Insider threats assessment in the real-world system

Zhong Xia MA

zma015@ec.auckland.ac.nz

Department of computer science

The University of Auckland

24 October 2006

Abstract

Insider attack is a very serious problem to a system of an organization. The problem can make the system work poorly and cause significant loss to the organization. Insiders like computer viruses, which consume the resources of the computer and make the computer runs worse and worse till the computer crash. The insiders can divulge the business secret to the competitors and cause serious loss to your organization and finally make the organization goes bankrupt. What keeps happening is that most leaders of the organizations have not noticed their systems have such a problem. Maybe it is the time for these leaders to think about doing an insider threat assessment. The insider threat has not been addressed effectively and we still do not have a perfect method to solve the problem. The current methods are more focus on the outsider attacks. Chinchani et al develop a method called *key challenge graph* to solve to insider threat problem. This paper will start a case study in the motion picture industry. The paper will assess the insider threat in the motion picture industry using the *key challenge graph* to see how this method works in the real-world situation.

Section 1 Introduction

[CERT&USSS2004] “From 1997 until his detection in early 2002, a foreign currency trader with an investment bank used a range of tactics, including changing data in various trading system, so it appeared he was one of the bank’s star producers. In actuality, he lost the bank over $600 million.”

This is a typical example of insider threat. An insider, who has the authorized to use the system, does something bad to the system. The formal definition of insider in [Chinchani2005]’s paper is “insiders are in a unique position with the privileges entrusted to them and the knowledge about their computational environment, and this already translates directly to a certain amount of capability”. This means each authorized individual who use the system can be an insider. What will happen if these authorized users do something bad to the system accidentally or purposely? For example, your competitor greases the palm of your employee for some business secret. The above example is a kind of insider threat. An Insider threat is “insiders who maliciously leverage their system privileges, and familiarity and proximity to their computational environment to compromise valuable information or inflict damage”, [Chinchani2005].

[Byers2003] says that “the US motion picture industry estimates that its revenue losses due to unauthorized copying and redistribution of movies via physical media exceeds $3 billion annually” and due to illegal movie download, “the projected revenue loses of up to $ 4 billion annually within the next two years”. So while this paper is written, the revenue loss will be definitely more than $ 4 billion. And [Byers2003] finds that 77% of the sources of these unauthorized copies are leaked from industry insiders. This means $2.31 billion revenue loses of the movie industry in 2003 was cause by insider threats. And the number will be bigger in 2006. By now, it is very clear that how serious the insider threat problem is, and how badly we need a good insider threat assessment method.

The paper will use [Byers2003] as a source to develop a case study. And use the insider threat assessment methodology describe in [Chinchani2005] to exam the insider threats in movie industry that are outlined by [Byers2003].

Paper organization the rest of the paper is organized as follows. In section 2, we will start the case study and explore the insider threats in the motion picture industry. Section 3 will analyses the insider threats using the *key challenge graph* developed by Chinchani et al. Next, we discuss how the *key challenge graph* works in the real-world system. And summarize the paper in section 5.

Section 2 Case study

Identify the insider

How do we define an insider for the movie industry? Is a customer, who uses camcorder to make a digital through-the-air copy, is an insider or is a customer who make a unauthorized copy from rental or purchased DVD ,VHS or from cable, satellite, or broadcast TV is an insider? No, they are not. We only count the people who are invoked in producing or distributing the movie product as insiders although some of them are not employed directly by movie studios (critics, awards judges).

Motivation

The movies come to the public generally in two ways, one way is through the cinema, and the other way is release in DVD and VHS. The movie industry has two markets and two kinds of customer, people who go to the cinema for the movies and people who buy DVD and VHS of the movies. The first kinds of customers, people who go to cinema for a movie, are tracing the freshness and visual and audio effects of the movie. They want to see the movie as soon as possible. During the period that between the finish date of filming a movie and the date of the movie release in cinema, the demand for the unauthorized copy is very high. Because the finical gains will be a lot, the insiders will like to try to make an unauthorized copy of the movie. The second kinds of customers who like to buy DVD and VHS and enjoy the movie at home will make the demand for DVD and VHS version of the movie very high before the official release date of the DVD and VHS version. The insiders will also get finical gains by making these kinds of unauthorized copies.

Classification

Base upon the two markets for the movie industry, we can classify the unauthorized copies of movie into two classes. The first class of the unauthorized should come out before the cinema release and it will be better if content quality of these copies is good. The second class will focus only on the content quality. So we can classify the insider made unauthorized copies described by [Byers2003] in to the following three classes.

