8-7-2011

Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise – an overview of considerations

Jeffrey A. Ingalsbe
University of Detroit Mercy, ingalsja@udmercy.edu

Dan Shoemaker
University of Detroit Mercy, dan.shoemaker@att.net

Nancy R. Mead
Software Engineering Institute, nrm@sei.cmu.edu

Recommended Citation

Ingalsbe, Jeffrey A.; Shoemaker, Dan; and Mead, Nancy R., "Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise – an overview of considerations" (2011). *AMCIS 2011 Proceedings - All Submissions*. 359.
http://aisel.aisnet.org/amcis2011_submissions/359

Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise – an overview of considerations

Jeffrey A. Ingalsbe
University of Detroit Mercy
ingalsja@udmercy.edu

Dan Shoemaker
University of Detroit Mercy
Dan.shoemaker@att.net

Nancy R. Mead
Software Engineering Institute
nrm@sei.cmu.edu

ABSTRACT

A megatrend triad comprised of cloud computing, converged mobile devices, and consumerization presents complex challenges to organizations trying to identify, assess, and mitigate risk. Cloud computing offers elastic just-in-time services without infrastructure overhead. However, visibility and control are compromised. Converged mobile devices offer integrated computing power and connectivity. However, end point control and security are compromised. Consumerization offers productivity gains and reduction in support costs. However, end point control and the organization's perimeter are compromised. This paper presents an overview of considerations for organizations impacted by the megatrend triad and, subsequently, shows how threat modeling techniques can be used to identify, assess, and mitigate the attendant risks.

Keywords

Threat modeling, cloud computing, mobile device security, consumerization

INTRODUCTION

A megatrend triad comprised of cloud computing, converged mobile devices, and consumerization presents complex challenges to organizations trying to identify, assess, and mitigate risk. Cloud computing offers elastic just-in-time services without infrastructure overhead. This is very attractive because hiring (or keeping) staff to perform things like payroll on one end of the spectrum and sever maintenance can be a burden on the bottom line. However, visibility and control are compromised. That is, organizations have a more difficult time answering questions like "where, exactly, is my data?" and "is this forensic copy of my data reliable?" Converged mobile devices offer integrated computing power and connectivity. This is very attractive because personnel can perform complex tasks while not physically at work and without WiFi connectivity. However, end point control and security are compromised. CMDs are more easily lost or stolen and the ways that security threats are handled on corporate laptops and desktops is not easily transferrable to CMDs because they don't have enough computational or battery power yet. Consumerization offers productivity gains and reduction in support costs. This is attractive because it allows a company to transfer a portion of the cost of ownership of endpoints to employees. However, end point control and the organization's perimeter are compromised. That is, standard loads that corporations have traditionally enforced with their endpoints are not possible with employee owned endpoints. In fact, there may be more push back because employees feel as if they are justified in using the endpoints for both personal and corporate use. This paper presents an overview of considerations for organizations impacted by the megatrend triad and, subsequently, shows how threat modeling techniques can be used to identify, assess, and mitigate the attendant risks. First, cloud computing is discussed. Definitions are given and considerations are discussed. Then, mobile devices and consumerization are discussed. Definitions are given and considerations are discussed. Then, threat modeling is presented as a way of identifying, assessing, and mitigating risk. Finally, recommendations for future work are made.

PREVIOUS AND RELATED WORK

The The oldest ancestor of this work was conducted and published at Ford Motor Company (Ingalsbe 2004), which represented Ford's IT portfolio from an **infrastructure** perspective using UML deployment diagrams. Subsequently, work on threat modeling work was conducted at Ford Motor Company (Ingalsbe, Kunimatsu, Baeten, Mead, 2008) which utilized Microsoft's Threat Analysis and Modeling process and tool to analyze (primarily) systems under development. Finally, the two efforts were married when a new threat modeling methodology using UML deployment diagrams was conducted at the University of Detroit Mercy (Ingalsbe, Shoemaker, Mead, Drommi, 2010). This paper extends the threat modeling methodology to include considerations for the megatrend triad.

CLOUD COMPUTING

In one sense, cloud computing is only the latest in a long line of technologies that seeks to streamline the operation of the enterprise. Some might argue that it is not a single technology but a set of technologies. Some might argue that it is not a set of technologies but, rather, a set of services offered using a particular business model and existing technologies. There is some truth in both arguments. So, it is important to agree on a definition of cloud computing for the context of this paper. Rather than dogmatically giving our definition, we would prefer to offer it as the logical alternative to several deficient definitions.

