Insider Threat Mitigation Using Moving Target Defense and Deception

Hassan Takabi
Department of Computer Science and Engineering
University of North Texas
Denton, Texas, USA
Takabi@unt.edu

J. Haadi Jafarian
Department of Computer Science and Engineering
University of Colorado Denver
Denver, Colorado, USA
Haadi.Jafarian@ucdenver.edu

ABSTRACT

The insider threat has been subject of extensive study and many approaches from technical perspective to behavioral perspective and psychological perspective have been proposed to detect or mitigate it. However, it still remains one of the most difficult security issues to combat. In this paper, we propose an ongoing effort on developing a systematic framework to address insider threat challenges by laying a scientific foundation for defensive deception, leveraging moving target defense (MTD), an emerging technique for providing proactive security measurements, and integrating deception and MTD into attribute-based access control (ABAC).

CCS CONCEPTS

• **Security and privacy** → *Formal methods and theory of security*; *Intrusion detection systems*; *Access control*; *Human and societal aspects of security and privacy*;

KEYWORDS

Insider Threat, Moving Target Defense, Deception, Attribute-based Access Control

1 INTRODUCTION

The threats from malicious insiders is a complicated challenge for organizations and are considered the most damaging and costly threat [10]. The computer emergency response team (CERT) defines a malicious insider as a current or former employee who has or had authorized access to an organization's information systems and has intentionally used that access to influence the confidentiality, integrity, or availability of the organization's information systems [15]. A report produced by the security management company AlgoSec in 2013, found that the majority of the information security professionals view insider threat as their primary organizational risk [1]. In 2015, a Federal Cybersecurity survey of 200 federal IT managers showed that 76% of the participants are concerned about leaks from insider threats [16]. Furthermore, just last year a report from the Ponemon Institute studied cyberattacks cases for over 237 companies in six countries around the world found that insiders threat was the most expensive attack and cost companies an average of $167,890 annually and this cost is likely to increase in the future [10].

Insider threat problem has been extensively studied, and various detection approaches have been proposed. These methods range from technical approaches such as process analysis, decoys, and honeypots, etc. to behavioral approaches based on psychological theories [4][5][7]. However, it still remains one of the most difficult security issues to combat. In this paper, we present an ongoing effort to alleviate this problem by developing a systematic framework that aims to lay a scientific foundation for defensive deception, leverage moving target defense (MTD) techniques, and integrate those methods into attribute-based access control (ABAC) model. Deception and MTD both aim at defeating insider threats one by misrepresenting the facts and the other by frequently changing the facts. The rest of the paper is organized as follows. Our proposed framework

- presents a deception logic that models both perlocutionary and quantitative (probabilistic) dimensions of deception, and an approach to generate coherent and affordable deception plans for insider threat prevention.
- leverages moving target defense (MTD) which is a promising paradigm based on the idea of proactively changing, e.g., moving, system configurations in an effort to deter potential future attacks. The goal is to increase the cost and time burden on the attacker to achieve an unauthorized access.
- integrates deception and MTD into ABAC, introduces the notion of honey elements in ABAC and extends ABAC model for insider threat detection.

In section 2, we provide a brief background information about the attribute-based access control (ABAC) and moving target defense (MTD). Section 3 describes our proposed framework and its components. Section 4 presents related work. Finally, section 5 concludes the paper.

2 BACKGROUND INFORMATION

Attribute-based access control (ABAC) has emerged as a promising alternative to traditional models (i.e., discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC)) and has drawn significant attention from both academia and industry. ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request. The U.S. National

MIST'17, October 30, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-5177-5/17/10…$15.00
https://doi.org/10.1145/3139923.3139935

Institute of Standards and Technology (NIST) defines attribute-based access control (ABAC) as "An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions" [6]. We define an ABAC policy π as a tuple $\{U, R, Op, A_u, A_r, d_u, d_r, Rules\}$, where U is set of users, R is set of resources, Op is a set of operations, A_u is set of user attributes, A_r is set of resource attributes, d_u represents user attribute data, d_r represents resource attribute data, and $Rules$ is a set of rules. The user-permission relation induced by a rule ρ is $[[\rho]] = \{\langle u, r, o\rangle \in U \times R \times Op | \langle u, r, o\rangle | = \rho\}$. Note that U, R, d_u and d_r are implicit arguments to $[[\rho]]$. The user-permission relation induced by a policy π with the above form is $[[\pi]] = \bigcup_{\rho \in Rules}[[\rho]]$.

