Intl. Conf. Security and Privacy (ISP'09), Orlando, FL, July 13-16, 2009.

Stopping the Insider Threat: the case for implementing integrated autonomic defense mechanisms in computing systems

Ghassan 'Gus' Jabbour[1] and Daniel A. Menasce[2]
[1]*The Volgenau School of Information Technology & Engineering*
George Mason University
Fairfax, VA 22030, USA
gjabbour@gmu.edu

[2]*Department of Computer Science*
George Mason University
Fairfax, VA 22030, USA
menasce@gmu.edu

Abstract

The increasing dependency on complex information systems that are, in many cases, interconnected on a global level has resulted in the rise of security attacks and computer crimes to levels that are alarming to any business entity that relies on such systems. In this paper we show the seriousness, risk, and malice of security attacks by insiders. We argue that organizations must exert serious efforts to prepare their computing systems to defend against it. We propose the use of integrated autonomic defense mechanisms that are inseparable from the systems that are being defended.

1. Introduction

Threats to the security of an information system may be initiated from either outside or from within an organization. Detecting such threats is critical to the security of any information management system or the overall health of any organization. But detecting a threat or an attack from within an organization, also referred to as the "insider threat", is the hardest to tackle and to mitigate. It has been a common practice to detect external threats through the use of software tools and technologies such as password enforcement, firewalls, encryption, two-factor authentication, access-control system audits, patch management, network traffic monitoring, and penetration testing. However, internal threats are much harder to address since there is no way to monitor the insider's intent, that is, it is difficult to foresee or forecast an employee's actions. This difficulty gets complicated by the fact that the definition of the term "insider" is not always clear or obvious. Many researchers agree that to this day, there is no one clear definition for that term.

Some of the available definitions of the term "insider" denote it as any person or system that has a privileged access to the domain or system that is being protected [1]. That person or system should be considered a potential threat since they can either use their privileged access or delegate that privilege to someone or some system that may compromise or adversely affect the behavior or availability of the system being protected. Therefore, whether an attacker uses a legitimate access to modify the behavior of a system or obtain an unauthorized access to it, the outcome could be disastrous. The degree of damage that an insider can inflict on a system may vary based on the level of the privilege that the insider has; however, we believe that any privileged access to a critical system should be considered a potential threat.

In the scope of our work, we focus our discussion on cyber security within the technology borders of the computing world. While physical security is also important and should be considered as part of a holistic organizational security policy, the objective of our research focuses specifically on protecting computing and information-based systems against the insider threat. We argue that while many methods (such as whistle blower policies, embedded or hidden cameras, clean desk policies, software tools) have been used to detect insider threat, this problem remains a main concern, and addressing it is essential to the survivability of any

organization or system that deals with sensitive, critical, and/or private information.

The rest of the paper is organized as follows: Section 2 reveals the magnitude of the threat and enumerates a list of security breaches that are damaging in one way or another. Section 3 makes the case for an autonomic defense mechanism that is totally integrated into the target system. Section 4 briefly describes the research that is being currently conducted by the authors regarding this research problem. Finally, section 5 sums up the paper with concluding remarks.

2. The Magnitude of the Threat

Research in the area of information security has shown that the employees of an organization are considered among the biggest threat to the information security of any organization [2], [3], [4], [5], [6]. Numerous studies continue to reveal the fundamental truth about the paradigm shift in today's approach to information security. Today, there is an evolving consensus regarding the biggest threat to the security of computing systems. It is believed that the biggest threat to such systems is not the traditional cyber-criminal attack inflicted by malicious hackers who reside in virtual locations, but rather the trusted employees. According to [7], protecting an organization against insiders who have malicious intent "requires effectively enforcing data access policies and auditing user activity with sensitive and confidential data and systems." The security breach incidents that took place over just the past few years have been damaging and almost non-stoppable.

In general, the insider threat is usually attributed to one of the following conditions: lack of policies, failure to adhere to policies, or the temptation by competition or malice for any given reason [8]. Also, the insider threat can be either intentional or unintentional. Unintentional compromise by an insider could be simply the result of a lack of understanding of or failure to adhere to the policy. Intentional compromise, on the other hand, is a malice action by a user who knows exactly what the objective is and how to reach it. But regardless of its type, the insider threat may be detrimental to any organization or a system. We enumerate in what follows some of the recent security incidents and breaches that were caused by insiders and that either inflicted or could have potentially inflicted major losses to organizations and government agencies.

