Analysis of the Insider Attack Issue in the Movie, Banking, and Computer Industries

Mu Li
ID: 3325484
Computer Science Department
University of Auckland
October 2005
Mli051@ec.auckland.ac.nz

Abstract:

Insider attacks are now a world wide concern. The term "insider" has been widely used in security studies. However, we do not yet have a standard technical meaning for the term “insider”. Many authors use “insider” as a technical term in their writing without providing a detailed explanation. The problem is the actual meaning of “insider” may not be the same due to different point of view. This paper will outline how the term “insider” has been defined in different ways, in security studies of the movie industry, the banking and finance sector, and general computer applications. We also analyze the characteristics of those insider attacks and compare methods which have been applied to prevent or deter insider attacks in different industries.

Introduction:

All around the world, various kinds of insider attacks have existed for quite a long time and the term “insider” appears in the stories of newspaper or internet very frequently. Although in everyday life, people share a common sense of what the insider is, reading among research papers, the definition of insider actually turns out to be somehow different from each other, especially when putting it in different backgrounds

In a brief view, “insider” is a person who is employed by a business and therefore has the chance to know some inside news or can access internal information or data. Compare with outsiders, insiders have better knowledge about how their system works and that is why insider attack may cause more damage than outsider attack.

This paper firstly provides the definition of insider that is specified in movie, banking, and computer industries; secondly it summarizes the similarities and differences of insider attack in those three industry fields and thirdly a comparison of several insider attack mitigations are provided.

1 The Definition of Insider

Some different definitions of insider are shown below; they are collected from various sources. From those interpretations we can see even such a simple word could be explained in so many ways. That is the reason why general readers might be confused about what exactly means by “insider” without detailed explanation.

Banking and Finance Industry
“Individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm.” [2]
Movie Industry
“Insiders are members of the (at least partially) trusted community.” [1]
Computer Security
“Individuals who were, or previously had been, authorized to use information systems they eventually employed to perpetrate harm.” [8]
“An insider is someone who has been (explicitly or implicitly) granted privileges authorizing use of a particular system of facility. (This concept is clearly relative to virtual space and real time because at any given moment a user may be an insider with

respect to some services and an outsider with respect to others, with different degrees of privilege)” [9]
“The boundary between insiders and outsiders is fuzzy. (We assume) every legitimate user is an insider. The term “insider” can have both physical and logical connotation. Physical outsiders can be logical insiders and vice versa.” [3]
“it’s not just your people (employees) who may be insiders, contractors, friends, and janitors are a risk” [10]
“: Typically, insider attacks are thought of in terms of users; we have argued that human insiders are only one example of an insider. Applications, viruses, and malware in general all can operate as insiders to a system…” [11]

All the definitions are selected from reliable and professional source. An interesting issue could be noticed that the definitions not only differ among industries but also within single industry, that is mainly depends on author’s point of view.

However, the technical meanings of “insider” among different authors also show some uncertainties. Some author prefers to use “common sense” to interpret insider, for example in [12], the definition of insider is simply interpreted as “ex-employees” but in [3] the author talked about insider seriously and point out that the role of insider and outsider is not unchangeable and in some conditions outsider could turn into insider depends on how much inside knowledge/technology/skills an outsider has.

By analyzing those definitions, it shows that share one “standard” definition of what is “insider” among different industries will not be a good idea. For example, in computer security field it is a major concern that ex-employee should be counted as insider because they do have background knowledge or access privilege even they do not serve their company anymore. The common way of insider attack in this field focuses on remote access and malicious code [8] therefore even a person did not work for a company anymore he may still have abilities to make damage. The situation is different in movie industry, base on [1], the most inside leaks happen during production and distribution process, therefore current employees are the major concern. And for ex-employees, as they generally do not have chance to access movie content, so they would not be counted as insiders.

