A Threat Analysis Model for Identity and Access Management

Nadia Jemil Abdu[1] and Ulrike Lechner[2]
[1]Unternehmensberatung H&D GmbH, Landaubogen 10, Munich, Germany
[2]Department of Computer Science, UniBw München, Werner-Heisenberg-Weg 39, Munich, Germany

Keyword: Security Threat Analysis, Threat Modeling, Digital Identity, Identity Management, Reference Model.

Abstract: Cyber attacks as a threat to business and national security have become concerns to organizations and governments. Potential impacts of attacks are financial loss, fraud, reputation damage, and legal costs. Identification of security threats is part of securing information systems as it involves identifying threats and challenges which need to be addressed by implementing appropriate countermeasures and realistic security requirements. Our study focuses on threat analysis and modeling for digital identities and identity management within and across complex and networked systems. Further, a preliminary version of a reference threat analysis model that supports threat analysis for identity management is proposed and discussed in this paper.

1 INTRODUCTION

IT security is among widely researched field both in academia and practice. This led to the development of several well-established security standards, mechanisms, tools and guidelines for managing and protecting computer-based information. Cyber attacks as a threat to business and national security have become one of the pressing concerns to organizations and governments. These attacks are increasing both in number and capacity to cause serious operational and financial damage. Cyber attacks as defined by (Dutt et al., 2012) are the disruptions in the normal functioning of computers and the loss of private information in a network due to malicious network events (threats). Such attacks could be motivated by various reasons mainly political, criminal and financial reasons (Pwc, 2011) where potential impacts are economic loss, fraud, reputation damage, legal costs and more (UcedaVélez and Morana, 2015).

Cyber security in general deals with the protection and security of assets and resources in the cyber realm. Being able to verify the identity of individuals, organizations or devices is a primary requirement in cyber security as access to any resource starts from identification of the requesting body. Also, damages that cyber attacks cause are often closely related to identities. Experience with a design study to replace a built-in software solution for Identity Management (IdM) by the off-the-shelf software products from Forgerock motivates our perspective on security threat analysis. We would like to develop an analysis method to guide practitioners on the security and business implications of identity management security. This paper explains our research approach and the current state of our research on a threat analysis model for Identity and Access Management.

We find several studies and threat techniques focusing mainly on design and implementation issues, such as security mechanisms for detecting attacks and countermeasures for reacting to security breaches (e.g. Oladimeji et al., 2006, Pudar et al., 2009). Some studies rather focus on the notion of threats, driven by risk-analyses carried out at the later stages of the development process life cycle (Xu and Nygard 2005) while many focus on threat analysis for specific systems (Stango et al., 2009; Dominicini et al., 2010; Ahmad et al., 2010). Studies on threat modeling for identity management include (Dong et al., 2008; Paintsil, 2013; Dominicini et al., 2010; Ahmad et al., 2010).

In this study we focus on threat analysis methodologies and processes and also identify threats on digital identities that will be used as a basis for our next and continuing work on threat analysis for digital identity management (IdM) within and across complex and networked systems environment. The aim of this work is to improve the existing threat analysis techniques by studying threats on IdM from

Abdu, N. and Lechner, U.
A Threat Analysis Model for Identity and Access Management.
DOI: 10.5220/0005790304980502
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 498-502
ISBN: 978-989-758-167-0

various perspectives and proposing a generic reference model and method valid for both IdM and other systems and applications if needed. In the following sections, we would like to discuss our research agenda and position our study by discussing the major concepts and milestones we aim to address.

2 METHODOLOGY

Overall we follow a design science research approach for we found this approach fit well with our research agenda. Design science is concerned with "devising artifacts to attain goals" as (March and Smith, 1995) puts it. Design science is technology oriented and attempts to create things that serve human purpose (March and Smith ,1995). We aim to construct a reference model that contributes to practice. Here are two descriptions of a reference model in information systems context. In (Fettke and Loos, 2007)- "An information system reference model is a typical, or paradigmatic model, which describe the information system or a well-identified part of it.". And (Rosemann, 2003) describes reference model as "Reference models are generic conceptual models that formalize recommended practices for certain domain.". For the empirical basis, we couple design science research approach with qualitative research methods namely expert interviews with experts in the field of cyber security and risk management, and case study method (Eisenhardt, 1989). The cases focus on vulnerability analysis, and threat and attack scenarios to help us understand and analyse threats, risk factors and impacts deeply. The current status of the threat model includes results from literature, two expert interviews, and a design study on enterprise identity management system.