In 1997, a United States Department of Defense (DoD) Inspector General report found that 87% of identified intruders into the department's information systems were either employees or others internal to the organization [3].

An E-Crime Watch Survey [9] that was conducted in 2004 revealed that current or former employees and contractors are the second greatest cyber security threat, exceeded only by hackers, and that the number of security incidents has increased geometrically in recent years.

According to a US-CERT (Computer Emergency Response Team) and US Secret Service survey published in 2006 the insider and outsider attacks measured as follows: outside attacks during the years 2004, 2005, and 2006 were 71, 80, and 68 percent, respectively, while insider attacks during the same years were 29, 20, and 32 percent, respectively [10]. The survey also found that the financial losses due to the insider attacks were much higher than those caused by outside attacks. In addition, the same study, on the problem of insider threat, found that "the majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable", that is, they were detected after the onset.

In 2006, the Department of Veterans Affairs experienced an unintentional compromise in their information security performed by an insider [11]. An employee of the department downloaded 25.6 million veterans', and some of their spouses', names, social security numbers, and dates of birth and disability ratings on a laptop which was later stolen from the employee's residence. The laptop was later recovered by the FBI who determined that the data was not accessed and was intact. However, it was suggested, as a result of the incident, that the government paid for credit monitoring for a whole year for all those who were affected by the incident ($25.6 million). While this unintentional attack did not compromise sensitive data, it certainly put a financial burden on the department.

Also in 2006, Coca Cola Co. experienced an intentional attack by an insider according to the Associated Press [12]. An administrative assistant at the company and two colleagues were accused of stealing samples of a new Coca Cola product and some company documents for the intent of selling it to its competitor Pepsi Co for $1.5 million.

A 2007 E-Crime Watch survey [13] indicated that 49% of the participants reported experiencing an e-crime in 2006 versus 38% the prior year. In addition 69% of participating organizations said that they have trimmed spending on IT security by 5% and corporate security by 15%. But when those same participants were asked whether insider or outside attackers caused the most

damage, the answers were as follows: insiders 34%, outsiders 37%, and unknown 29%. In addition, those participants indicated they may not be giving as much attention to insider threats as would seem justified. The survey revealed that background checks dropped from use in 73% of the organizations last year to only 57% this year, account and password management policies dropped from 91% of the organizations last year to 84% this year, employee monitoring from 59% to 42%, and employee security awareness training from 68% last year to 38% this year.

While many companies are usually complacent when it comes to guarding against potential threats from the inside, a 2005 CSI/FBI Computer Crime and Security Survey concluded that insider jobs occur as often as external attacks thus encouraging companies to "anticipate attacks from all quarters" [14].

In most cases, organizations focus their security efforts on external threats to their computing infrastructure relying on an individual's morals or ethics to govern the issues involved with the insider threat spectrum. They rely on their employees to adhere to policies and never do wrong. However, this can prove to be a fatal mistake. In many cases, internal security policies are considered the base for regulatory compliance, best practices, and insider incident prevention. However, it is believed that a policy by itself is not very useful if it is not backed by consequences [8]. It is argued that if an insider believes that he or she will be prosecuted if they cause a security breach, whether intentionally or unintentionally, then they are less likely to break the policy and breach the security. But in the scope of this research we take this argument one step further by arguing that, in some cases, even the knowledge of a possible prosecution may not deter an insider from performing a malicious attack. The incident at Coca Cola Co. in 2006, for example, illustrates how a group of people collectively stole a sample of a new Coca Cola product in addition to some corporate documents with the intention of selling it to Pepsi Co. for $1.5 million. In this specific case, one has to assume that at least one, if not all, of the group of three must have thought about the magnitude and illegality of their action. It is rather obvious that such actions would most certainly lead to prosecution. However, the knowledge of the consequences did not deter them from pursuing their objective.

Therefore, relying on the employee to do what is right or ethical is never a guarantee of security. People's morals and ethics vary from person to person and so it is a naive proposition to think that members of an organization will always do what is in the best interest of that organization or its clients. Regardless of the scope and enforcement of written policies, and the training and education of the personnel on organizational policies and security, someone is bound to break the rules and organizations must be prepared for such situations.