Class A: fresh and good content quality

- Unauthorized copying of a movie in the editing room or nearby in the supply chain, whether first cut or final product. These copies often have small difference from the released version or include incomplete audio or visuals. Some of these copies are marked with obtrusive text that identifies their source, or in clued on-screen counter.
- Unauthorized copying of a critic’s advanced copy of a movie. This may have the text “screener copy only, property of some name” appearing on the screen occasionally.
- Unauthorized copying of a promotional or preview screening copy. This may be marked in a similar fashion to critics’ versions.
- Unauthorized copying of an awards judge presentation of a movie. Copies may be marked with the text “for your consideration”.

Class B: perfect content quality

- Unauthorized copying of a consumer medium such as DVD or VHS at the factory or any other point prior to sale. These copies are unmarked and of near perfect quality

Class C: neither fresh nor good content quality

- Digital through-the-air video recording by a projectionist at a cinema with aspect-correct video, suitable exposure, and direct audio. These copies have highly variable video quality, but often can be very good.

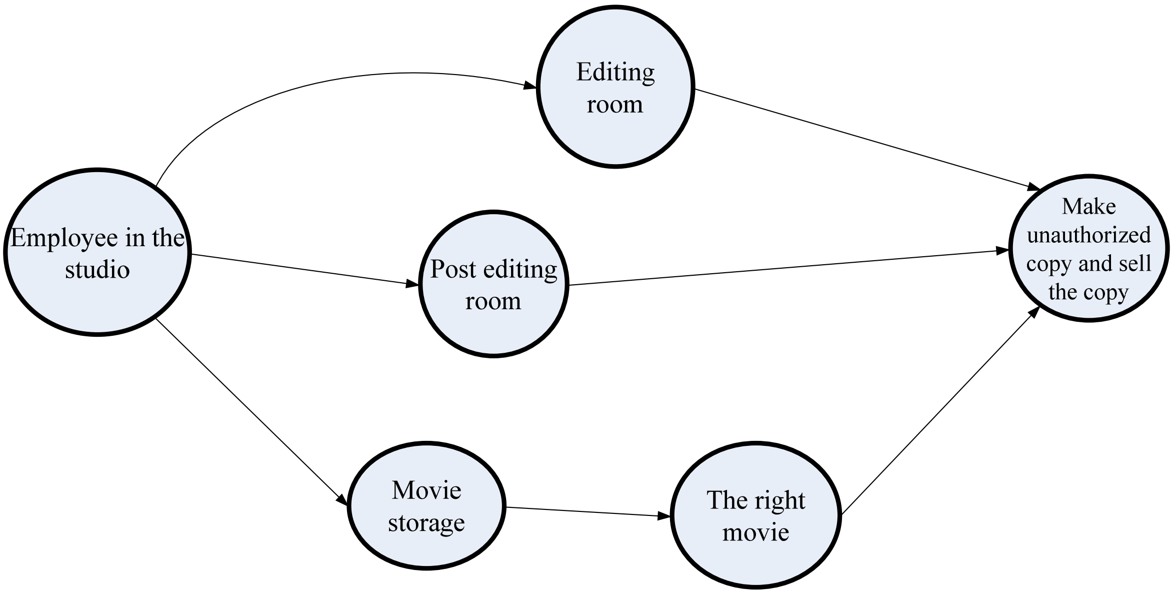
Section 3 Analysis

In this section we will use the *key challenge graph* to analyses the insider threats that cause the unauthorized copies of movie in the previous section.

Section 3.1.1

Make unauthorized copies of a movie in the editing room or nearby the supply chain.

Any employee in the movie industry and have the privilege to use or reach the authorized movie copy could be the insider for this insider threat. For example, the editor of the movie could make an unauthorized copy of the movie and sell it to someone. The figure below is a key challenge graph drawn for this kind of insider threat.