Cloud Computing is Not

Cloud computing is not another flavor of traditional IT outsourcing. There are several reasons why we believe this to be true. First, traditional IT outsourcing involves engaging an external entity to deliver services for an organization per specific contract provisions. The organization, which may be subject to specific regulations, can visit the external entity to inspect, audit, and prove that their data is being handled in a way that is acceptable. The cloud computing business model works only if servers and data can be provisioned dynamically in a scalable, elastic manner and that allows the organization to "dial-up" and "dial-down" their usage. Allowing organizations to visit sites, audit, and prove proper data management would require that the cloud computing business model change. Second, for the external entity, economies of scale preclude drawing up specialized contracts for each organization that engages them. That is not to say that there are not organizations that will provide specialized cloud services on a one-off basis. It is simply not the norm.

Kinds of Cloud Computing

There are two different (but similar) ways to classify clouds. The first is public versus private clouds. The second is internal versus external clouds. When discussing public and private clouds the conversation is typically about control. When discussing public versus private clouds the conversation is typically about ownership. Public (and external) clouds are built to provide multi-tenant environments while private (internal) clouds are grown to provide cloud-like services inside the enterprise or across a small number of enterprises.

Things Clouds Deliver

Cloud computing environments can be thought of as delivering the following things as a service: application, process, storage, infrastructure, platform, and security. This is not a complete list by any means but it is meant to show the diversity of the offerings of cloud providers. "Platform as a service" providers allow their customers to build a platform on which their customers can develop applications (e.g. force.com).

Things to Consider

From a cyber security perspective, there are several important things to consider. They fall into four broad categories: compliance, data, forensic, and exposure.

Compliance considerations include being able to prove that you are compliant with laws, regulations, standards, contracts, or policies. As was pointed out previously, the cloud computing business model is based on hiding (not in a nefarious sense) implementation details from the organization so that the external entity can achieve economies of scale. That is, the external entity must be able to move servers, data, and processes from one virtual location to another based on what is happening with their entire customer base (not just one customer). Additionally, compliance considerations include being able to understand whether you are compliant in every jurisdiction in which your servers, data, and processes operate. That is, the external entity may store your personnel data in a location where there are restrictions on how you can handle that data.

Data considerations include being able to understand who has access to your data. Remember that access to the physical box means access to the data. Some multi-tenant environments have provided opportunities for data leakage between virtual machines. Additionally, data considerations include being able to understand how long your data sticks around, how it is backed up and how it is recovered. Legal considerations are even more concerning. The implications of using cloud services for attorney-client communications or storing attorney-client information in the cloud is not clear. Additionally, it is not clear whether using things like gmail constitutes a violation of an attorney's code of ethics or an attorney's code of professional responsibility. The UK Information Commissioner's Office recommends that all data be encrypted prior to being sent to the cloud. While this may increase an organization's ability to ensure that their data is kept confidential, it decreases the utility of the cloud environment.

Forensic considerations are compounded by the fact that there are currently no established digital forensic guidelines that specifically address the investigation of cloud computing systems (Svantesson and Clarke, 2010). Electronic discovery in the cloud is not a simple matter. In fact, the acquisition and analysis of evidence from cloud computing systems may be impossible. Additionally, organizations must be able to prove that the forensic evidence that they obtain has not been altered. Organizations own their data and are responsible for reasonably safeguarding that data. That responsibility does not get transferred to the external entity providing cloud services.

MOBILE DEVICE TOTING

In this context, we define mobile devices as hand-held computing devices with integrated cell phone technology. They are becoming increasingly powerful and capable of connecting to the internet at speeds that compare to broad band connections in the home (i.e. 3 Megabits per second). Additionally, apps are being written that do everything from Bluetooth networking to online banking to automatic sensing. These devices can be as powerful as laptops that are only a few years old.

Things to Consider

From a cyber security perspective, there are several important things to consider. First, endpoint protection for mobile devices cannot be done in the same way that it has been done for desktops and laptops. Because of battery life issues and computing power issues, the mobile devices must make compromises when it comes to endpoint protection. Second, we are very close to having mobile devices (our definition) shipments exceed those of traditional computers. This makes them more attractive as a target for malware writers. Additionally, users are responsible for the propagation of the majority of the mobile malware by simply clicking through warnings or confirmations. Third, it cannot be assumed that applications written for the mobile devices are vetted based on how they handle user data. A well written app that passes the online store vetting process may still be irresponsibly handling customer data.

