A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders

ANDREW P. MOORE, CERT® Program, Software Engineering Institute
MICHAEL HANLEY, CERT Program, Software Engineering Institute
DAVID MUNDIE, CERT Program, Software Engineering Institute

A research project at the CERT® Program is identifying enterprise architectural patterns to protect against the insider threat to organizations. This paper presents an example of such a pattern—Increased Monitoring for Intellectual Property (IP) Theft by Departing Insiders—to help organizations plan, prepare, and implement a means to mitigate the risk of insider theft of IP. Our case data shows that many insiders who stole IP did so within 30 days of their termination. Based on this insight, this pattern helps reduce that risk through increased monitoring of departing insiders during their last 30 days of employment. The increased monitoring suggested by the pattern is above and beyond what might be required for a baseline organizational detection of potentially malicious insider actions. Future work will develop a library of enterprise architectural patterns for mitigating the insider threat based on the data we have collected. Our goal is for organizational resilience to insider threat to emerge from repeated application of patterns from the library.

Categories and Subject Descriptors: **H.1.1 [Models and Principles]**: Systems and Information Theory—*Value of information*; **H.1.2 [Models and Principles]**: User/Machine Systems— *Human Information Processing; Human Factors.*

General Terms: Security

Additional Key Words and Phrases: insider threat, security pattern, organizational pattern, enterprise architecture, information security, information assurance, cyber security

ACM Reference Format:

Moore, A.P., Hanley, M., and Mundie, D. 2012. A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders. 18th Conference on Pattern Languages of Programs (PLoP). PLoP'11, October 21-23 (October 2011), 10 pages.

1. INTRODUCTION

Over the last decade, the CERT® Program at the Software Engineering Institute has cataloged hundreds of cases of malicious insider crimes prosecuted in United States courts. Insiders include current or former employees, contractors, and other business partners—anyone with authorized access to an organization's systems beyond that provided to the general public. Malicious insider threat is the potential harm from insiders intentionally using or exceeding their authorized access in a way that damages the organization. Notice that this definition includes individuals who do harm by misusing their legitimate access privileges and those who do harm by taking advantage of their knowledge of the organization and its systems. However, it does not include individuals who damage the organization unintentionally. While the inadvertent insider threat is an important one, it is beyond the scope of our work.

Insider threats do not typically involve a technically sophisticated attack traversing strategically layered countermeasures or a complex back-and-forth between attacker and defender. However, insider threat defense needs to be broad because of the insider's authorized physical and logical access to the organization's systems and intimate knowledge of the organization itself. Current solutions to insider threat are largely reactive and tactical; they do not address the architectural needs demanded by the holistic nature of the problem. As a result, the sensitive, possibly classified, information stored on organizations' information systems is highly vulnerable to disgruntled employees, who may decide to seek revenge for a

Author's address: A.P. Moore, CERT Program, Software Engineering Institute, Carnegie Mellon University, 4500 Fifth Avenue, Pittsburgh, PA 15213; email: apm@cert.org. Michael Hanley, CERT Program, Software Engineering Institute, Carnegie Mellon University, 4500 Fifth Avenue, Pittsburgh, PA 15213; email: mhanley@cert.org. David Mundie, CERT Program, Software Engineering Institute, Carnegie Mellon University, 4500 Fifth Avenue, Pittsburgh, PA 15213; email: dmundie@cert.org.

perceived injustice, or greedy employees, who may decide to take advantage of organizational information for their own personal advantage.

Our analysis of the case data has identified more than 100 categories of weaknesses in systems, processes, people, or technologies that allowed insider attacks to occur. Many of these weaknesses are due to failures during the system or software development life cycle that are then perpetuated by failures associated with people, processes, and technology. Research at the CERT Program is identifying enterprise architectural patterns that protect against the insider threat to organizational systems. Enterprise architectural patterns are organizational patterns that involve the full scope of enterprise architecture concerns, including people, processes, technology, and facilities. This broad scope is necessary because insiders have authorized online and physical access to systems. In addition, insiders have knowledge of vulnerabilities in organizational business processes, which malicious insiders have exploited as often as they have exploited technical vulnerabilities.