3 DIGITAL IDENTITY MANAGEMENT

We follow the notion of Evans Pughe (Evans Pughe, 2008) who defines digital identity as *"digital identity is the growing mass of information about ourselves and our social or business transactions and relationships that exists in digital form whether stored within commercial or government databases."* Digital identities are representations of entities. An entity is a generic term that refers to an active agent capable of initiating or performing a computation of some sort (for example, an end user invoking a command or a program, a programming agent acting on behalf of a user, a running daemon process, a thread of execution, a hosting system or a networking device) (Benantar, 2006; Staite and Bahsoon, 2012). This definition broadens our understanding of what entities can digitally be represented.

Identity management covers aspects from tools to processes that are used to represent and administer digital identities in different contexts depending on association of different information with each identity. Protecting identity and its management is among the most critical security concerns(Staite and Bahsoon, 2012). For this study IdM is of particular interest as it is a security subsystem by itself. IdM is not only a technical concept but also an interdisciplinary topic, which can be studied from various perspective and fields of study such as sociology and philosophy. For the sake of this research we go beyond the computer science / network security perspective and adopt a more holistic information systems and IT security perspective.

4 THREAT ANALYSIS

Security is about protecting what is considered to be an asset to individual users and organizations from misuse and malicious acts. Securing a system is vague unless one tends to be specific and clear about system behavior and assets, attackers' resources and the system's' security requirements as discussed by (Jason and Mitchell, 2011). Security requirements are driven by security threats and identification of such threats is part of securing information systems as it involves identifying threats and challenges which need to be addressed by implementing appropriate countermeasures and realistic security requirements (Zissis and Lekkas, 2012).

(Shostack, 2014) describes the term asset as something of value and highlights the three ways it is commonly used in threat modeling. They are: things attacker want, things one wants to protect, and stepping-stone to either of these. Accordingly asset could be an abstract or concrete resource of value (e.g. private data, user passwords or keys, services, processes, money, confidential business data, reputation, etc.). Weaknesses in systems can be exploited by attackers to gain unauthorized access to a system compromising it to gain access to assets and resources of the system. Such threats, if not handled well, lead to interruptions or destruction of any valuable service or data.

In scholarly literature and practitioners' reports, several authors defined and described threat modeling

and its importance in security analysis and secure software development (Myagmar, 2005; Möckel and Abdallah, 2010; Dominicini et al., 2010). According to (Jason and Mitchell, 2011), threat analysis is a formal process of identifying, documenting and mitigating security threats of a system. Cyber threat analysis, as defined by (Kostadinov, 2014), is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks. One of the main goals of threat analysis is to help identify emerging threats and analyze attacks. Once threats are analyzed it is possible to factor the risks and business impacts and decide on how to reduce the risk by applying effective security measures (UcedaVélez and Morana, 2015).

Threat modeling is a phase in threat analysis and it consists of a system, assets, and an attacker as components. It usually involves characterizing a given system (using UML, State diagram, Data Flow diagram, etc.), identifying its assets and access points and identifying threats, and determining vulnerabilities (Dominicini et al., 2010; Myagmar, 2005). The three popular approaches to threat modeling are asset centric, attacker centric and software centric approaches (Shostack, 2014). The approaches are named after the focus and perspective used to implement the threat modeling i.e. asset, attacker, and software. Software-centric models focus on the software being built or a system being deployed (Shostack, 2014). Asset-centric focus on protection of assets and involve identifying assets of an organization entrusted to a system or software (Möckel and Abdallah, 2010). Attacker-centric approach focuses on profiling an attacker's characteristics, skill set and motivation to exploit vulnerabilities in order to identify threats (Shostack, 2014).

4.1 A Reference Threat Analysis Model for Identity Management

In this section we discuss our proposed model to support threat analysis for digital identities. Security threats to identities come from every direction. Vulnerabilities from system architectures, deployment environments, and management processes contribute to the overall threats to identity. The model was constructed from the preliminary result of our literature analysis and a case study conducted on system customization. Figure 1 depicts current version of model and it represents various components that we believe are important to consider while doing threat analysis for digital identity management.

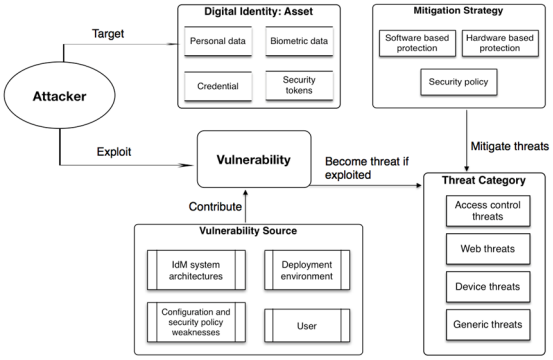

Figure 1: A Reference Threat Analysis Model For IdM.

