Computer Science 725 Term Paper

Assessment of Keyboard Acoustic Threats by Insiders

Bruce Megget
UPI - bmeg002
ID - 3081213

Abstract:

In the past, companies aimed to protect themselves from viruses and attacks from the outside world. Recently, the balance has shifted and there is a larger threat to companies from insider attack. Companies must now be aware of employees intentionally causing harm. Companies are becoming more aware of this form of attack and are attempting to mitigate it. However, as companies increase their security, insider attacks will become more severe and technical. Keyboard Acoustic Emanations is a technique of 'eavesdropping' on another user to determine what they are typing on their keyboard. This kind of attack allows an attacker to gain sensitive information with less risk involved. Though it is broadly considered that this kind of attack is far from being effective, new studies in this area show that it is becoming a very real possibility. This paper aims to bring to view the possibility of an insider attack using Keyboard Acoustic Emanations.

Introduction

An online magazine [7] states that “Insiders commit about 80 percent of all computer- and Internet-related crime, and these crimes cause an average loss of about [US]$110,000 per corporate victim”. Because of this large risk of attack from insiders, companies are beginning to take necessary steps to protect their assets. A recent paper “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector” [2] discussed various cases where insiders were able to take advantage of certain resources in the company they worked for, for either their gain, or the companies loss. [2]’s main focus was on insider attacks in the finance and business sector, but results found in this sector follow a general trend found in all business sectors. Through analysis of [2] and many other relevant articles, my paper will discuss the possibility of insider attack using keyboard acoustic emanations.

The section, “Definitions” describes various definitions that will be used throughout this paper. The definitions are either created in this paper or referenced from previous definitions.

Firstly, I will discuss the current techniques utilized by insiders when perpetrating these offences. It will also discuss some reasons for these attacks and begin to bring forward the idea that Keyboard Acoustic Emanation attacks could be possible.

Secondly, I will describe two current implementations for launching a Keyboard Acoustic Emanations attack. The first method [1] involves using Neural Networks and needs to be taught specifically by inserting examples into the neural network. The first method does not try and understand what is being typed. For all the algorithm knows, the keys are being entered at random. The second method [5] takes a different approach and makes the assumption that what is typed in the keyboard follows some basic rules. These rules make the system a lot more versatile and accurate. This will be explained in further detail later on. I will also evaluate the performance of the Keyboard Acoustic Emanations attack method.

Finally, I will then discuss the possibilities of Keyboard Acoustic Emanation attacks in the same situations as current insider attack patterns, and reasons that this type of attack can be as effective if not more effective than current insider attack techniques.

In the discussion section I will discuss some possible countermeasures to Keyboard Acoustic Emanations attacks. I will also provide some critical and appreciative comments about the resources that have been used in this paper.

Definitions

Insider:

Defining an insider is a difficult task. There has been no absolute definition given, so in some situations it is difficult to define where the line between an insider and an outsider is. This paper will use the definition of an insider acquired from [3]. They state that "[An insider is] any person who has knowledge of, or access to, valuable nonpublic information about a corporation." For the purposes of this paper, this definition is acceptable.

Insider Attack:

An insider attack can be defined as an attack of a system by an insider with the intention of causing deliberate harm to the said system. For this paper I will use the definition as given by [2]. They state an insider attack as being, "[An attack] by insiders […] who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations."

Victim:

The term "victim" is used in the section describing Keyboard Acoustic Emanations attacks. It refers to the individual that is being attacked by the

keyboard acoustic emanations method (i.e., the person who is typing is being listened to).

Attacking System:

The term “attacking system” is used in the section describing Keyboard Acoustic Emanations attacks also. When used in this paper, it is describing the system that the attacker is using to eavesdrop on what is being typed by the victim.

Keyboard Acoustic Emanations:

Keyboard Acoustic Emanation attacks are presently not a common occurrence in any field, so there is no concrete definition. This paper will use the definition of Keyboard Acoustic Emanations as being “A means of calculating what is being entered in a neighbour’s keyboard by recording the sound emitted by each key press and re-calculating which key has been pressed and recording it on the attacker’s system”. The word neighbour in this definition refers to someone situated within a 15 meter radius of the attacker.

Current Insider Threat Techniques

Previously, companies had to protect themselves from attacks originating from the outside world. However, recent attacks are more commonly originating from within a company. These attacks are caused by insiders seeking either to cause harm to a company, or for financial gain. This shift in scale (from outsider attacks to insider attacks) has come unexpectedly to many companies, causing unexpected (and significant) damage when a successful attack is performed. For example, [2] states that one such company that suffered from an insider attack sustained approximately 3 million dollars worth of damage due to one “disgruntled employee” seeking payback.