As shown in Figure 1, we plan to develop a library of insider threat enterprise architectural patterns based on the data we have collected, our completed analyses of the data (Cappelli et al. 2008, Moore et al. 2011, Hanley 2010, Hanley et al. 2011), and previous work documenting security patterns and architectural styles (Schumacher et al. 2006, Ellison et al. 2004). We will develop a baseline enterprise architecture that establishes the organizational starting point for the application of these patterns. Based on that starting point, an organization would choose architectural patterns from the library to meet its security needs. Using this process, the organization would refine its enterprise architecture to have greater protection against insider threat along the dimension handled by the pattern. The organization would develop a greater overall resilience to insider threat by repeated application of patterns from the library to refine its enterprise architecture. In turn, the use of these patterns will lead to insights into how they can be improved.

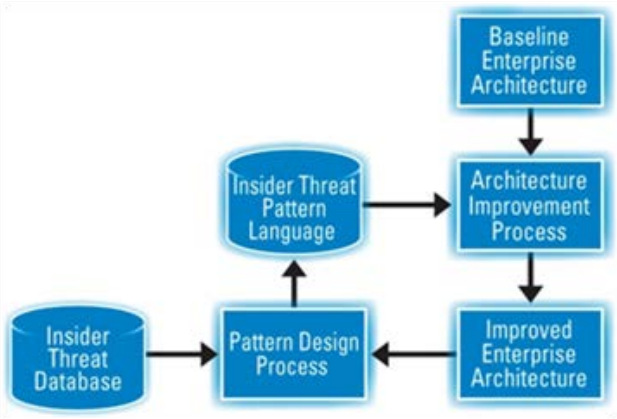

Fig. 1. Approach to developing an insider threat enterprise architectural pattern library

This paper presents a pattern we are developing as a proof of concept of the use of patterns to document insider threat mitigation strategies. The pattern calls for increased monitoring of insiders leaving the employment of an organization based on the insight from our case data that many insiders who stole their organization's information stole at least some of it within 30 days of their termination. The pattern is presented in the standard POSA form.

2. INCREASED MONITORING FOR INTELLECTUAL PROPERTY (IP) THEFT BY DEPARTING INSIDERS

2.1 Intent

The Increased Monitoring for IP Theft by Departing Insiders pattern helps an organization plan, prepare, and implement a means to mitigate the risk of insider theft of IP. Case data shows that risk is greatest at the point of employee termination. This pattern helps reduce that risk through increased monitoring of insiders leaving the employment of an organization. The increased monitoring suggested by the pattern is above and beyond what might be required for a baseline organizational detection of potentially malicious

insider actions. This detection and response pattern should also be used in addition to patterns for the prevention of insider theft of IP.

The intended audience of this pattern is data owners within an organization as well as managers across the organization from departments in Information Technology, Human Resources, Physical Security, and Legal. Data owners are those individuals who make the decisions regarding the protection requirements for certain data, including who has access to the data.

The pattern applies to organizations large enough to have these distinct departments and roles. However, smaller organizations may also benefit from application of this pattern if they can identify individuals that have the associated responsibilities. The pattern will be directly applicable to organizations based in the United States since the insider behaviors were seen in criminal cases prosecuted therein. Application to organizations based outside the U.S. should be careful to ensure that the countermeasures put in place are legal and acceptable given the regulation and norms prevalent in the country of origin.

2.2 Example[1]

Steve was a software developer for a company specializing in data-mining software development. At its inception, the company employed Steve and his friend Gary, a sales representative. Gary left the company a few years later to form his own company, which also specialized in developing applications for business data mining. Later that same year, Gary contacted Steve to persuade him to join his startup to help develop a competing product. With a promise of more control and the chance to make a fortune, Steve agreed. At Gary's urging, Steve also decided to take some of the code that he helped develop at his current company to implement the more sophisticated algorithms at the new startup.