CONSUMERIZED

Consumerization involves personal consumer products being brought into the enterprise. The motivation can be that the products are more powerful in some way than the products being used by the enterprise. Consumerization initiatives involve allowing employee owned mobile devices or laptops to connect to the corporate network. We distinguish between corporate owned devices and employee owned devices by following the money. If the money for the device comes for the company (even if it is a stipend or a reimbursement) then we consider the device "corporate owned".

Things to consider

The implication of consumerization is that new uncontrolled endpoints will be attached to the corporate network with different operating systems than the organization is used to supporting. Corporate systems and filestores will be accessed with the uncontrolled endpoints. Corporate data will leak (or migrate) to the uncontrolled endpoints and become comingled with personal data. This is a problem for several reasons. First, if the organization does not own the device, they don't have a legal right to demand its surrender when there is an issue. Recovery of corporate data may accidentally involve viewing personal data which the organization has no right to see. Second, products that support mobile device usage in the enterprise (e.g. The Blackberry Enterprise Server or BES) are not all created equal. In fact, feature sets and product maturity vary widely. The perception is likely to be that one mobile device is the same as any other mobile device and since Blackberrys have been in the enterprise for a long time there should be no issue with allowing any other mobile device. Third, if the mobile device is requested by a court handling the employee's divorce and the same mobile device is requested by a court handling the organization's class-action lawsuit who wins?

THREAT MODELING

The considerations outlined above for the cloud computing, mobile device toting, consumerized enterprise show that the megatrend triad will make the identification, assessment, and mitigation of risk more difficult and complex. Enter threat modeling, a process in which an organization (as a whole) participates in order to understand threats to assets and the vulnerabilities that would allow them to be realized and to agree on mitigations that would lessen or eliminate harm to those assets. The ancestry of this work includes the definition of a threat modeling methodology. A high level definition of that methodology follows intermingled with an explanation of the way in which the methodology addresses the considerations for cloud computing, mobile devices, and consumerization outlined above.

Prerequisites for Threat Modeling

Effective threat modeling requires the participation and buy-in of executive management, subject matter experts, business representatives, and security personnel. Before endeavoring to threat model the cloud computing, mobile device toting, consumerized enterprise the personnel handling each of those corporate initiatives must be engaged. Additionally, an agreement on the definition and calculation of risk will be needed. This can be accomplished by engaging finance, purchasing, OGC, and program management groups.

When to Threat Model

Threat modeling purists recommend that it be performed during the design phase but organizations dealing with the megatrend triad will are likely to have existing systems in place which will be modified for the cloud and mobile devices. Therefore, in this case, threat modeling will likely be performed on interconnected, legacy systems.

Kinds of Threat Modeling

There are (at least) a handful of threat modeling methodologies in existence. Two of the most prominent come from Microsoft. They are Microsoft TAM (Threat Analysis and Modeling), and Microsoft SDL-TM. Another was developed by Frank Swiderski and Window Snyder (Swiderski and Snyder, 2004). They are reasonable methodologies and are accompanied by free tools. However, they are deficient for handling interconnected, deployed systems (see our previous work) so we will be using the Enterprise Threat Modeling methodology.

How to Threat Model

Enterprise threat modeling involves building a customized deployment diagram that restricts the real estate of the diagram as in Figure 1. A critical part of the threat modeling process involves understanding the pieces of the system and how they fit together. Only then can the discussion about assets and their value begin. Enforced consistency in the presentation of the system facilitates the analysis of the system. Each folder is populated with stereotypical nodes (like servers, endpoints, routers, databases, and etcetera). The nodes are interconnected (associated) with each other. For every stereotypical node, attributes are identified (like the component or software stack on the node, the policy stack that applies to the node, the security stack that protects the node, and the information stack that resides on the node). After identifying all of the nodes and their interconnections, there are a handful of starter questions for each node that will prompt conversation about threats to the node. Threats are classified using STRIDE (Howard and LeBlanc, 2001). It stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. Threats are analyzed using DREAD (Howard and LeBlanc, 2001). It stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. By assigning a 0-5 value for each DREAD letter a final risk value is obtained that allows threats to be compared. Responses to each threat are negotiated with the entire team and include: avoid (get out of that activity altogether), transfer (let someone else assume the risk, e.g. insurance), and mitigate (reduce the risk by putting controls in place). Each of the subsections below explains how the considerations above are addressed.

Actors

Actors are people (or systems) that interact with your system to achieve something of value. In the context of this paper, actors will be users of cloud computing services (e.g. someone initiating a paycheck run) or mobile device users. Additional questions to be asked for these actors would be

- What does the employee's job function require them to have access to?
- Has the employee had any additional training that would mitigate their risk of using either cloud services or a mobile device?