In November of 2008, records from a cellular phone used by then President-elect Obama were improperly breached, apparently by employees of the cell phone company Verizon Wireless. In a statement released by the company's president and CEO, Lowell McAdams, Verizon Wireless revealed that "a number of Verizon Wireless employees have, without authorization, accessed and viewed President-Elect Barack Obama's personal cell phone account" [15].

Finally, the results of a survey conducted by RSA, the Security Division of EMC, revealed that while 94% of the surveyed employees were aware of their organization's IT security policies, 53% have felt the need to work around the security policies in order to get their work done [4].

Below is a listing of the headlines of some of the cases that involved or surrounded the problem of insider threat attacks, and the financial damage these attacks have or could have inflicted on businesses:

- Banks to blacklist rogue workers in fraud fight (2005): Major U.S. financial institutions are working to set up a new defense against insider fraud: a database of employees who are known to be scam risks [16].

- Massive bank security breach uncovered in N.J.: Bank employees implicated in the conspiracy; 500,000 victims alleged [17].

- In 2005, Apple Computer filed two lawsuits accusing insiders and partners of leaking proprietary information. In one case, Apple is suing two men it says distributed prerelease versions of Tiger, the next iteration of Mac OS X. In a separate action, it is suing unnamed individuals who leaked details about a forthcoming music device code-named Asteroid [16].

- A United Healthcare Insider Charged in Cal Data Theft (2008): A former United Healthcare employee has been charged in connection with 163 identity theft cases at the University of California, Irvine. The company has notified the 1,100 students who had their data accessed and is offering them identity theft protection services, the spokeswoman said [18].

- IT Wary of Insider Attacks as Economy Slows Down (2008) [18]:

- A disgruntled administrator working for the city of San Francisco has locked access to a critical network by resetting administrative passwords to its switches and routers.

- A UNIX systems administrator at Medco Health Solutions Inc. in Franklin Lakes, N.J., planted a logic bomb on an internal system that would have deleted data on 70 servers if it had gone off. The attacker had feared he was going to be laid off from the health care provider.

- Wells Fargo Code Used to Illegally Access Consumer Data (2008): Wells Fargo Bank N.A is in the process of notifying some 7,000 individuals that a thief may have accessed their Social Security numbers and other personal information by illegally using the financial services firm's access codes. These codes are usually used by Wells Fargo employees to gain access to consumer credit data. Wells Fargo's senior company counsel said that the investigation has confirmed that "a significant number of unauthorized transactions had been made using Wells Fargo's codes." He said that Social Security numbers, birth dates, addresses, driver's license numbers and in some cases, credit account information, were illegally accessed [18].

- Facebook Bug Leaks Members' Birthday Data: Facebook accidentally exposed the birth dates of its 80 million members over the weekend in July 2008. A glitch in a test version of Facebook's Web site inadvertently exposed the birthdays of Facebook's 80 million members [18].

- Stealing PINs lands a former Verizon Wireless employee in prison: The employee admitted to stealing the PINs and selling them to retailers across the country while he worked as a customer service representative in 2002 and 2003. Authorities working on the case revealed that the subject continued his crimes for four months after he left Verizon [19].

- State Breach Disclosure Laws - Update: In 2008 five U.S. states (and D.C.) have adopted new data breach disclosure laws. The five states are Alaska, Iowa, South Carolina, Virginia, West Virginia, and the District of Columbia [20].

- Tough economic climate can heighten insider threat (2008): As companies downsize, they need to keep an eye out for disgruntled employees [21].

- Feds allege plot to destroy Fannie Mae data (2009): The attack by a fired Fannie Mae worker was thwarted, but according to the Justice Department, had the virus been successfully released, it could have cost millions of dollars and shut down operations for a week at the largest U.S. mortgage finance company [22].

3. The Inevitability of autonomic defense mechanisms

Autonomic computing is a sub-discipline of computer science that deals with the design of self-managing systems, i.e., with systems that are self-optimizing, self-configuring, self-healing and self-protecting [1], [23], [24], [25], [26]. In this paper we focus our attention on the self-protecting dimension of autonomic computing as it applies to computer and information systems' security, particularly databases.

We elaborate on the concept of embedded autonomic defense mechanisms, as presented in [27], and defined as those systems that implement their defense mechanism as an integral and inseparable part of the system that is being defended or protected. As argued in [27], any defense mechanism that resides outside the system that is being protected is vulnerable to compromise by insiders. Such insiders, who have the power to disconnect a monitoring tool or security software from communicating with its target system, can wreck havoc in the entire defense mechanism of an organization's computing system or network. Therefore, organizations must be proactive in protecting their data and computing infrastructure from the insider threat.