During the last six months of the year, Steve progressively accessed and downloaded parts of the source code. The downloaded code included the portion he wrote and some other portions written by his teammates. He even tried to obtain technical information about the code from his colleagues. Some employees noticed Steve's unusual activities, but they viewed him as a workaholic and did not report their observations to their supervisors. After downloading the last major component early in December, Steve submitted his resignation effective the end of the year. He cited family reasons for his resignation and mentioned his plan to find a less stressful job after a short break. Steve's boss asked him to work with a junior member of the team to take on Steve's responsibilities after he leaves.

Several months after Steve's departure, some of the company's customers called to cancel orders, claiming they could get similar software for a lower price. The company conducted an internal investigation and discovered Steve's pattern of frequent accesses and downloads prior to his resignation. They also recognized the company offering the lower-priced software as the company that Gary recently formed. Management was extremely concerned that their IP had been compromised, and they called in law enforcement to investigate.

2.3 Context

The context for this problem is an organization that has valuable IP at risk of insider theft. Intellectual property includes any sensitive or confidential information owned by an organization that it would like to protect. An insider of an organization includes any employee, contractor, or other business partner of an organization. The critical point of action by the organization is when an insider is being terminated either voluntarily (e.g., through resignation) or involuntarily (e.g., through firing).

2.4 Problem

How can the organization mitigate the risk of losing its critical IP in a cost-effective way? Data on 48 cases of theft of IP in our insider threat database shows that well over 50 percent of the insiders who stole their organization's information stole at least some of the information within 30 days of their termination. Current case trends suggest that organizations regularly fail to detect theft of IP by insiders, and even when theft is detected, organizations find it difficult to attribute the crime to any specific individual.

The solution to this pattern is affected by the following forces:

- ***Cost of monitoring:*** Monitoring insiders' online actions can be costly, so it is necessary to balance the extent of monitoring with the value of that monitoring.

[1] The example described is a fictional, but representative, case of insider theft of IP derived from studying the patterns of such cases in the CERT insider threat database. It was adapted from work done by Christopher Nguyen while employed at the CERT Program.

- ***Employee privacy:*** Organizations need to ensure they do not violate employees' legal rights to privacy.
- ***IP ownership rights:*** Organizations need to ensure they have ownership rights to the IP they wish to protect so that if disagreements arise, the organization's right to the IP stands up in the courts.
- ***Employee productivity:*** Insiders' time and effort are valuable resources to an organization. Organizations may desire or need to keep employees productive while they are on the payroll as long as organizations can balance productivity with the risk of IP theft.
- ***Monitoring propriety:*** Organizations need to ensure they are monitoring employees according to applicable laws and industry norms. For example, organizations should properly obtain insiders' consent to monitoring as a condition of employment.

2.5 Solution

To deal adequately with the risk that departing insiders might take valuable IP with them, the organization must ensure that the necessary agreements are in place (IP ownership and consent to monitoring), critical IP is identified, key departing insiders are monitored, and the necessary communication among departments takes place. When an insider resigns, the organization should increase its scrutiny of that employee's activities within a 30-day window before the insider's termination date.

Computer audit logs of employee online actions must be kept for at least 30 days so that those logs may be scrutinized even if an insider decides to terminate his association immediately. The logs must have been protected from tampering by the insider and the person who monitors the logs must be trustworthy to report suspicious behavior found upon investigation. Actions taken upon and before employee termination are vital to ensuring IP is not compromised and the organization preserves its legal options. Keeping audit logs for longer than 30 days may be useful for more in-depth investigation of suspicious behavior and for prosecution of any criminal activities.

Figure 2 illustrates the structure and dynamics of the solution as a sequence diagram. The structure is represented by the main organizational departments or groups involved in the solution along the top middle of the diagram: human resources, data owners, and IT staff or systems. The IT systems could play the IT-related role if the monitoring role is automated, or IT staff could if the monitoring is manual. The insider's involvement is shown along the left side of the diagram and the monitoring of the critical IP is shown along the right side.