From [2], “In 87% of the cases studied, the insiders employed simple, legitimate user commands to carry out the incidents. In only a small number of cases was a more technical knowledge of network security required.” With current standards the way that they are, companies are not properly protected against insider attack, so are vulnerable to these simple kinds of attack. Companies even suffer losses due to poor security training of their employees. This means that the employees don’t even know that they are causing the company to lose money. They have not been taught otherwise by the company. If a company can not even limit accidental losses through security errors, how can it possibly protect itself from a sophisticated technique such as Keyboard Acoustic Emanations?

From results obtained by [2] we can deduce some statistics about insider threat patterns. In [2]’s studied cases of insider attacks only 43% of these cases were committed when the attacker was logged in with their own account. This shows that the majority of attacks occurred while the insider was using another individual’s account to commit the attack. This could be some attempt to protect their identity, or acquire extra authorization by using a “more important” employee’s user login. In order to use another individual’s account, one must gain access to this account. Current techniques for gaining access to another individual’s password include password sniffing or social engineering. These

techniques are effective at obtaining the desired password (with knowledge of how to go about it) but are high risk. Currently companies are one step behind the insider attacks or hacker attacks. Once a company has been attacked, security is modified to counteract that method of attack. However, counteracting one method will not stop further attacks altogether. Attacks will be made using different means. Security analysts believe that predicting possible future attacks is difficult and so preventing them is unachievable. The paper “Towards a theory of Insider threat assessment” [8] however, demonstrates a system that insinuates that it is possible to “reveal possible attack strategies of an insider”.

[8] describes an approach to counteract insider attacks and predict them before a company suffers losses. Their approach uses what they call a key challenge graph. The aim of this threat model (the key challenge graph) is to view insider threats by a large-scale view and not just from analyzing single attacks. Using their model they can also predict attack patterns that involve social engineering. By using a model such as the one described in this paper companies do not have to wait until an attack occurs. They can predict possible scenarios and counter them. This may be the case for a Keyboard Acoustic Emanations attack.

Keyboard Acoustic Emanations techniques

Previous to [1] Keyboard Acoustic Emanations had not been published. The release of this paper has started speculation as to the effectiveness of this type of attack. The more recent paper, [5] (that will be seen in the ACM Conference on Computer and Communications Security in November this year) crushes any speculation as to the real-world application possibilities of this type of attack.

The Keyboard acoustic emanation attack method proposed in [1] involves a lot of training to become an accurate attacking tool. To gain the best results an attacker would need to train their system using the keyboard that the victim would be using during the attack. In some situations it may be difficult to get access to the keyboard of the victim in order to train the attacking system. However, an attacker's system only needs to be trained once for each keyboard, and accuracy will remain high for different victims on the same keyboard. With a trained system, [1] boasts a 79% success rate when re-calculating what was typed by the victim. Figure 1 shows the results of testing. The system was tested with 10 inputs for each of the 30 keys. The results show three numbers. The first is the amount of times the system recognized the key correctly. The second is the amount of times the correct key was the systems second choice, the third number was the amount of times the correct key was the systems third choice. The system implemented in [1] also states that it has an accuracy of 52% when the attacking system is trained on one keyboard and then set to eavesdrop on another keyboard of the same brand and type. This method would make it less difficult to train the system, but the accuracy of the attack would drop.

Keyboard A, ADCS: 1.99						
key pressed	q	w	e	r	t	y
recognized	9,0,0	9,1,0	1,1,1	8,1,0	10,0,0	7,1,0
key pressed	u	i	o	p	a	s
recognized	7,0,2	8,1,0	4,4,1	9,1,0	6,0,0	9,0,0
key pressed	d	f	g	h	j	k
recognized	8,1,0	2,1,1	9,1,0	8,1,0	8,0,0	8,0,0
key pressed	l	;	z	x	c	v
recognized	9,1,0	10,0,0	9,1,0	10,0,0	10,0,0	9,0,1
key pressed	b	n	m	,	.	/
recognized	10,0,0	9,1,0	9,1,0	6,1,0	8,1,0	8,1,0

Figure 1: Sourced from [1]
System is tested with 10 inputs for each of the 30 keys

[5] implements a new system for launching a Keyboard Acoustic Emanations attack based on rules. For example, when a user is typing an English word and they have typed “t-i-g-h”, there will be a much stronger chance that the next letter typed will be a ‘t’ rather than a ‘b’. To train their described system, a ten minute recording of the victim typing on the keyboard is applied as input into the attacking system. Once this has been input and the attacking system is properly configured it can calculate what is being typed in real time by the same victim on the same keyboard. [5] reports a success rate of 90 - 96% for character recognition and 75 – 90% for word based recognition. Some results of testing can be seen below in Figure 2. This shows the rate of recognition vs. the amount of time the system is given to train. [5]’s approach is claimed to be better than [1] because it does not involve the huge training step that is needed. Instead, by recording the victim typing for ten minutes, the system can be trained making training a much less laborious task. [1]’s system based its results on every instance of a key press. It did not try and calculate words written by the victim. However, [5]’s system determines the key being pressed on the victim’s keyboard by applying it to rules as briefly described above. [5]’s algorithm uses standard machine learning and speech recognition techniques to configure the attacking system to attack other systems.