Moving target defense (MTD) is an emerging paradigm for providing security guarantees by proactively changing, e.g., moving, the configurations of a protected system [8] . Opposed to traditional approaches which assume security configurations remain immutable, MTD strives to reduce the possibility of a successful attack by negating any advantages the attacker may have. For instance, complicating the reconnaissance process in which an attacker gathers information about the current configurations of the victim system; or by deterring ongoing attacks that were crafted based on previously-discovered (and later changed) configurations. In addition, MTD strives to increase the cost : overall deployment time and number of internal or external components of the victim system that need to be compromised in order to carry on a successful attack. Finally, effects to the usability of the protected system, e.g., response time and end-user access patterns, should be minimized in an effort to prevent run-time inconveniences that may complicate the adoption of MTD-based techniques in practice.

3 THE PROPOSED FRAMEWORK

In order to address insider threat challenges, we propose a framework that combines defensive deception, moving target defense and ABAC as shown in Figure 1. We first lay a scientific foundation for defensive deception and build a framework to generate coherent deception plans. Next, we develop an approach to leverage moving target defense techniques based on attribute-based access control (ABAC) model. We, then integrate both deception and MTD into ABAC.

ABAC relies on specifying, collecting and processing attributes belonging to access entities involved in a given request (e.g., users, protected resources, and the environment). In such a context, the unintended assignment of attributes to entities may completely compromise the security of the access mediation process. Based on this problem, we assume a threat model where the attributes listed in a given policy can become compromised by an attacker, for example, by creating an unintended attribute-access entity assignment, or by deliberately manipulating the value or set of values depicted by a correctly-assigned attribute. Particularly troubling is an insider who can issue themselves new attributes or otherwise compromises one of the attribute provisioning systems. In this case, an insider can escalate their privileges to compromise the security of the system.

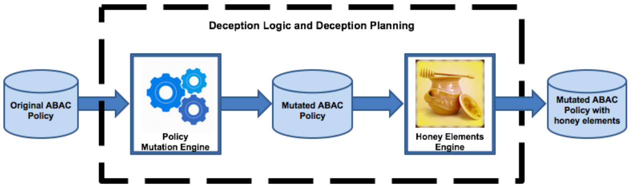

Figure 1: The Proposed Insider Threat Mitigation Framework

3.1 Defensive Deception for Insider Threat

Although deception is not new and it has been explored for insider threats mitigation [9, 12, 14, 18], most of the focus has been on individual and random deception systems or techniques where each pursues its own isolated goal with limited effectiveness. Traditionally, the focus has been on deployment of honey* (honeypots [13], honey file [19], honey routers [3]) technologies in place of the network that are potentially of interest to insiders. However, these technologies, unless meaningfully and consistently combined, have limited effectiveness against insiders who are usually informed and use stealthy and persistent reconnaissance and exploitation techniques. Instead, defeating such informed insiders requires a meaningful combination of these deception techniques in a coherent and consistent deception plan that maximally engages the insiders, leads them to the desired false conclusions, and is not easily susceptible to detection. These false conclusions would then persuade the insider to adopt a false course of action in her planning, thus leading to a high benefit for defense against insider threats. For example, instead of configuring each honeypot individually, we configure a group of honeypots in coordination, by considering the attack graph of potential multi-step insider infiltration into our system, our defense priorities and insiders' potential goals and motifs.