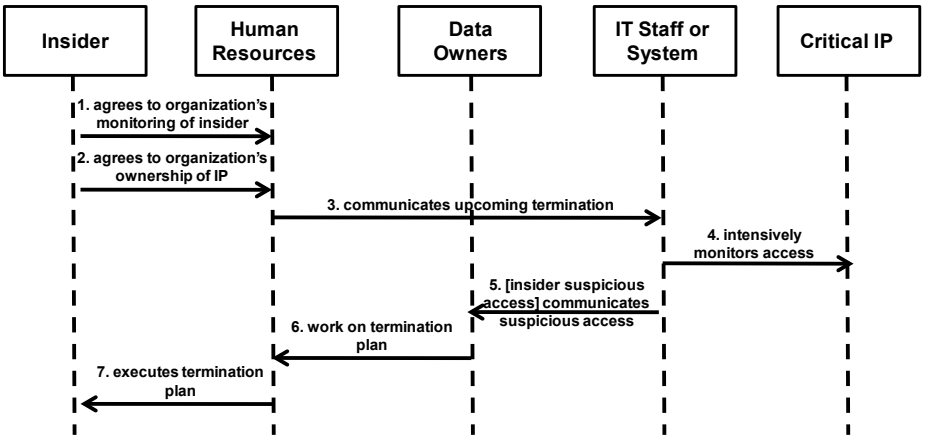

Fig. 2. Sequence diagram for increased monitoring of departing insiders

The solution dynamics are portrayed in the interactions among the actors with the roles and responsibilities listed along the top of Figure 2. An organization needs to make sure its employees, as a condition of employment, consent to monitoring (see Interaction 1) and agree that the organization owns the critical IP (Interaction 2). The employee's clear and formal acceptance of the organization's IP ownership helps ensure that the organization's right to ownership will stand up in court. Consulting with the organization's legal counsel will help ensure the organization is on firm legal ground. The organization can

convey ownership to employees through devices such as nondisclosure agreements, IP ownership policies, and references to IP ownership in a network-acceptable-use policy.

We assume that data owners identify and properly label their IP. HR needs to track insiders who have access to the IP so that when the insider resigns HR can ask IT staff or systems to monitor that insider's online behavior for signs of suspicious exfiltration of IP (Interaction 3). Data in the insider threat database shows that scientists, engineers, programmers, and salespeople are especially likely to steal IP. IT staff or systems need to closely monitor the insider's access to critical IP during the 30-day window before termination (Interaction 4) because many IP thieves have stolen information within this window. Although the organization may decide to begin monitoring before the 30-day window, restricting monitoring to this period may allow the organization to balance the monitoring costs with the risks of losing the IP. No matter what level of monitoring is used, organizations must ensure that insiders are treated consistently and fairly.

IT staff or systems must inform the data owners of any suspicious access to critical IP, and the data owners must be included in the response decision-making (Interaction 5). The organization needs to be able to either block exfiltration or detect it and confront the employee. If the suspicious activity occurs prior to termination, HR and the data owners need to formulate an appropriate response as part of the termination plan (Interaction 6). The organization can then confront the employee with that response during the exit (termination) interview (Interaction 7). If the insider has violated an agreement regarding IP, the organization may wish to pursue legal remediation, with advice from its legal counsel.

2.6 Implementation

Investigation and response activities may be necessary if IT staff or systems discover suspicious activity by the insider. During the 30-day window, several items may warrant a detailed investigation. Based on findings from a more focused study of technical concerns in cases of theft of IP (Hanley 2010), organizations should be especially concerned with exfiltration of data using the organization's network, specifically through either corporate email or personal webmail access. Considerations should include the following:

- ***Download of a large volume of critical IP to removable media/laptop or via remote file access:*** Large-volume downloads close to insider termination may indicate that the insider is preparing to exfiltrate data. Case information suggests that users who exfiltrate a large amount of information via email or other means first move that data over the network to their workstation. Movement of data within enclaves or across enclaves that exceeds normal traffic patterns may signal this type of event.
- ***Email to the organization's competitors or the insider's personal account:*** Most insiders who steal information through networked systems do so by either emailing information off the network through a corporate account or through webmail. Corporate email accounts can be configured to alert the organization to suspicious events from mail transaction logs. For example, if an organization enumerates (but does not blacklist) suspicious transactions, such as data transfers to competitors, then it can be alerted to any mail traffic generated to/from the departing employee, particularly if these messages appear to have attachments or have relatively large byte counts. Further, many insiders email IP to their personal webmail accounts and then forward it to an outside collaborator. For example, a user can simply open a browser, log into a personal Gmail account, attach documents, and send them off the network. Organizations need to consider monitoring for uploads to known webmail domains to mitigate these behaviors.