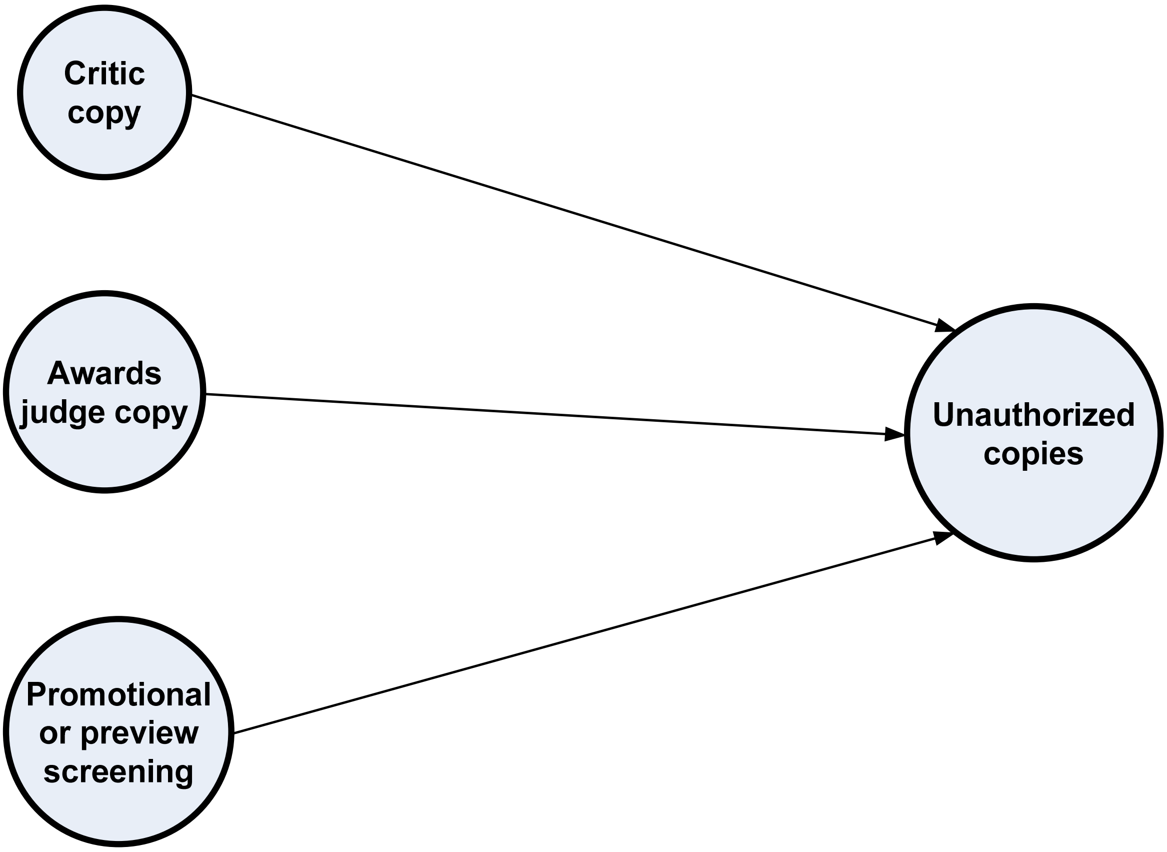


The start point is someone who is an employee in the studio, so he has knowledge about the studio and can access the studio. Base on the privileges the studio grants to the insider, the cost of the insider for the key challenges process will be different. The key challenge for the channels between the start vertex and the editing room, posting editing room and movie storage vertexes are mainly the access control challenge. That is whether you have the access key for the physical doors. If the insider has the privileges to enter these areas, the cost will be very less; otherwise the cost will be a lot. The keys in the editing room vertex and the post editing room vertex will be the original copy of the movie. The original copies of the movie are the keys for the next key challenge processes. If the insider has the keys, the work will become easy and he can make an unauthorized copy of the movie. Otherwise the insider attack fails and the insider has to try some other place to find the original copy of movie, and the cost will increase a lot. The key in the movie storage vertex will be all the original copies of the movies that the studio has made. The insider will have to face another key challenge process, find the movie that he wants. The cost in this key challenge process will be the time that takes an insider to find the movie. And the key for this key challenge process is whether the insider knows how movies in the store are placed. If the movies are not labeled, and the insider does not know where his garget is, he could spend a lot of time to view each movie in the store to find the one he wants. Once he finds the movie, the next step will become very easy, and this attack is successful. The total cost is the cost of each key challenge.

For example, the door of the editing room is locked using a normal lock, the key challenge will be whether the insider has the key for the lock. If the insider has the key, he just uses the key to open the door, and the cost is only a few seconds, if he does not have the key, the cost will be the time it takes the insider to break or crack the lock. After entering the editing room, the attacker can find some information or resources, which is described as the key on a vertex in the key challenge graph. In this example, the information or the resource is the original copy of the movie he wants. The next key challenge is making an unauthorized copy of the movie. If the attacker does find the movie, he can then pass the next key challenge process easily. He can enter the next vertex and get an unauthorized copy of the movie. If the attacker does not find the original copy of the movie, the attacker has to try some other location that may hold the movie and the cost for the attack increase.