There is an interesting case mentioned in [1], it is, an early version of Universal's movie *The Hulk* is put on web before the theatrical release. It is a typical inside attack measuring by the author's rule "if the copy appearance date is prior to cinema release" [1]. The authors emphasize that "note that we consider all participants in the movie production and distribution process other than the end consumer to be insiders, although some are not employed directly by movie studios" [1]. However, the fact is, Kerry Gonzalez, the person who actually put the movie content on the internet is not an "insider", as he is not an employee of any movie company or trusted community at that time. So, the question is: who is the insider? From the information I searched from internet, the story goes like this: the online version of "Hulk" originated from a copy given to an advertising agency and an ad agency employee loaned the copy to a friend who subsequently loaned it to Gonzalez. Therefore although this is definitely an inside attack, Gonzalez is by no means an insider, the real insider is the person who worked for that advertising agency. From this case we can see how complex the definition of "insider" and "inside attack" are when it occurs in the real world.

2 Key Findings of Insider Attack Studies

The research of insider attack has been studying for several years. From 1996, CSI and FBI annually released their survey result which focuses on computer crime and security in order to raise the level of security awareness among different industry sectors. In this section, the key findings of insider attack will be discussed from those aspects:

- The insider's motive
- Insider characteristics
- Pre-attack behavior and planning
- Detecting the attack

By analyzing from those aspects, a better understanding on insider attack can be obtained. And it is helpful when we make policies to work against such kind of attack. The detailed analysis of insider attack mitigation will be discussed in part three.

2.1 The Insider's Motive

From [2] and [8], they show that the most insiders (81%) in Banking and Finance sector were motivated by financial gain; while in Computer security sector, most insider cases (92%) were triggered by a negative work-related event. For movie industry, according to [1], however, there is no clear evidence about motive and goal.

I searched the cases related to inside leaks and unauthorized duplication in the movie industry on the internet. However there is only few cases available and most of them do not talk about the case itself in details. Although it is difficult to elicit the insiders' motivation from the limited resource, some assumptions can be concluded. For example, Carmine Caridi, a Motion Picture Academy member who handed over his awards screeners for illegal duplication, ordered to pay $300,000 penalty to Warner Bros. Entertas ainment Inc. Caridi provided the DVD quality screeners to Sprague, who was found, owned hundreds of Academy screeners for recent and current movies in a search of his residence [13, 14]. Although Caridi denied receiving any money for the screeners, it is quite difficult to explain Sprague's intention aside from financial considerations.

2.2 Insider Characteristics

By comparing research results in [2] and [8], some insider characteristics can be summarized in a more common view.

Firstly, in both industry fields, perpetrators did not share a common profile. Insiders are in different age, have different racial and ethic background, also varied with gender and marital status.

Secondly, the working backgrounds of perpetrators in [2] are different from those in [8]. Most insiders in banking and finance sector did not hold a technical position, but most insiders who conduct computer system sabotage were either previously or currently employed in a full-time technical position.

Thirdly, most insiders (70%) in banking and finance sector committed acts while on the job; in contrast, insider attack in computer system sabotage was mainly performed by ex-employees and the majority of attacks took place outside normal working hours.

While the insider attacks differ a lot between the two industries, they do share some similarities—the research result shows that most of the insiders do not have an arrest history. But only few insiders were perceived as problem employees in [2] compare with the situation in [8]. In [8] most of the insiders had acted out in a concerning manner in the workplace and noticed by others.

2.3 Pre-attack Behavior and Planning

In both [2] and [8], perpetrators planned their action in advance and the intention of insider attack could be noticed by others. The difference is, in banking and finance sector those people who had knowledge of the insider's intention are often directly involved in the planning or stand to benefit from the activity, while in [8], those signs of coming attack are always ignored as the "strange nature" of technique geeks.

Due to the lack of information, no conclusion or assumption can be summed up in the movie industry. The insider attack study in movie industry is not fully explored compare with other fields.

2.4 Detecting the Attack

In both [2] and [8], insider attack incidents are not only detected by security staff. Incidents are detected by a range of people both internal to the organization and external such as customers, security personnel and non-security personnel.

In banking and finance sector, most of the insiders are detected by customers (35%) including account holders, credit card holders and money lenders [2]. In addition, most of the insiders are detected through manual procedures (e.g. auditing). This finding proved that in this sector, both the conducts of attack and detection involve little high-tech knowledge.

The attack detection in computer security sector becomes a little bit complicated. Although most insiders only use “unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures” to perform an attack, the majority of attacks are only detected once a noticeable system irregularity occurred or a system became unavailable [8]. In addition, insiders also took steps to conceal their identities by using others account or creating unauthorized accounts and backdoors. Those actions increase the difficulty to identify the insider and that is why using forensic examinations against insider attack has becoming more and more popular [8].