The central part of the model is ***digital identity: asset*** to signify identities as assets and a primary target of attackers. Depending on the context and the entity to represent, a digital identity may consist various attributes such as personal or private data (e.g. name, birth date, credit/debit card information, identification number), biometric data (e.g. fingerprint, hand geometry, retina scans, iris scans, face recognition), credentials to access systems (e.g. passwords, PIN, certificate), and can be in a form of security tokens (e.g. smart cards, encrypted token).

A digital identity has a lifecycle with ***management processes*** from being assigned to an entity until its disposal. Part of the identity information (selected attributes) is used for authentication and authorization i.e. access control purpose. Identity maintenance and revocation are among the identity management processes as well. In the model, major management processes in identity management are included (as described in Jøsang et al., 2007, Slamanig and Stranacher, 2014). Provisioning is the creation of the identity record and its population with the correct attributes. Access control refers to the processes used to control access to specific assets. Authentication and authorizations are the major processes in this category where a person or an entity, in general, is verified against who he/she claims to be and the access right to system resources. Termination is removing identities from the system once they are at the end of their lifecycle. According to (Shostack, 2014), a process might disclose information (e.g. leaking memory address, etc.) that inform further attacks. Threats to identity management processes are part of the model, as we want to study and identify vulnerabilities of these processes.

There are various systems and tools, commonly known as *identity management systems* that support the effective use and protection of digital identities. These systems are implemented in different ***identity***

management system architectures. The three main architectural models widely used are centralized, isolated and federated models. The classification is based on deployment of the various components of the systems such as identity data storage and users access control. The architectures might have different implications on threats due to their mode of operation. Unlike other models, federated model allows inter-organization and interdependent management of identity rather than internal use only (Bhargav-Spantzel et al., 2005; Ahmad et al., 2010; Bertino and Takahashi, 2010) which may contribute to system vulnerability differently from other architectural models.

Identity management systems can be deployed on premise, on the cloud, mobile devices or combination of any of the platforms. We would like to consider contribution of ***deployment environments*** of IDM systems to threats, as the maturity level of the platforms in terms of efforts to include improved security technologies is different (e.g. strong authentication) (Novakouski, 2013). We also extend our view on potential threat targets to include services and interactions, (business) processes, hardware and media. This allows us to have a comprehensive analysis and better organization of threats. On the model, the vulnerabilities component represents weaknesses in the system architecture, deployment environment or management processes. It is worth considering as threats can be facilitated by the presence of vulnerabilities and security control gaps exposing assets to potential exploits. ***Mitigation plan*** completes a threat analysis process. It constitutes protection mechanisms, and security controls to countermeasure those threats and vulnerabilities found likely for exploitation (Siponen and Vance, 2010; Bulgurcu et al., 2010).

When complete, we aim the model to support threat analysis and modeling for identity management by comprising threats and vulnerabilities that primarily target identities, attackers techniques, and mitigation plans. This is to simplify the analysis process and support system designers, risk managers, and/or stakeholder interested in security analysis of digital identities. Best practices and important parameters are opted to be included in the reference model and procedures. For specific systems, one has to instantiate it accordingly as requirement, architecture, deployment environment, and other aspects of systems vary from one another.

5 OUTLOOK

In this paper we presented our ongoing research on security threat analysis and modeling for identity management. We also proposed a model to support threat analysis for digital identity. The model is in its infancy as it is constructed based on preliminary results from our literature review and a case study conducted on identity management system customization. More work is ahead of us with threat analysis, and refinement of the proposed model by identifying threats that primarily target identities from the various sources of vulnerabilities. This allows having a validated counter measure in place for the identified threats.

ACKNOWLEDGEMENTS

This research has been funded within the Marie Curie Research & Innovation Actions by the European Union Seventh Framework Program FP7/2007-2013 under REA grant agreement n°_317382, NITIMesr.

REFERENCES

Ahmad, Z., Suziah, K. & Manan, A., 2010. A Study on Threat Model for Federated Identities in Federated Identity Management System. , pp.618–623.

Benantar, M., 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Springer.

Bertino, E. & Takahashi, K., 2010. *Identity Management: Concepts, Technologies, and Systems*, Artech House.