Organizations with a central logging scheme can configure a query to search indexed log files for events that align closely with this pattern of behavior by departing insiders during their last 30 days of employment. Consider the following implementation outline:

if *the mail is from the departing insider*
and *the message was sent in the last 30 days*
and *the recipient is not in the organization's domain*
and *the total bytes summed by day are more than a specified threshold*
then *send an alert to the security operator*

This solution first keys upon the population of departing insiders, and then it sets a time window of 30 days, representing the window before termination, in which to search for suspicious mail traffic. Since the

30-day window is the finding from behavioral modeling work that we find most interesting, this serves as the root of the query. Possible data sources that could be used to instantiate this attribute in a live query include an Active Directory or other LDAP directory service, partial HR records that are consumable by an indexing engine, or other proxies for employee status such as physical badge access status. HR systems do not always provide security staff with a simple indicator that an employee is leaving the organization. Instead, suitable proxies (preset account expiration, date the account is disabled, etc.) can be used to bound the 30-day window for targeted monitoring. Assuming employers actively disable accounts at termination, the appropriately generated alert can be queried for the associated event ID or known text (as in the example implementation below) to find all employees leaving the organization. Depending on the structure of the remainder of the query, particularly if the only initial result is a user identification (UID) string, some customization here to convert a UID string to a user's email address may be useful. The example later in this paper simply concatenates the UID to the local domain name.

Once the query identifies all mail traffic from departing users in their 30-day window, the next search criteria identifies mail traffic that has left the local domain namespace of the organization, or another logical boundary in the case of a large federation of disparate namespaces or a wide trust zone with other namespaces. This identifies any possible data exfiltration via email by identifying messages where the intended recipient resides in an untrusted zone or in a namespace the organization otherwise has no control over. Specific intelligence or threat information may allow for significant paring of this portion of the query down to perhaps even very specific sets of "unwanted" recipient addresses by country code top-level domains (ccTLD), known-bad domain names, or other similar criteria.

Because not all mail servers indicate an attachment's presence uniformly, the query next narrows mail traffic leaving the local namespace or other organizational boundary by byte count per day to indicate data exfiltration. Setting a reasonable per-day byte threshold, starting between 20 and 50 kilobytes, should allow the organization to detect when several attachments, or large volumes of text pasted into the bodies of email messages, leave the network on any given day. This variable provides an excellent point at which to squelch the query as a whole.

An Implementation Using Splunk. Organizations using Splunk[2] for centralized log indexing and interrogation can configure it to raise an alert when it observes the behaviors discussed above. The following is a Splunk rule that organizations could adjust to their particular circumstances. The sample rule uses a sample internal namespace to illustrate the implementation. We assume a generic internal namespace of corp.merit.lab, with two servers of interest. MAILHOST is an Exchange server, and DC is an Active Directory Domain Controller.

```
Terms: 'host=MAILHOST
        [search host="DC.corp.merit.lab"
                Message="A user account was disabled. *"
                | eval Account_Name=mvindex(Account_Name, -1)
                | fields Account_Name
                | strcat Account_Name "@corp.merit.lab" sender_address
                | fields - Account_Name]
        total_bytes > 50000 AND recipient_address!="*corp.merit.lab"
        startdaysago=30
        | fields client_ip, sender_address, recipient_address,
        message_subject, total_bytes'
```

Breaking this query into manageable segments shows how it tries to address all the items of concern from this pattern.

