Real-time Contextual Intrusion Detection

Emergent Research Forum papers

Abdul Rahim Charif
Citrix Systems Inc., Nova Southeastern University
ac1835@mynsu.nova.edu

Executive Summary:

Cybersecurity is a growing problem. Cyber-threats are now affecting society on personal, organizational and national levels. Current threat detection and prediction models are far from being operational in realistic scenarios. Suggested threat detection approaches in current research are merely prototypes trained and tested with similar data sets, relying on well-known attacks and attack signatures steps. Attack prediction detection models suffer from false positives. In this paper, we present context-based threat detection model using design science. Our proposed detection model decreases false positives with greater detection of malicious activities. The proposed detection system aligns with organizational information security policies to provide better detection of insider threats.

In order to implement this model in an organization, activities, roles, views and context at which the organization operates should be well defined. Users of the organizational information system are assigned roles to which they are allowed to achieve certain goals by running certain activities. Those activities are associated with specific views of organizational resources. The detection system will evaluate access to resources based on the context of the request and would report any possible violations that users may attempt.

Our proposed detection model offers reduced false positives with greater detection of malicious activities compared to other threat detection models. The proposed detection system aligns with organizational security policies ensuring the detection of insider threats.

Keywords

Threat Detection; Intrusion Detection; Real-time Situational Awareness; Design Science

Introduction:

Cybersecurity is a growing concern amongst organizations, as they are becoming more aware of the numerous threats to their critical information assets, and the heavy costs associated with the corruption, loss, or theft of such information. According to a survey conducted by Vormetric (Poll, 2015), 40% of the participating organizations experienced a data breach, or failed a compliance audit in 2014; with 89% perceiving their organization was at greater risk to insider incidents. Furthermore, 19% of respondents in a survey indicated that costs due to insider threat might result in over $5

million USD (Cole, 2015). This has led to organizations increasing their spending to maintain or improve on cybersecurity to address the internal threats (Poll, 2015).

Organizations address insider threats by implementing both technical and managerial controls. A viable solution to addressing the insider threat problem is the use of intrusion detection systems (IDS) (Mohan, Vaidehi, A, Mahalakshmi, & Chakkaravarthy, 2015). IDS produce alerts to indicate malicious activity is taking place based on well-known attacks and attack signature steps (Fayyad & Meinel, 2013). Alternatively, managerial controls such as information security policies (ISPs), and security education, training and awareness (SETA) programs are used to manage employees' behaviors with regards to information assets (Guo, Yuan, Archer, & Connelly, 2011). However, current controls are limited in addressing the insider threat problem.

Technical solutions, such as IDS and IPS, produce many false positives, which are alerts produced to indicate malicious activity is taking place, when in fact the activity is legitimate. On the managerial side, ISPs are developed to align with the objectives of the organization, and specifies roles and responsibilities for employees; yet, employees are not always complaint with ISPs (Guo et al., 2011). Employees may violate ISPs maliciously or non-maliciously, which further increases the risk posed by insider threat (Guo et al., 2011).

The aim of this paper is to propose a threat detection model that overcomes the limitations of current technical and managerial approaches to the insider threat problem. We propose a context-based threat detection model that would reduce false positives and better detect malicious activities. While, current approaches to threat intelligence and intrusion detection mostly rely on aggregations of network events, we believe that detection of unwanted or malicious activity on any system can be captured by modeling the context of system activities. Any activity that does not align with security policies and defined context can be considered malicious. This approach will allow us to overcome the limitation of current intrusion detection systems that either focus on signature activities or focus on attempting to predict unusual activities.

Our threat detection model contributes primarily by proposing a more accurate solution to current threat detection approaches. Specifically, current systems are limited in detecting malicious insider activity due to high rates of false positives; a context-based threat detection model would reduce false positives, which would lead to more effective detection of malicious or non-malicious activity, primarily by insiders. Secondly, any misalignment with ISPs is reduced through the implementation of our context-based threat detection model. The constraints and restrictions articulated within the ISPs are captured through the various contexts within the threat detection model. Essentially, any security requirement or limitations developed at the ISP level, which are aligned with the objectives of the organization, can be implemented properly at the technical level using the context-based threat detection model. Finally, complexity is reduced as opposed to current threat detection models. Current threat detection models rely on large amounts of data to process, which can create problems such as slow rate of learning and increased detection time (Devaraju & Ramakrishnan, 2011). Our threat detection model provides a more coherent approach whereby malicious insider activity could be detected based on the context under which an employee had access to

particular information. The following sections would discuss the related work, our research approach, and finally the discussion and conclusion.