End points

End points are nodes that allow actors to interact with the system being modeled. End points are "how" actors connect to the system. In the context of this paper, end points will be things like employee owned mobile devices, corporate owned mobile devices, and cloud application endpoints. Additional questions to be asked for these endpoints would be

- How is the cloud application vetted? E.g. is it an app that has been downloaded by the employee?
- What end point protection is in place on the device?
- Has the employee received training on the end point?
- What corporate data will be stored or transmitted by the device?
- Is there remote wipe capability?
- Is there corporate support for the device?

Infrastructure

Infrastructure nodes allow the representation of things like routers, gateways, firewalls, load balancers, and etcetera. They are often handled by networking groups or vendors. So, discussions can be deferred to those personnel.

Upstream and Downstream Systems

In the strictest sense, an upstream system is one that is a source of data for the system being modeled and a downstream system is one that is the destination for data mastered by the system being modeled. In the context of this paper, the upstream and downstream systems will be cloud systems. They may interconnect with client nodes, presentation nodes, application nodes, database nodes, and storage nodes. This is where the nebulous of the cloud environment will become very apparent. Additional questions to be asked for upstream and downstream systems would be

- What laws, regulations, standards or policies cover the nodes?
- What is the information stack on the nodes?
- What audit, backup, and recovery options are available?
- Is eDiscovery supported?
- What are the characteristics of the vendor?
- Do you have preferred status with the vendor or are you one of the crowd?
- Has the vendor had security issues in the last 3 years?

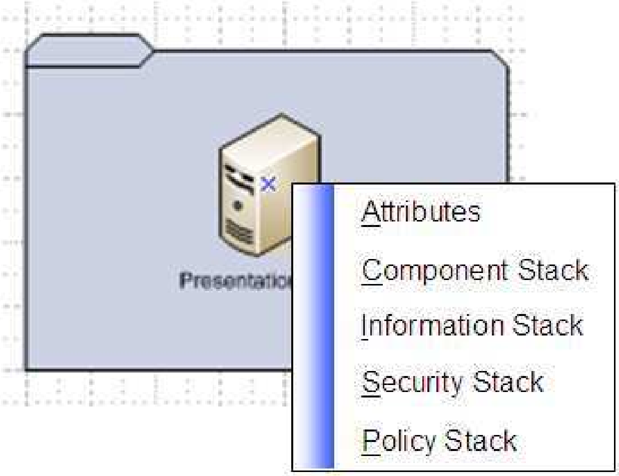

Figure 2. Example of a node

Application, Database, Storage Nodes

Application, database, and storage nodes may reside in the cloud depending on your organization. You may choose to put those nodes in the upstream or downstream systems folder or you may simply change the color of the font on the icons in order to designate them as cloud nodes. The same questions as were asked for upstream and downstream systems in the cloud should be asked here.

Advantages of this approach

Graphically seeing the representation of mobile devices, cloud computing services, and consumerized devices as they interconnect with corporate systems is invaluable in terms of analyzing risk. Threat modeling the systems using ETM promotes an open dialog with all stakeholders for each threat identified. Expensive tools do not need to be purchased, Microsoft Visio is used to populate the template.

FURTHER WORK

Further work needs to be done on how to graphically represent the risk identified in the threat model and the severity of the ratings that were given. Additionally, as the legal realm more fully develops responses to cloud computing issues, they need to be incorporated.

CONCLUSION

A megatrend triad comprised of cloud computing, converged mobile devices, and consumerization presents complex challenges to organizations trying to identify, assess, and mitigate risk. Threat modeling helps. A graphical representation the system will help organizations see their interconnected systems and subsequently make decisions about whether to engage in corporate initiatives that would move services to the cloud, or allow employee owned mobile devices.

REFERENCES

1. Swiderski, F. and Snyder, W. (2004), "Threat Modeling," Microsoft Press
2. NIST Special Publication 800-53 (2007), "Recommended Security Controls for Federal Information Systems", National
1. Institute of Standards and Technology U.S. Department of Commerce
2. Svantesson, D. and Clarke, R. (2010) "Privacy and consumer risks in cloud computing", Computer Law & Security
3. Review, Elsevier Ltd.
4. Howard, M., and LeBlanc, D., (2001) *"Writing Secure Code (With CD-ROM)",* Microsoft Press
5. Ingalsbe, J. Kunimatsu, L. Baeten, T. Mead, N (2008) "Threat Modeling – Diving into the Deep End", IEEE Software
6. Magazine