Mail from the Departing Insider: *'host=MAILHOST []*. This query is actually a nested query. In this demonstration, the outermost bracket refers to a mail server, MAILHOST, and looks for a set of information first pulled from DC, a domain controller in the sample domain. Because the log query tool seeks

[2] Splunk (http://splunk.com) is an indexing and data analysis suite. It was used for this demonstration only because of prior operational experience with the tool.

employees leaving within the 30-day activity window, the logical place to start looking for employee information is the local directory service.

HR systems do not always provide security staff with a simple indicator that an employee is leaving the organization. To account for this situation, suitable proxies (preset account expiration, date the account is disabled, etc.) can be used to bound the 30-day window for targeted monitoring. Assuming employers actively disable accounts at termination, an appropriately generated alert can be queried for the associated event ID or known text (as in this demonstration) to find all employees leaving the organization. The query then concatenates the account name associated with the disable event to a string that ends with the organization's DNS suffix ("@corp.merit.lab" in this demonstration) to form a string that represents the email sender's address. This ends the first component of the query and provides the potentially malicious insider's email address.

Total Bytes Summed by Day More than Specified Threshold: *total_bytes > 50000.* Not all mail servers provide a readily accessible attribute indicating that an email message included an attachment. Thus, the mail server is configured to filter first for all messages "of size" that might indicate an attachment or a large volume of text in the message body. This part of the query can be tuned as needed; 50,000 bytes is a somewhat arbitrary starting value.

Recipient Not in Organization's Domain: recipient_address!="*corp.merit.lab". This portion of the query instructs Splunk to find only transactions where the email was sent to a recipient not in the organization's namespace. This is a vague query term that could generate many unwanted results, but it does provide an example of filtering based on destination. Clearly, not all messages leaving the domain are malicious, and an organization can filter based on more specific criteria such as specific country codes, known-bad domain names, and so on.

Message Sent in the Last 30 Days: startdaysago=30. This sets the query time frame to 30 days prior to the date of the account disable alert message. This can be adjusted as needed, though the data on insider theft of IP exhibits the 30-day pattern discussed previously.

Final Section: fields client_ip, sender_address, recipient_address, message_subject, total_bytes'. The final section of the query creates a table with relevant information for a security operator's review. The operator receives a comma-separated values (CSV) file showing the sender, recipient, message subject line, total byte count, and client IP address that sent the message. This information, along with a finite number of messages that match these criteria, should provide sufficient information for further investigation.

2.7 Example Resolved

Despite having signed an IP agreement and consented to monitoring as part of his employment, Steve still decided to take the source code with him when he left the company. He felt guilty at his exit interview when he confirmed that he understood that the organization owns the IP, but the temptation to join Gary and finally make some "real money" was too great. Besides, he developed much of the code that he was taking, so he felt entitled to it.

But because the organization was monitoring Steve's online behaviors in the weeks prior to his resignation, they saw the download of software components, some of which Steve had not even been associated with. Further investigation showed a pattern of downloads during the second half of the year. The company consulted with their legal counsel about the proper course of action. At the end of the exit interview, they confronted Steve about his pattern of suspicious downloads.

Shocked by this development, Steve insisted that this was just part of trying to do his job well. Secretly, however, he was devastated and unsure what to do. He had already supplied much of the source code to Gary, but he realized that the company had a solid case if it decided to go to court. He called Gary to tell him about the development. Gary audibly gasped upon the news and hung up. Steve never heard from Gary again. The company mailed a cease-and-desist letter to Gary informing him of the court action they would take if he continued selling the stolen software. Intimidated by the possibility of the legal costs

associated with a court battle and the loss of his only developer, Gary closed his business and started working for his father-in-law's retail sporting goods store selling children's tennis apparel.