Related Work:

Traditional intrusion detection systems focus on detecting malicious packets on a computer network (Anderson, 1980). It is the network or system administrator responsibility to track IDS alerts. Network and security managers must have complete situational awareness in order to understand the impact of the attack on the network. Commercial IDS have developed from generating low level alerts to creating an administrator friendly high level alerts and in some cases visualized for ease of interaction (Mathew, Giomundo, Upadhyaya, Sudit, & Stotz, 2006). For IDS to be proactive to network attacks and threats, it must infer context of activities; recognizing events is not sufficient for detecting malicious attacks. Current attack detection techniques are far from being operational outside of their testing environment and inside real networks. Detection systems are trained and tested with similar data sets (Cipriano, Zand, Houmansadr, Kruegel, & Vigna, 2011), relying on well-known attacks and attack signatures steps (Fayyad & Meinel, 2013). Such systems make assumptions that cannot reflect in operational networks such as sensibility to attackers generated noisy IDS alerts. The knowledge acquired from correlating IDS alerts was merely enough to deduce attacker's next step. Using an attack library, signature of attacks (Ning, Cui, Reeves, & Xu, 2004), or construction of activities based on correlation of intrusion alerts (Ning, Cui, & Reeves, 2002)(Qin, 2005) is simply not sufficient to proactively detect threats.

More recently, (Ding, Aleroud, & Karabatis, 2015) used a similar approach by aggregating packets into network flows and correlated them with security events generated by signature attacks. Such approaches rely on different levels of predefined knowledge about attacks, the proposed techniques are not able to provide valid alert correlations for unknown attack relations. Recent approaches focus on prediction models. (Cipriano et al., 2011) correlated IDS alerts into attack sessions stored in a hash table which is input to a training algorithm. Additionally, (Katipally, Yang, & Liu, 2011) applied mining IDS alerts and used them as input to a Hidden Markov model (HMM) to predict the behavior of attackers for the purpose of profiling them. Similarly, (Luktarhan, Jia, Hu, & Xie, 2012) used HMM for modeling complete attack scenarios, however, their applicability to operational networks is questionable, in addition to the ability to offer real time protection. Alert analysis input to the model requires expertise knowledge, which affects its efficiency by human factors. However, we found similarity in our approach with (Luktarhan et al., 2012), as the focus on the behavior analysis rather than packet level analysis.

Research Approach:

In this paper, we follow design science research paradigm to introduce a threat detection model. The design science research paradigm addresses relevant research problems and introduces solutions that solve these problems in a more efficient manner (Gregor & Hevner, 2013)(Hevner, March, Park, & Ram, 2004). Design science artifacts

are collections of ideas and capabilities that enables the development of systematic solutions for the problem under study. The artifacts may comprise of a set of constructs, models or even a set of symbol that provide abstractions, methods and prototypes explaining the process of systematic implementation.

Information system research following the design science paradigm can apply three different research methodologies; constructivist paradigm, positivist paradigm and developmentalist paradigm (also called socio-technologist paradigm). In this paper we take a socio-technologist stance to achieve our research objective. We believe that a socio-technologist stance will provide a balance between a positivist and a constructivist paradigm. The socio-technologist paradigm focuses on the creation of technology and the technology itself to affect individual and organizational experience in a positive manner. Information systems environment can be seen as a social implemented system (Gregg, Kulkarni, & Vinze, 2001).

Model Development:

Classical detection systems whether network based or host based consist of network traffic sensors that monitor network activity and possibly an event logger with a set of signature databases. At the core of threat detection system, is the logic that drives threat detection. This logic allows us to distinguish between malicious and non-malicious activity. The primary classes of detection methodologies are signature-based detection, anomaly-based detection and stateful protocol or packet inspection (Scarfone & Mell, 2007).

Signature based detection compares known threat signature to observed logged events to identify incident. This approach is limited to a set of known attacks. In addition, it is unable to detect attacks that comprise of multiple events. Anomaly based detection compares definitions of what activity is considered normal against logged events to identify significant deviation. This method may fall victim for false positive, malicious activities may be inadvertently profiled as non-malicious activity. In addition, profiling does not necessarily reflect real-world network activities. Lastly, stateful packet analysis compares predetermined profiles of generally accepted network protocol activity for each protocol state against logged events to identify deviation. This approach is difficult and almost impossible because of the need to model network protocols sate plus, an addition to being quite resource intensive. In this paper, we are proposing the logic that drives the threat detection system to be context based. We believe the use of context of activities will allow us to overcome the limitations discussed in current approaches.

Existing research views on security context and context awareness focuses on security problems in ubiquitous systems that embrace enterprise cloud and mobility (Jovanovikj, Gabrijelčič, & Klobučar, 2014) but was not applied in threat detection systems. Focusing on mobility, researchers introduced ConXsene (Miettinen, Heuser, & Sadeghi, 2014) a context-aware access control framework for mobile devices utilizing automated classification of contexts based on sensed context data. Security context is defined as a "set of contextual information considered relevant for the process of security, regarding a particular task or activity" (Jovanovikj et al., 2014). We believe that security context and contextual information flow is crucial for the design of a threat

detection system. Contextual information is key to aligning the detection system with ISPs.