Section 3.1.2

Make unauthorized copies from a critic’s advanced copy of a movie, from a promotional or preview screening copy or from an awards judge presentation of a movie. The original copy of the movies are all marked with texts, for example the copies for the awards judges are marked with the text “for your consideration”. The unauthorized copies made from these sources are both fresh and the content quality are nearly perfect. So the insider threats caused by the critics, award judges and promotion or preview people can make the industry a serious loss. These copies will affect both the cinema and the DVD market of the movie.

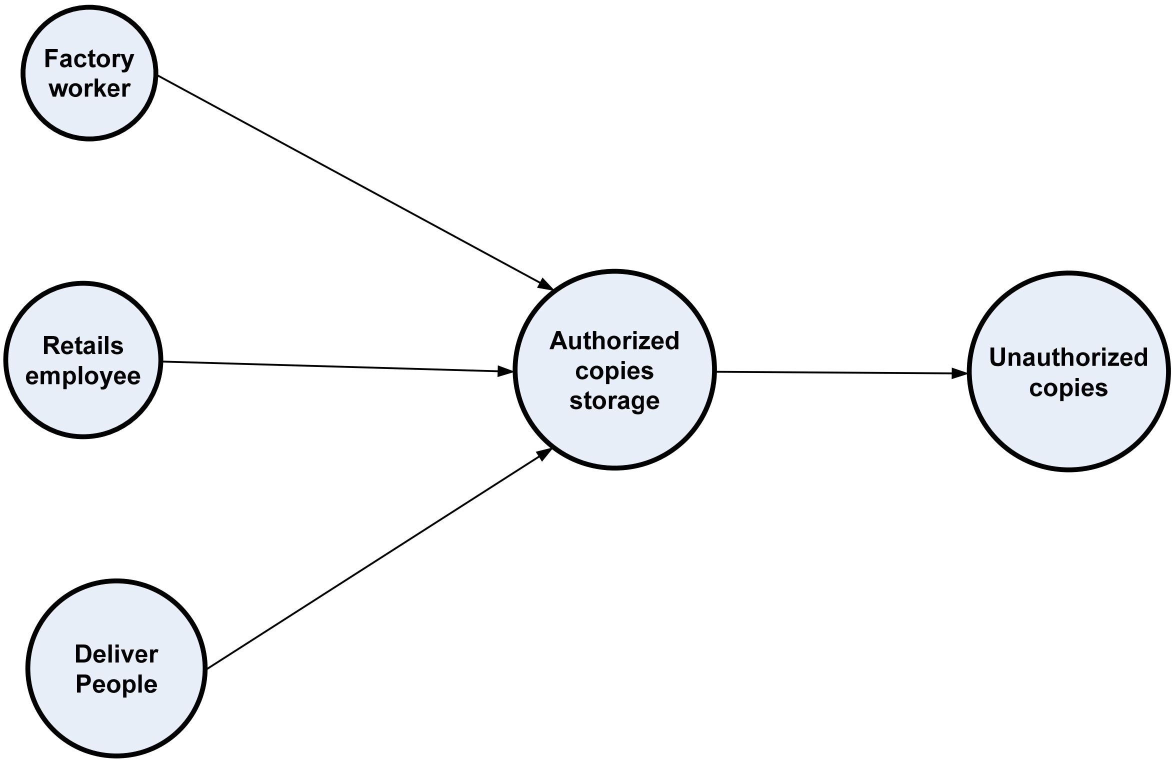


The above figure is a *key challenge graph* for these insider threats. The start vertex is to be in one of the groups. The keys on the vertex are the marked authorized copies of the movie, because the studio and the FBI can track the mark text on the copy to find the insider. The key challenge for them is to eliminate the text mark in the copies. If the texts are removed properly, the probability of being caught is low and the cost is less, otherwise the cost will be thousands of dollars fine or some years in the prison. In [Byers2003], the pre-leased copy of *The Hulk* was posted on the internet. Although the text on the bottom right corner was blocked by Gonzalez, the studio and the FBI still can track the source copy of the unauthorized copy.

Section 3.2.1

Make unauthorized copying of a consumer medium such as DVD or VHS at the factory or any other point prior to sale. These copies are unmarked and of near perfect quality.