Again, insider attack in the movie industry has not been studied very extensively. The reason of why [1] was widely referenced by lots of articles and essays is that paper is the pilot of insider attack study in the movie industry sector. In the past, the highlighted topic discussed within this field focuses on how to prevent movie piracy and now the focus turns to exam the source of pirated movie. It is a progress.

3 Insider Attack Mitigation

Since insider attack has been widely aware by public, many prevention efforts have been developed after researching and analysis security measures in different industries. The following overview of insider attack prevention is classified into two sub-areas. The first one focuses on the “human factor”, the second one focuses on the “technical factors”.

As an attack cannot be performed successfully without human being’s involving, only focusing on technique improvement might not have the best efforts. According to researching results, there are clear evidences show that technique skills is not the only necessarily strength for an insider. Many attacks succeed due to weak security or management policies. Even an organization has fully developed policies, if those policies are not executed/applied completely, insider will always find a way in. Additionally, insiders have been more and more carefully when they perform their acts, they might use more than one way to cover their actions and conceal the trace they left. Therefore, it is necessary that companies and organizations review their employee management policies frequently to improve and adjust the efficiency of their policy.

The table below lists the different methods which have been suggested and applied [1, 2, 3, 8, 9, 12]. Of course, it is likely that some measures are not publicized for security concern. By analyzing this table, we can measure if a rule in one particular industry could be applied to others and improve the overall effects of insider attack mitigation.

Management aspect (concerned with human factors)	
Banking and finance industry	● Password management including mandatory password protection/password-protected screen savers and change the root password (remote access) when it is necessary ● Explore way to allow employees to report suspicious behavior to one central person or location ● Increases an employee's awareness of the organization's ability to monitor actives and of the possibilities of a persecution or civil lawsuit against the insider
Computer industry	● Pre-hire screening of employees ● Training and education for increasing the awareness of insider attack ● Management attention is needed for employees who experience negative work related events. ● Establish formal grievance procedures and additional forums for employees to voice concerns. ● Document reports of problematic behavior and develop procedures to respond to such report ● Comprehensive password policies ● Comprehensive computer account management policies ● Law enforcement should be notified for investigation assistance ● Cyber-insurance to complete company safety net (expansive)

	● Separation of duties ● Two person control policy
Movie industry	● Sends screeners on video rather than DVD ● Metal detectors and employing security guards equipped with night vision goggles and binoculars at their pre-release screening ● Using messengers to hand-deliver prints of popular movies with phony labels the theaters (which is not very effective) ● Cut down on their use of test-market screenings ● Changing their release strategies to reduce or eliminate time lag between movie openings in difference in different countries ● two person controls policy
Technical aspects (concerned with technical factors)	
Banking and finance industry	● Secure networks from the full range of users ● Using log file: the computer account, IP address, action taken, and the time that action was performed should be logged ● Employee a layered security approach to allow remote access to email and non-critical data but restrict access to critical data and information system only to employees physically located inside the workplace ● Information such as login account, date/time connected and disconnected, and IP address should be logged for all remote logins
Computer industry	● Split key encryption ● An overall increase in monitoring, logging and security countermeasures (may leads to general inconvenience) ● Eliminate the use of reusable passwords ● Logic bomb and other malicious code detection ● Layered security for remote access ● Protect system logs
Movie industry	● Pre-released copies marked with anti-piracy

	messages/watermarks/overt textual marking---identifying the source ● Metal detectors and employing security guards equipped with night vision goggles and binoculars at their pre-release screening ● Combine ranges of technologies and produces into comprehensive solutions

Password management and remote access management are necessary. Nowadays, most organizations have been aware that they must use password as a weapon to protect their crucial data. However, not every organization has full understanding about how to achieve this goal. For example, 27% of the insiders who had system administrator access had been terminated or resigned but their access was not disabling; 33% of the insider who were privileged users had been terminated or had resigned but their access was not disabled[8]. Obviously, companies are put at risk by poor password management and this rule is not only suit for computer system sabotage but it could be also applied on the password management in banking and finance industry.