2.8 Consequences

The Increased Monitoring for IP Theft by Departing Insiders pattern has several benefits:

- ***Insiders stay relatively productive.*** Employees' time and effort are valuable resources to an organization, especially when the organization is trying to transfer knowledge, skills, and responsibilities from a departing insider to someone else. This pattern allows organizations to keep insiders productive as long as they are on the payroll, while keeping the risk that the insider will abscond with the organization's IP at an acceptable level. This pattern allows insiders the dignity of working up to the point of their departure and does not strain the relationship between current and departing insiders.
- ***Monitoring is tailored to ensure cost effectiveness.*** The organization can tailor their monitoring for theft of IP to those insiders most likely to commit the crime: insiders voluntarily or involuntarily departing the organization. Monitoring all employees all the time is not an affordable or practical option for most organizations. This pattern provides organizations a means to balance the extent of monitoring with the value provided by that monitoring.
- ***Monitoring is relatively fair.*** Organizations must be careful not to target particular employees for monitoring for unlawful or unethical reasons (e.g., ethnicity, gender, creed) and that they get insiders' consent to monitor. This pattern recommends getting insiders' informed consent to monitoring as a condition of employment and using the same criteria for increased monitoring for all employees departing the organization.
- ***IP ownership is upheld.*** This pattern makes sure that organizations have the proper IP agreements in place when prospective employees accept and start employment with the organization. This reduces the chance of misunderstanding and increases the chance that organizations will maintain their rights to the IP should disagreements arise.

The Increased Monitoring for IP Theft by Departing Insiders pattern also imposes liabilities:

- ***Access to non-committed insiders is allowed.*** A risk of getting value from insider work until termination is that the insider may act counter to organizational interests. In that period between resignation and termination, the insider's loyalty to the organization will be diminished. If those risks are unacceptable, even with the added precautions provided by this pattern, organizations may need to cut off access immediately after resignation.
- ***Insiders may be alienated.*** Requiring prospective employees to agree that the organization owns employee-developed IP and that they consent to monitoring of their use of organization systems may put the organization at a disadvantage when hiring. Organizations may have difficulty hiring or keeping the people they need, especially if the agreements required are more stringent than industry norms. In addition, an insider's knowledge or suspicion that the organization is monitoring them may negatively affect the insider's trust relationship with the organization. Loss of loyalty to the organization may result. Educating insiders on the reasons and mutual benefits of organizational monitoring may help to counteract these negative consequences. Insiders may learn to "fly under the radar." Insider IP thieves in the cases in our database have been technically unsophisticated and opportunistic, for the most part. This suggests some simple roadblocks to the theft are going to go a long way in preventing damages to organizations. However, there is the possibility that insiders will discover that organizations are using the 30-day window as the basis for detecting planned theft of IP. If rather than deterring the crime, insiders simply steal the IP before the 30-day window, a game of "cat-and-mouse" will ensue between the organization and the insider and this pattern will become largely ineffective. However, this pattern should deter as many insiders along this path of escalation as it does encourage them to become stealthier, so we still believe that benefits will accrue overall.

2.9 Known Uses

The authors are unaware of any implementation of the pattern in a production environment. However, there are prototype implementations being tested in a laboratory environment, and components of the

pattern are widely deployed and embodied in cyber security standards required by the Federal Information Security Management Act of 2002 (FISMA), a United States federal law mandating a foundational level of security for all federal information and information systems. NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," describes the controls required by FISMA (NIST 2009). NIST 800-53 includes, among many other things, best practices regarding audit log review and analysis (AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING) and protection against data exfiltration across boundaries (SC-7 BOUNDARY PROTECTION). These controls form the basis of the Increased Monitoring for IP Theft by Departing Insiders pattern. The requirement that NIST 800-53 controls must be based on broad community consensus prior to their inclusion and the requirement that federal agencies must by law implement these controls indicate that domain experts believe that the basis for the Increased Monitoring for IP Theft by Departing Insiders is solid.

In addition, this pattern is based on the CERT Program's analysis of insider threat cases, which show that well over 50 percent of the theft of IP cases involved significant downloads in this 30-day window. We believe this provides well-grounded evidence that this pattern will be effective for organizations wishing to balance monitoring cost with IP theft risk.