We followed Organization-based access control (OrBAC) (Kalam, El Baida, & Balbiani, 2003)(Cuppens & Miege, 2003) when designing our detection system. Unlike other access control models, OrBAC can apply rules that specify contextual permissions for specific circumstances. Additionally, from a control perspective, the OrBAC model can specify granular authorization including prohibitions, obligations and recommendations; unlike classical access control models which are only restricted to permissions. Conceptualizing control in processes using constructs in OrBAC will provide the comprehensiveness required and adaptation to organizational security policy. Our adoption of context from the OrBAC model allows us to inherently model the complexity of socio-technical systems or the human activity system.

We take OrBAC modelling concepts in consideration when defining our design. We abstract ISPs at the organizational level from the implementation of the policy. The abstract level defines the concepts of organization, role, activity, view, context and security rules to express the abstract policy. The abstract policy, specified at the organizational level, is specified using roles, activities and views which respectively abstract the concrete subject, actions and objects. The role of a subject is simply called a role as in the RBAC model, the organization employs a subject so it defines that role. On the other hand, an action is an abstraction of activity. Different organizations may consider activities to belong to different actions. The abstraction of an object is called a view. A view is an organizational concept used to structure the policy specification for using objects, i.e. a view groups objects on which the same security rules apply. In OrBAC, one can define that a subject may have the permission, prohibition or obligation to do an activity on some object given an associated context is true.

The formalism of the OrBAC model uses first-order logic notations, which allows each organization to specify its own security policies. These security policies are represented using an array of first order predicates. We adopt notations and constructs from the OrBAC model in our design method. Even though we are adopting OrBAC constructs, the unique contribution in this work is the use of OrBAC constructs in the design of a threat detection system (see Table 1). The context concept has been introduced in the OrBAC model in order to express dynamic rules (Cuppens & Miege, 2003). Contexts correspond to any constraint that joins a subject, an action and an object. Contexts maybe temporal, spatial, user-declared, prerequisite or provisional. We use the contexts suggested in (Cuppens & Miege, 2003) (Cuppens-boulahia, 2008) (see Table 2).

Table 1 OrBAC constructs

Construct	Definition

Organizations	central entity may represent multiple organizations, or an organized group of subjects.
Subjects	person, actor, entity or an automated agent
Actions	means for subjects to access objects
Objects	static entities e.g. files, records.
Roles	a set of subjects to which the same security rule applies.
Activities	a set of actions to which the same security rule applies.
Views	a set of objects to which the same security rule applies
Contexts	a condition on which rules only apply when the condition is true

Table 2 Contexts defined in OrBAC

Context	Definition
Temporal	depends on the time at which the subject is requesting for an access to the system
Spatial	depends on the subject location
User-declared	depends on the subject objective
Prerequisite	depends on characteristics that join the subject, the action and the object
Provisional	depends on previous actions the subject has performed in the system

The conceptualization used in our design is consistent with OrBAC access control model from an information system point of view. Our nascent design theory (Gregor & Hevner, 2013) in this conceptualization is that, the underlying process activity

implementation i.e. interaction between subjects, objects and actions is completely abstracted, thus allowing us to draw our method schematic in an abstract, holistic and systematic manner. The following rules represent the modeling concepts for a threat detection system (see Table 3).

Table 3 Context Based Threat Detection Modelling Concepts

Modelling concept	**Definition**
Abstract ISP definition (Organizations define the abstract Roles, Activities and Views)	A subject fulfills an organizational role. Organizational roles are fulfilled by subjects
	an activity is considered a set of actions; actions are simple operation that collectively represent an activity
	A view uses a set of objects. Objects are used by a view.
Context Based Detection	A role may have the permission, prohibition, recommendation or obligation to do an activity coordinated on some view if and only if the given context is true

Using these rules, we can deduce design for a threat detection system with security policy in mind. (See Figure. 1).

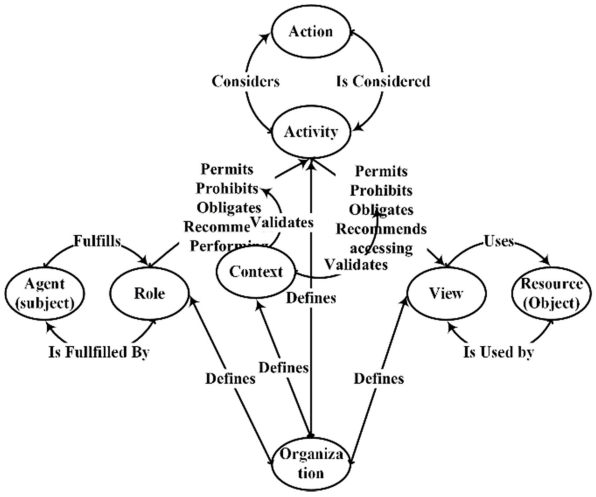

Figure 1 Real-time Context Based Intrusion Detection

Discussion:

The threat of insiders compromising organizations critical information assets has led to the implementation of different technical and managerial controls. Technical controls include the use of IDS to detect malicious activities based on well-known attacks, or attack signature steps (Mohan et al., 2015)(Fayyad & Meinel, 2013), while ISPs are managerial solutions used to control employees' behavior. However, these approaches are limited, since IDS are prone to many false positives, while employees may violate rules mandated by ISPs. To address these limitations, we proposed a context-based threat detection model, whereby employees can only gain access to specific information, and use such information based on specific contexts.

Our threat detection model adopts the constructs of OrBAC, whereby the activity, role, view and context are defined by the organization. The activity consists of actions, role consists of subjects (such as an employee), and views consist of objects (i.e. information, files). The context is a condition whereby rules are only applied if the condition is true (i.e. an employee can only access information if a specific condition is present). Essentially, by introducing a context-based threat detection model, an employee's actions on a particular information asset could be traced back to malicious or non-malicious activity. Our threat detection model therefore increases the accuracy of detecting malicious or non-malicious activity, while reducing false positives.

Our threat detection model proposed in this study provides alignment of detection system with that of ISPs. Specifically, ISPs define the roles and responsibilities for employees, which are aligned with organizational objectives. The context under which employees use information would correspond with ISPs by capturing the constraints articulated in the ISPs. In essence, the implementation of our threat detection model would enforce the proper implementation of ISPs within an organization.

Our context-based threat detection model also addresses a major limitation of current IDS, which is the issue of complexity (Devaraju & Ramakrishnan, 2011). Complex threat detection systems can introduce multiple problems such as delayed detection time, and slow learning, as in the case of anomaly-based IDS (Devaraju & Ramakrishnan, 2011). We also see great complexity in resource intensiveness in statefull packet inspection detection methods. However, our threat detection model provides a more logical and consistent approach to detecting malicious activity, by specifying the context under which information can be accessed and by whom. Any action done on information can be traced back to the employee that had access to it, as well as the context under which he/she had access to such information. This removes the complexity of matching activities to already established malicious activities, or learning behavior patterns to detect malicious versus legitimate activity. Essentially, the insider threat problem could be reinterpreted simply in terms of context, which may be temporal, spatial, user-declared, prerequisite, or provisional.

Conclusion:

In this paper, using design science paradigm, we introduce a threat detection model overcoming existing models limitations. Our proposed detection model offers reduced false positives with greater detection of malicious activities. The proposed detection system aligns with organizational security policies ensuring the detection of insider threats. Our proposed model overcomes the problems of current approaches, which consists of many false positive. Specifically, since this approach is centered on context, which is defined based on ISPs, detection of malicious activity should be more accurate.

REFERENCES:

Ahn, W., Chung, M., Min, B. G., & Seo, J. (2015). Development of cyber-attack scenarios for nuclear power plants using scenario graphs. International Journal of Distributed Sensor Networks, 11(9), 836258.

Bishop, M., Coles-Kemp, L., Gollmann, D., Hunker, J., & Probst, C. W. (2010). 10341 Report--Insider Threats: Strategies for Prevention, Mitigation, and Response. In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Candell, R., Stouffer, K., & Anand, D. (2014, October). A cybersecurity testbed for industrial control systems. In Process Control and Safety Symposium, International Society of Automation, Houston, TX.

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. Computing & Information Systems, 21(2), 10-18.

Midia, P. (2002). Perspectives on Penetration Testing—Black Box vs. White Box. Network Security, 2002(11), 10-12.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.

Mitnick, K. (2011). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Hachette UK.

Pieters, W. (2011). Representing humans in system security models: An actor-network approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1), 75-92.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication, 800(115), 2-25.

Tang, A. (2014). A guide to penetration testing. Network Security, 2014(8), 8-11.

Tischer, M et al., "Users Really Do Plug in USB Drives They Find," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 306-319.

Tomanek, M., & Klima, T. (2015). Penetration Testing in Agile Software Development Projects. arXiv preprint arXiv:1504.00942.

Watson, G., Mason, A., & Ackroyd, R. (2014). Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Syngress.

Whitman, M. E. (2003). ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY. Communications Of The ACM, 46(8), 91-95. doi:10.1145/859670.859675

Whitman, M. E., & Mattord, H. J. (2010, October). The enemy is still at the gates: Threats to information security revisited. In 2010 Information Security Curriculum Development Conference (pp. 95-96). ACM.

Wood, P. (2006). The hacker's top five routes into the network (and how to block them). Network security, 2006(2), 5-9.