Unlike computing system security frameworks that exist today, which mostly detect imminent problems, generate an alert, and produce a report, the autonomic defense framework that we propose implements the total integration of the defense mechanism into the system that is being protected as shown in Figure 1. The defense mechanism is embedded into the core components of the computing system and is inseparable from it.

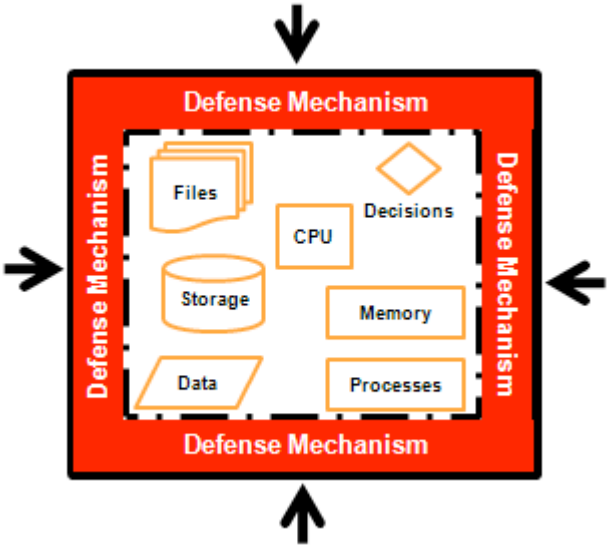

Figure 1. Autonomic Defense Mechanism of a computing system

Access to any data or system objects of the computing system is first intercepted and checked by the defense mechanism before any processing takes place. Decisions on whether to allow actions to take place is based on system owner-built policies that are accessible and modifiable only by a group of people that only collectively make up the system owner authority. Having more than one person approve all processes or requests eliminates unilateral actions when it comes to changing or modifying the policy.

The system owners build policies to support certain business objectives. These policies are stored within the system that is being protected and are used to verify requests (or attempts) to change system configurations, and to enforce the policy mandates. When a power user or a hacker initiates an attempt to change security configurations, the request goes through a process of verification before it can be acted upon. This step is carried out by system embedded processes that have built-in logic for checking the request against the security policy. If the request complies with the predefined security policy that governs its scope of applicability then the request is applied. If, on the other hand, the request does not comply with the policy, then the request is rejected and the system owner (s) is alerted of the failed attempt.

The autonomic defense approach, as we propose it, ensures two main and very important security measures that the lack of which could be detrimental to any computer or information system that stores sensitive data. The first security feature ensures that the system is being defended at all times without any possible interruption. The second security feature presumes that no entity, whether external or internal to the environment within which the system operates, is trustworthy. All actions have to be verified against the security policy at all times.

Attaining such a standard of securing computing systems can only be achieved by incorporating the defense mechanism totally and completely into the core components of those computing systems. In other words, the computing system must have self-protection characteristics that enable it to rely on its own abilities to mitigate potential risks.

The Reference Monitor concept, which is similar to our approach, was introduced in 1972 by James Anderson [28]. The concept is based on ideas that are somewhat similar to what we propose in our paper, especially with respect to the reference validation mechanism (which is an implementation of the reference monitor concept). The reference monitor model states that the validation mechanism must be tamper proof (i.e., authorization is always enforced) and must always be invoked (i.e., every access is mediated). The main difference between the reference model and our approach is the autonomic nature of our approach. The topology of the Reference Model places the “reference monitor” component as a separate entity from the “resource” component. In fact, the model allows for the implementation of one reference monitor for multiple resources, and multiple reference monitors for multiple resources. Our approach adds an important additional requirement, which states that the implementation of the security enforcement mechanism be an integral and inseparable part of the system (or resource) that it is protecting.

4. Conclusion

This paper presented a strong case showing that insider threat is a major problem that organizations must be aware of and proactively mitigate if they are to minimize security breaches and attacks against their sensitive data and computing infrastructure. We also presented a list of some of the major security breaches in recent years. We argued that the most effective approach to uninterrupted defense strategy is to make the defense components an integral and inseparable part of the whole system. In addition, we alluded to an innovative approach to implementing autonomic capabilities into database systems in order to enable self-protection. The cornerstone of our approach is the full integration and verification of security policies into the database that they are intended to protect. By

doing so we embed into the database autonomic capabilities that provide it with a superior self-protection mechanism that surpasses, in its effectiveness, existing database security frameworks.