Bhargav-Spantzel, A., Squicciarini, A.C. & Bertino, E., 2005. Establishing and protecting digital identity in federation systems. *Proceedings of the 2005 workshop on Digital identity management*, 14(3), pp.11–19. Available at: http://iospress.metapress.com/content/FRCJV8NFEMH5DXC9\nhttp://doi.acm.org/10.1145/1102486.1102489.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly*, 34(3), pp.523–548.

Dominicini, C. et al., 2010. Threat Modeling an Identity Management System for Mobile Internet. In *Proc. of the 9th International Information and Telecommunication Technologies Symposium (I2TS'10)*.

Dong, X., Clark, J. a. & Jacob, J.L., 2008. Threat modelling in user performed authentication. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5308 LNCS, pp.49–64.

Dutt, V., Ahn, Y.-S. & Gonzalez, C., 2012. Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 55(3), pp.605–618. Available at: http://hfs.sagepub.com/cgi/doi/10.1177/001872081 2464045 [Accessed May 4, 2015].

Eisenhardt, K., 1989. (1989) Building theories from case study research A. M. Huberman & M. B. Miles, eds. *Academy of Management Review*, 14(4), pp.532–550.

Evans Pughe, C., 2008. A crisis of identity. , (June). Available at: www.theiet.org/engtechmag.

Fettke, P. & Loos, P. eds., 2007. *Reference Modeling for Business Systems Analysis*, Idea Group Publishing.

Jason, B. & Mitchell, J.C., 2011. Security Modeling and Analysis. *IEEE Security and Privacy*, 9(June), pp.18–25. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5708126.

Kostadinov, D., 2014. Cyber Threat Analysis. *Infosec Institute*. Available at: http://resources.infosecinstitute.com/cyber-threat-analysis/.

March, S.T. & Smith, G.F., 1995. Design and natural science research on information technology. *Decision Support Systems*, 15, pp.251–266.

Möckel, C. & Abdallah, A.E., 2010. Threat modeling approaches and tools for securing architectural designs of an e-banking application. *2010 6th International Conference on Information Assurance and Security, IAS 2010*, pp.149–154.

Myagmar, S., 2005. Threat Modeling as a Basis for Security Requirements. *In StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability*, pp.94–102.

Novakouski, M., 2013. User-Centric Identity Management: A Future Vision for IdM. *CrossTalk: The Journal of Defense Software Engineering*, 26(September-October).

Paintsil, E., 2013. Towards Automation of Privacy and Security Risks Analysis in Identity Management Systems. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp.720–727. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6680907 [Accessed April 21, 2015].

Pudar, S., Manimaran, G. & Liu, C.-C., 2009. PENET: A practical method and tool for integrated modeling of security attacks and countermeasures. *Computers & Security*, 28(8), pp.754–771. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000522 [Accessed August 3, 2015].

Pwc, 2011. Cybercrime: Global Economic Crime Survey. , (November). Available at: www.pwc.com/crimesurvey.

Rosemann, M., 2003. Application Reference Models and Building Blocks for Management and Control. In P. Bernus, L. Nemes, & G. Schmidt, eds. *Handbook on Enterprise Architecture SE - 17*. International Handbooks on Information Systems. Springer Berlin Heidelberg, pp. 595–615. Available at: http://dx.doi.org/10.1007/978-3-540-24744-9_17.

Shostack, A., 2014. *Threat Modeling: Designing for Security*, John Wiley & Sons, Inc.

Siponen, M. & Vance, A., 2010. Neutralization: New Insights Into The Problem Of Employee Information Systems Security Violations. *MIS Quarterly*, 34(3), pp.487–502.

Slamanig, D. & Stranacher, K., 2014. User-Centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure. , pp.153–163.

Staite, C. & Bahsoon, R., 2012. Evaluating identity management architectures. In *Proceedings of the 3rd international ACM SIGSOFT symposium on Architecting Critical Systems - ISARCS '12*. New York, New York, USA: ACM Press, p. 11. Available at: http://dl.acm.org/citation.cfm?doid=2304656.2304659.

Stango, A., Prasad, N.R. & Kyriazanos, D.M., 2009. A threat analysis methodology for security evaluation and enhancement planning. *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*, pp.262–267.

UcedaVélez, T. & Morana, M.M., 2015. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*,

Xu, D. & Nygard, K., 2005. A Threat-Driven Approach to Modeling and Verifying Secure Software., pp.342–346.

Zissis, D. & Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), pp.583–592. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167739X10002554 [Accessed July 11, 2014].