This insider threat happens to the distribution process, and anyone who is employed in the related system could be an insider. The DVD or VHS factory will produce the copies of the movies and deliver the copies to the retails for sale.



It will very hard to prevent the insider threats happen at this stage. There are so many people invoked in this stage. The key for the key challenge to get an authorized copy is the privilege the insider has in the system. The key challenge for the people at the start vertexes is to get an authorized copy of the movie. The cost is the probability of being caught. The higher privilege the insider has, the lower the probability they are caught and the lower the cost is. And once the insider success, the key in the authorized copies storage vertex is the authorized copy of the movie, and the cost to make an unauthorized copy of the movie is really low as there is no key challenge for this step.

For example, a worker in the DVD factory starts an insider threat. The insider will have to get an authorized copy from the production line or from the storage of the factory. If the insider is storage administer, the cost for him to get an authorized copy is very low. The cost of this insider threat is low.

Section 3.3.1

“Make a copy of digital through-the-air video recording by a projectionist at a cinema with aspect-correct video, suitable exposure, and direct audio. These copies have highly variable video quality, but often can be very good.” [Byers2003]

This kind of insiders is nearly in the same situation of a critic. The insiders have directly connection with the source. An insider in a cinema faces less risk than a critic. On the other hand, the content quality of the unauthorized copy is not as good as one made from critic copy.

Section 4 Discussion

The *key challenge graph* looks very easy, but when we use it to analyses a real-world system, we can find out that the method becomes harder than we thought. The method is easier to use when it is used to analyses the insider threat caused by insiders exceeding their privilege than analyses the insider threat caused by insiders abusing the privileges.

In section 3.1.1, we use the method to analyses the insider threats in the editing room. This is the kind of insider threats caused by insider exceeds their privilege (you can argue this is a kind of abuse privilege, this depends on who is the insider). We label the vertexes well and keys in each vertex are very clear. We can draw the graph step by step, everything work smoothly.

In section 3.1.2 we analyses the insider threats caused by abuse of the privilege with the key challenge graph. We need to think more about how to label the vertex. The key on the start vertex is nearly the same as the target vertex. It is very easy to mix up the keys on the start vertexes with the target.

The method is not perfect and it has some disadvantages. One of the disadvantages is the definition start vertex and another is the measurement of the cost of the key challenge.

The starting vertex describe in [Chinchani2005] is the location of the insider, but what are the locations for the insider threats caused by critic and awards judges? They can get marked authorized copy of the movie and they can watch the copy anywhere they want. It is really hard to define the starting vertex that way, so we just assume that the starting vertex is the privilege, that is to be a critic or awards judges.

The costs of the key challenge process are also hard to define, the costs for a critic to make an unauthorized copy of movie is not any kind of access control, it is the time that the insider spend on remove the mark text, plus the cost if he is caught.

The logic in the key challenge graph works very well for assessing the insider threats in the motion picture industry. Insiders have to pay a price to move to the next vertex, and the key challenge graphs of each kind of insider threats show the costs. The leaders in the motion picture industry can increase the cost to prevent the insider threats.

The key challenge graph is good, and it can be used to analyses insider threats in a real-world system, work out the costs of insider threats. The security people can enhance the system by increasing the cost for the insider threats. When the finical gain is less than the cost of insider threats, there will be no insider threats in the system. Some of the elements in the key challenge graph need to be extended, so the key challenge can be used to analyses the insider threats in more systems, not only the system in the computational environment.

Section 5 Summary

The paper first does some introduction about the insider threats, and then it describes the insider threats in the motion picture industry. By using the key challenge graph to analyses the insider threats in the motion picture industry, we can exam the practicability and usability of the key challenge graph. We can find out that method is not perfect, but it can solve the insider threats problem.

Reference

CERT & United States Secret Services, *Illicit Cyber Activity in the Banking and Finance Sector*, August 2004, <http://www.ustreas.gov/usss/ntac/its_report_040820.pdf>, (October 2006), Introduction.

S. Byers, L. Cranor, D. Korman, P. McDaniel and E. Cronin, “Analysis of security vulnerabilities in the movie production and distribution process”, *Proceedings 2003 ACM Workshop on Digital Rights Management*, ACM Press, 1-12, 2003.

R. Chinchani, A. Iyer, H. Q. Ngo and S. Upadhyaya, “Towards a theory of insider threat assessment”, *Proceedings of the 2005 International Conference on Dependable Systems and Networks*, IEEE, 2005.