To this aim, We need to revisit the defensive role of deception and unleash its full potentials for insider threat prevention and detection, by redefining cyber deception as a planned and goal-oriented combination of deception techniques. This requires a deception planning framework that provides necessary paradigms for defining various deception actions, along with their inter-dependencies, benefits, and costs. More importantly, such framework must provide paradigms for modeling how such deceptive actions would as a whole manipulate cognitive thinking process of insiders with different goals and sophistication levels. It must also be able to reason and identify the most beneficial deception plan with the given budget.

Our goal is to lay a scientific foundation for defensive deception, by (i) providing a formal definition of deception as manipulating cognitive thinking process of an adversary (insider in our case), (ii) presenting a deception logic that models both perlocutionary and quantitative dimensions of deception, and (iii) augmenting this modeling logic with necessary quantitative reasoning paradigms to generate coherent and affordable deception plans.

Formally, we define deception planning as identifying a set of deceptive actions that achieves a deception goal against insider threats with maximum benefit and minimum (or budget-constrained) cost.

A formal model of deception must model at least the following core components:

- Attributes: it must be able to model attributes, which usually consists of configurations and parameter values of the system.
- Beliefs: it must be able to model beliefs as insider's expected perception of facts, which may or may not be different from reality and actual values of the facts.
- Actions: it must be able to model potentially deceptive representation of the facts in the system and their manipulative effect on adversary's perception of facts (beliefs). The model must also be able to define inconsistency among actions because inconsistent actions would reveal the deception plan.
- Attacker Types: it must be able to model This could be done using information about the level of access the employee has as well as the psychosocial reasoning that uses a data-driven approach based on personnel data that are likely to be available [5].
- Deception Goal: it must be able to model deception intention as a set of perceptions (beliefs) to which insider is intended to be driven. Conceptually, the intention of deception in a generic context is to make insider develop certain false beliefs. In other words, this intention is to induce insider toward certain states of knowledge about some facts in the system. However, in order to allow scientific reasoning for cyber deception, and make various deception models comparable, we need to quantify the benefit associated with each potential deception plan.
- Causation rules: most importantly, it must also be able to model cognitive thinking process of a potential insider and the effect of deceptive actions on it. This is done by a set of rules that define how a combination of certain facts, actions, and/or belief induces a consequent belief in insider's mind and how insider's beliefs over a fact or group of facts affect her beliefs about another fact. These causation rules link actions to the intention.
- Deception Plan: The deception plan is a solution to the augmented deception model, that is defined in the framework using the deception logic. To this aim, the deception framework augments the deception model with additional constraints (e.g., for calculating state likelihoods), and rewrites causality rules and deception goals as SMT constraints. Then, using an underlying SMT solver, the framework solves the model and determines appropriate assignments to variables.

Although our main focus is on insider threat, the proposed deception framework provides logic, interfaces, and mechanisms for fabricating deception plans for any given domain, and for interacting with the domain to deploy the plan, as well as updating the plan based on feedback. The logic is an abstraction over satisfiability modulo theories (SMT), that is able to model perlocutionary aspects of deception (e.g., belief, cause-and-effect, and intention), as well as its quantitative traits (belief likelihoods, budget, and exposure risk). The framework includes necessary mechanisms for validating and solving the model in order to generate a sound deception plan.

This deception modeling problem is reducible to 0-1 knapsack problem, where beliefs are items, impacts are their item values, costs are their weights, and budget is the maximum weight capacity. The knapsack problem is known to be NP-hard. This is why we convert the problem to a satisfiability problem, using generalized Boolean/arithmetic format of satisfiability modulo theories (SMT) [2], in order to make it solvable in a scalable manner. SMT formulas provide a much richer modeling language than is possible with Boolean SAT formulas. Although satisfiability problems are NP-complete in general, recent advances in SMT solvers have made them scalable to problems with millions of variables [11].

The framework should also incorporate probabilistic deception to determine probabilities of deception success and failure into the framework and its effect on insiders' beliefs. This can be done by adding probabilities to causation rules.

