21] M. Maybury, et al. "Analysis and detection of malicious insiders." MITRE CORP BEDFORD MA, 2005.

[22] A. Moore, D. Cappelli, R. Trzeciak, "The big picture of insider IT sabotage across u.s. critical infrastructures," in: S. Stolfo, S. Bellovin, A. Keromytis, S. Hershkop, S. Smith, S. Sinclair (Eds.), Insider Attack and Cyber Security, Vol. 39 of Advances in Information Security, Springer US, 2008, pp. 17-52.