2.10 See Also

- ***Insider Threat Detection Baseline Pattern.*** While monitoring is an essential part of mitigating insider threat, the Increased Monitoring for IP Theft by Departing Insiders pattern focuses on the added monitoring above a baseline level that is specifically targeted to the risk of exfiltration by a departing insider. Baseline levels of monitoring not tied to a specific time window need to be in place to detect other manifestations of the insider threat. In the future, we hope to define more general insider threat detection patterns, but we believe the Increased Monitoring for IP Theft by Departing Insiders pattern should stand alone. That said, this pattern will likely need to be refactored when we do define other detection patterns because it has elements that apply to insider threat detection generally.
- ***Trust Trap Mitigation Pattern*.** The Trust Trap Mitigation pattern focuses on problematic organizational behavior in which excessive trust of insiders can lead to insufficient monitoring, a lack of detection of concerning activities, and even greater trust in potentially misbehaving insiders (Mundie and Moore 2011). The Increased Monitoring for IP Theft by Departing Insiders pattern provides a means for organizations to make sure their monitoring of departing insiders sufficiently limits the possibility of organizations falling into the trust trap with respect to IP theft.
- ***Escort Terminated Insider Pattern***. This pattern recommends cutting off the insider's network access and escorting the insider off the premises immediately after receiving notification of the insider's resignation. This pattern would put much more emphasis on risk reduction than the insider's productivity following resignation notification. However, negative unintended consequences are possible, including lost productivity and goodwill, especially if the insider is immediately escorted off the premises. Providing a severance package as sign of goodwill could mitigate these negative consequences.

3. CONCLUSION

Architectural patterns and pattern systems developed through this research will enable coherent reasoning about how to design and, to a lesser extent, implement enterprise systems to protect against insider threat. Instead of being faced with vague security requirements and inadequate security technologies, system designers will be armed with a coherent set of architectural patterns that will enable them to develop and implement effective strategies against the insider threat in a timelier manner and with greater confidence.

ACKNOWLEDGEMENTS

The authors extend our heartfelt appreciation to Dr. Eduardo Fernandez, Professor in the Department of Computer Science and Engineering at Florida Atlantic University. His review and guidance as part of the PLoP 2011 conference shepherding process led to immense improvement in the understanding and articulation of this pattern. In addition, we thank Paul Ruggiero of the Software Engineering Institute for his careful and detailed technical editing of this pattern, which dramatically improved its readability and flow. Finally, thanks to Carly Huth for providing helpful advice regarding the legal aspects of our example scenario.

REFERENCES

Buschmann, F.; Henney, K.; & Schmidt, D.C. Pattern-Oriented Software Architecture Volume 5: On Patterns and Pattern Languages. Wiley, 2007 (ISBN 978-0471486480).

Cappelli, D.M.; Moore, A.P.; Trzeciak, R.F.; and Shimeall, T.J. Common Sense Guide to Prevention and Detection of Insider Threat (3rd ed.). CERT Program, Software Engineering Institute, and CyLab of Carnegie Mellon, 2008.

Ellison, R.J.; Moore, A.P.; Bass, L.; Klein, M.; and Bachmann, F. Security and Survivability Reasoning Frameworks and Architectural Design Tactics (CMU/SEI-2004-TN-022). Software Engineering Institute, Carnegie Mellon University, 2004.

Hanley, M. “Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data.” Proceedings of the 2010 NSA CAE Workshop on Insider Threat, November 2010.

Hanley, M.; Dean, T.; Schroeder, W.; Houy, M.; Trzeciak, R.F.; and Montelibano, J. An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases (CMU/SEI-2011-TN-006). Software Engineering Institute, Carnegie Mellon University, 2011.

Moore, A.P.; Cappelli, D.M.; Caron, T.C.; Shaw, E.; Spooner, D.; and Trzeciak, R.F. “A Preliminary Model of Insider Theft of Intellectual Property.” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2, 1 (Special Issue Addressing Insider Threats and Information Leakage, 2011): 28-49.

Mundie, D.A. and Moore, A.P. , “A Pattern for Trust Trap Mitigation,” Proceedings of the 2011 Conference on Pattern Languages for Programs, forthcoming.

NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” Revision 3, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

Schumacher, M.; Fernandez-Buglioni, E.; Hybertson, D.; Buschmann, F.; and Sommerlad, P. Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons, Ltd, 2006.

This material is based upon work funded and supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.