Additionally, the framework should include adaptive deception which refers to the process of adapting the deception plan to recently collected knowledge regarding insider's type and knowledge. Information collected regarding an insider can have an effect on the deception model in two distinct manner. Firstly, the collected knowledge regarding insider may change assumption about adversary types. Secondly, it may allow framework to determine the state of insider's knowledge regarding some facts. This new information regarding insider's knowledge can be incorporated into the model, by asserting them as tautological causality rules (rules without antecedents). The objective is to devise a reactive deception plan that considers insider's partially-observable actions in real-time composition of the plan, while avoiding insider's potential counter-deceptions.

3.2 Moving Target Defense for Insider Threat Mitigation

Although Moving target defense (MTD) has been extensively investigated in cyber defense literature, most of the work focuses on outside attackers and to the best of our knowledge, this is the first work to utilize MTD for defense against insider threats. The key idea of MTD is to increase the difficulty and cost to an attacker to perform a successful attack: if the insider does not know the exact attributes used in the access control decision, then the insider's attack is either unsuccessful or much more expensive (i.e., must compromise many attributes). In our approach, we propose to analyze the actual access requests to discover additional attributes that are correlated to the original attributes in a given authorization policy. Taking an original authorization policy as an input, our approach first obtains the original attributes listed in the policy and inspects the attribute set to locate attributes that are correlated to the original ones by leveraging well-established machine learning techniques. Later, these newly-extracted attributes are used to enhance the original policy, by adding additional constraints to existing policy rules, thus producing a new mutated policy that is then forwarded to the access mediation infrastructure for enforcement.

The intuition behind this approach is that the entities involved in a given access request typically exhibit additional attributes besides the ones in the original policy. In our system, if the original attributes are compromised, the newly-extracted ones may still deter the unintended exploitation of the original policy. Furthermore, the insider does not know which of the additional attributes will be checked, which will increase the cost and time burden on the attacker to compromise additional attributes to finally achieve an unauthorized access. In addition, we aim to mitigate the harm to usability, such as end-users no longer able to access previously-available resources, by striving to obtain a high degree of correlation between the original attributes and the newly-extracted ones. Our approach to solve this challenge is intended to dynamically expand ABAC policies by detecting the attributes that are strongly correlated to the entities involved in access requests. By mutating policies, an ABAC system can increase resilience to attack and increase complexity and cost to an attacker.

We will develop techniques based on deep neural networks to address these issues. Specifically, we propose to use deep belief networks (DBNs) to exploit certain features (e.g. inductive bias) offered by neural networks. We generalize the knowledge from the logs which is used to train a deep belief network (DBN). The generative power of such deep belief networks (DBNs) allows us to obtain insights about certain parameters that are significant in generating good candidate rules from a small amount of logs and to find the policy most likely to generate the behavior (usage of entitlements) observed in the logs.

The framework also introduces the notion of “honey permission" which are defined as permissions that exceed the authorized access [9] and the notion of “honey attribute" into ABAC to be used with the deception plan. The goal is to detect an attempt to access sensitive resources by unauthorized users without allowing the insider actually access the sensitive resources. Integrating deception and policy mutation into ABAC increases burden for insiders. The deception logic presented here is used to model and automatically generate deception plan and ... for insider threat mitigation purpose.

4 RELATED WORK

Designing efficient and scalable frameworks for monitoring and detecting the malicious insiders is a significant research interest. Many research studies have been investigating and analyzing the problem, and many approaches have been provided include implementing security awareness frameworks, separation of duties and least privilege, anomaly detection, etc. Deception has been used in insider threats [14][12][18] [9]. Honey* is often used as an umbrella term for deception systems. The quintessential example of these systems are honeypots; decoy resources that are placed in a computing system or network to be probed, attacked and compromised by the attackers. For example, Thompson et al. present a content-based framework to detect insider anomalies in accessing documents and queries [12]. Salem et al. apply the machine learning techniques to identify the malicious intent in information gathering commands [14]. Kaghazgaran et al. proposed a model to consolidate honey permissions into role-based access control [9]. Also, Park et al. introduce a software-based decoy system to entrap malicious insiders [18]. Other approaches exploit the psychological behaviors of the insiders. For example, Greitzer et al. present a comprehensive view of psychological approaches combined with a computational approach to detecting the insider [4]. Theoharidou et al. propose various criminology and related social science theories on the behaviors of insiders [17].