10. References

[1] Bishop, M. and C. Gates, Defining the Insider Threat. CSIIRW'08 - ACM, 2008.

[2] Mallery, J., Hackers Are Not the Biggest Threat to Data: Employees Are. Information Systems Security, www.infosectoday.com, 2007.

[3] Bishop, M. and D.A. Frincke, Combating the Insider Cyber Threat. IEEE Security & Privacy, 2007: p. 61-64.

[4] RSA, The Insider Security Threat in I.T. and Financial Services: Survey Shows Employees' Everyday Behavior Puts Sensitive Business Information at Risk. http://www.rsa.com/press_release.aspx?id=9703, 2008.

[5] Tan, L., Asia worried about insider threat. ZDNet Asia, http://www.zdnetasia.com/insight/specialreports/it-priorities/2008/0,3800016949,62047738,00.htm, 2008.

[6] Cisco, Cisco Data Leakage Study Assesses the 'Insider Threat'. Global Security Research Reveals Scope of Employee Risk, Biggest Concerns Around Information Loss Due to Inadvertent and Malicious Behavior. http://newsroom.cisco.com/dlls/2008/prod_111208.html, 2008.

[7] Witting, M., The Biggest Security Threat for 2008 and Beyond: End Users. TechNewsWorld, 2008.

[8] Carroll, M.D., Information Security: Examining and Managing the Insider Threat. InfoSecCD Conference'06 - ACM, 2006.

[9] CERT, 2004 E-Crime Watch Survey. 2004.

[10] US-CERT, 2006 E-Crime Watch Survey from CSO Magazine Reveals Insider Threats are on the Rise. www.us-cert.gov, 2006.

[11] Wilshusen, G.C., Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. United States Government Accountability Office, 2008: p. 1-35.

[12] Associated-Press, Pepsi Alerted Coca-Cola to Stolen-Coke-Secrets Offer. www.foxnews.com, 2006.

[13] CERT, 2007 E-Crime Watch Survey. www.cert.org, 2007.

[14] FBI, 2005 FBI Computer Crime Survey. www.fbi.gov/publications/ccs2005.pdf, 2005.

[15] Henry, E., Obama's cell phone records breached. www.cnn.com, 2008.

[16] CNET, CNET News. http://news.cnet.com, 2005.

[17] Costello, T., Massive bank security breach uncovered in N.J., www.msnbc.msn.com, 2005.

[18] CSO, CSO Online. www.csoonline.com, 2008.

[19] Lee, H.K., Stealing PINs land Folsom man in pen. San Francisco Chronicle, 2006.

[20] Goodchild, J., State Breach Disclosure Laws - Update. www.csoonline.com, 2008.

[21] Vijayan, J., Tough economic climate can heighten insider threat. www.computerworld.com, 2008.

[22] Dishneau, D., Feds allege plot to destroy Fannie Mae data, The Associated Press, 2009.

[23] M.C. Huebscher and J.A. McCann, ``A survey of Autonomic Computing - degrees, models and applications,'' ACM Computing Surveys, Vol 40, Issue 3, August 2008.

[24] O. Babaoglu, M. Jelasity, A. Montresor, C. Fetzer , S. Leonardi, A. van Moorsel, and M. van Steen, eds., Self-Star Properties in Complex Information Systems, Lecture Notes in Computer Science, Vol. 3460, Springer Verlag, 2005.

[25] S. Hariri and M. Parashar, eds., Autonomic Computing: Concepts, Infrastructure, and Applications, CRC Press, 2006.

[26] D.A. Menasce and J.O Kephart, Guest Editor Introduction, Special issue on Autonomic Computing, IEEE Internet Computing, Vol. 11, No. 1, January/February 2007.

[27] Jabbour, G. and D.A. Menasce, Policy-Based Enforcement of Database Security Configuration through Autonomic Capabilities. The Fourth International Conference on Autonomic and Autonomous Systems (ICAS 2008), March 16-21, 2008, 2008

[28] Anderson, J., Computer Security Technology Planning Study, ESD-TR-73, Vol. II, October 1972.