Access control, especially remote access, is another important issue to all companies. In 87% of the cases, the victim organizations permitted employees remote access and in 56% of the cases the attacks were conducted solely via remote access [8]. In banking and finance sector, although most insiders committed acts while on the job, there is still 30% of the incidents were carried out from insiders' home via remote access [2]. Layered security for remote access should be applied and all computer accounts should be carefully tracked to ensure that all access can be disabled for terminated employees.

By analyzing those methods, it is clearly that the "human factor" has been emphasized more than "technical factor" in all three industry fields. This result indicates that there is a general agreement that besides pure technical upgrade, companies and organizations have learned to look beyond their information technology and security to their overall business processes. Providing formal grievance procedures will help employee to voice their concerns, it will reduce and prevent potential insider attack at the very beginning which is motivated by negative work-related events.

3 Discussion and Conclusion

In this paper I have discuss the insider attack study in three industry fields. By looking at the time sequence of those papers, we can see technical upgrade still plays an important role, but more and more researchers have begun to look at this question in a different angle. Good management and well designed policies are definitely as important as high technology to fight against insider attack.

Every year, many companies suffer from the insider attack. In the banking industry, the loss range from a low of US $168 to over US $691 million; in computer system sabotage sector, the loss ranged from a low of US $500 to a high of US $10 millions [2, 8]. However, when I was doing information searching, I met the difficulty in data collection. When an insider attack happened, not every company reported it to law enforcement, around half of companies said there were not aware that they could report these incidents [4, 5, 6, 7]. A more common reason is, companies are afraid of negative impacts from public and damage of reputation [4, 5, 6]. More available data and cases will help researchers to have a better understanding on insiders attack and companies themselves will benefit from sharing insider attack information.

4 Acknowledgements

My warm thanks go to Clark Thomborson for his guidance and suggestions while I am writing the paper and for his inspiring comments, suggestions and help in making my writing especially the abstract part understandable.

References:

[1] Byers, L. Cranor, D. Korman, P. McDaniel, and E. Cronin, "Analysis of security vulnerabilities in the movie production and distribution process", in
Proc. 2003 ACM Workshop on Digital Rights Management, ACM Press, 1-12, 2003.

[2] D. Cappelli, M. Keeney, E. Kowalski, A. Moore, M. Randazzo,
"Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector", CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University (PA, USA), 25 pp., August 2004.

[3] Ramkumar Chinchani, Anusha Iyer, Hung Q. Ngo, Shambhu Upadhyaya, "Towards A Theory Of Insider Threat Assessment"
Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05) - Volume 00 table of contents
Pages: 108 - 117

[4] Richard Power, "2002 CSI/FBI Computer Crime and Security Survey"
Available at: http://www.reddshell.com/docs/csi_fbi_2002.pdf

[5] Richardson**,** "2003 CSI/FBI Computer Crime and Security Survey"
Available at: http: //www.security.fsu.edu/docs/FBI2003.pdf

[6] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson
"2004 CSI/FBI Computer Crime and Security Survey"
Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[7] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson
"2005 CSI/FBI Computer Crime and Security Survey"
Available at: http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

[8] Michelle Keeney, J.D., Ph.D. Dawn Cappelli Eileen Kowalski, Andrew Moore, Timothy Shimeall, Stephanie Rogers “Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors”
May, 2005
Available at: http://www.cert.org/archive/pdf/insidercross051105.pdf

[9] Peter G. Neumann, "Inside risks: risks of insiders"
December 1999 Communications of the ACM, Volume 42 Issue 12

[10] John Viega, Matt Messier, "Security Is Harder Than You Think"
July 2004, Queue, Volume 2 Issue 5

[11] Herbert H. Thompson, Richard Ford, "The Insider, Naivety, and Hostility: Security Perfect Storm"
June 2004 Queue, Volume 2 Issue 4

[12] Ann Quigley, "Inside Job"
2002 netWorker, Volume 6, Number 1, Pages 20-24

[13] E. McClam, "N.J. man pleads guilty to posting "Hulk" bootleg"
Available at: http://thekinetik.net/forum/showthread.php?t=7740&goto=nextoldest

[14] Gregg Kilday, Paul Bond, “FBI arrests man in Oscar screener case”
Available at:
http://www.hollywoodreporter.com/thr/article_display.jsp?vnu_content_id=2075640