5 CONCLUSION AND FUTURE WORK

The insider threats have become a growing challenge, and many studies have focused on mitigating such attacks. In this paper, we have presented an ongoing work on a new framework that combines moving target defense techniques, defensive deception, and attribute-based access control (ABAC) to provide a proactive approach for insider threat detection and mitigation. This framework is just a starting point and developing its components in detail require a big effort which is focus of our ongoing work. Once the framework is developed, evaluating different components and the framework as a whole will be the next step.

REFERENCES

[1] AlgoSec. 2014. AlgoSec Survey:State of Network Security 2014. (2014). "http://www.algosec.com"

[2] Nikolaj Bjørner and Leonardo de Moura. 2009. $Z3^{10}$: Applications, Enablers, Challenges and Directions. In *Sixth International Workshop on Constraints in Formal Verification Grenoble, France.*

[3] Abdallah Ghourabi, Tarek Abbes, and Adel Bouhoula. 2009. Honeypot router for routing protocols protection. In *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on.* IEEE, 127–130.

[4] Frank L Greitzer and Deborah A Frincke. 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security.* Springer, 85–113.

[5] Frank L Greitzer, Lars J Kangas, Christine F Noonan, Angela C Dalton, and Ryan E Hohimer. 2012. Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *System Science (HICSS), 2012 45th Hawaii International Conference on* (2012), 2392–2401.

[6] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2014. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (2014).

[7] Jeffrey Hunker and Christian W Probst. 2011. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *JoWUA* 2, 1 (2011), 4–27.

[8] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and X. Sean Wang. 2011. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats* (1st ed.). Springer Publishing Company, Incorporated.

[9] Parisa Kaghazgaran and Hassan Takabi. 2015. Toward an Insider Threat Detection Framework Using Honey Permissions. *Journal of Internet Services and Information Security (JISIS)* 5, 3 (2015), 19–36.

[10] Ponemon Institute LLC. 2016. Cost of Cyber Crime 2016: Reducing the Risk of Business Innovation. (2016). https://saas.hpe.com/en-us/marketing/cyber-crime-risk-to-business-innovation

[11] Leonardo Moura and Nikolaj Bjørner. 2009. Formal Methods: Foundations and Applications. Springer-Verlag, Berlin, Heidelberg, Chapter Satisfiability Modulo Theories: An Appetizer, 23–36. https://doi.org/10.1007/978-3-642-10452-7_3

[12] Younghee Park and Salvatore J Stolfo. 2012. Software decoys for insider threat. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security.* ACM, 93–94.

[13] Niels Provos et al. 2004. A Virtual Honeypot Framework.. In *USENIX Security Symposium*, Vol. 173.

[14] M Ben Salem and Salvatore J Stolfo. 2009. Masquerade attack detection using a search-behavior modeling approach. *Columbia University, Computer Science Department, Technical Report CUCS-027-09* (2009).

[15] George Silowash, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J Shimeall, and Lori Flynn. 2012. *Common sense guide to mitigating insider threats 4th edition.* Technical Report. DTIC Document.

[16] SolarWinds. 2015. SolarWinds Survey Investigates Insider Threats to Federal Cybersecurity. (2015). http://www.solarwinds.com/company/newsroom/press_releases/threats_to_federal_cybersecurity.aspx

[17] Marianthi Theoharidou, Spyros Kokolakis, Maria Karyda, and Evangelos Kiountouzis. 2005. The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security* 24, 6 (2005), 472–484.

[18] Paul Thompson. 2004. Weak models for insider threat detection. *International Society for Optics and Photonics,Defense and Security* (2004), 40–48.

[19] Jim Yuill, Mike Zappe, Dorothy Denning, and Fred Feer. 2004. Honeyfiles: deceptive files for intrusion detection. In *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC.* IEEE, 116–122.