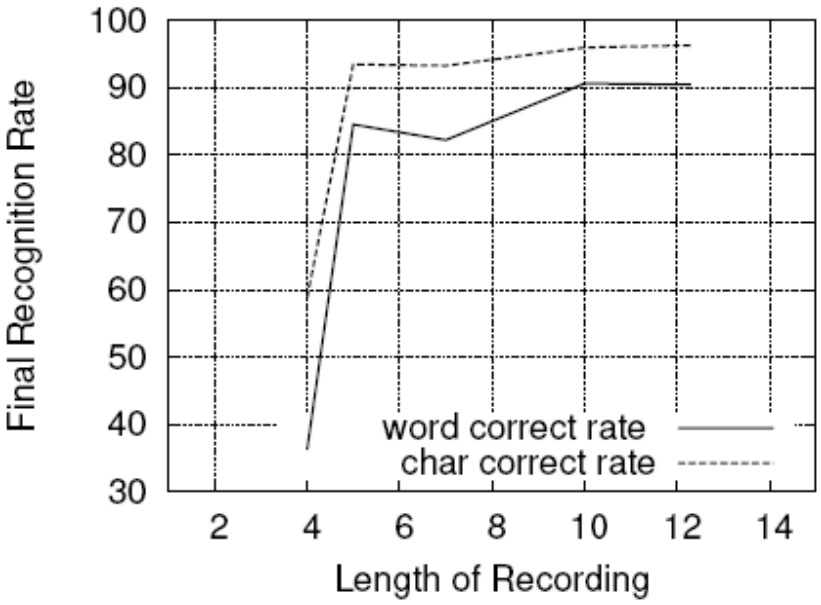

Figure 2: Sourced from [5]
Recognition rates are tested for differing lengths of training time

Keyboard Acoustic Emanations attacks have the advantage over other forms of attack. The attacker does not have to be hardwired, or even connected to a network to be able to attack another individual's system. Using parabolic or shotgun microphones [4], an attacker can be a distance up to approximately 15 meters away from the victim and still receive a relatively clear signal, allowing the attacker to perform a successful attack without needing to be directly in contact with the victim.

Insider threat using Keyboard Acoustic Emanations

The next logical step onwards (as companies learn to protect themselves from current attack schemes) is for attackers to create new innovative ways to attack their system. As shown earlier in this paper majority of the time insiders will not use their own account when performing illegal attacks. If an attacker uses his/her own account, they have a direct line to trace the attack back to them, and run a big risk that they will be tied to the attack.

Using Keyboard Acoustic Emanations attacks on a local computer allows an attacker to gain access to another user's password and login details while keeping separate and anonymous. As described in [5], all that is needed to create an effective Keyboard Acoustic Emanations attack is a laptop or desktop computer with 1G of memory, and a microphone. With approximately 10 minutes of training time and 30 minutes of computational time, the attacking system trained and ready to use.

According to [5] "… 90% of 5-character random passwords using only letters can be generated in fewer than 20 attempts … 80% of 10-character passwords can be generated in fewer than 75 attempts." Good password management is widely known. Examples of it are; use a combination of numbers and letters, don't use birthdates or pets names, change it often, etc. However, individuals are still using bad password practices for usually the simple reason being, they do not want to have to re-remember passwords again and again. Therefore they stick with one password that is easy to remember for a long time. This is typically one that relates to some aspect of their life, or some simple combination of letters and numbers. It is because of this fact that an attack using Keyboard Acoustic Emanations could succeed in determining a user's password.

According to [2], 23% of insider attacks were caused by insiders wanting revenge on the company, 15% were dissatisfied with the company management, culture or policies, and 15% committed the attack because they wanted respect. Financial incentive is a big part of insider attacks within companies, but it is not the only reason. Many times, an insider attack aimed through revenge can be as devastating (if not more so) than an insider attack aimed at receiving a money reward. The example given previously in this paper where the company lost 3 million dollars because of a disgruntled employee shows this. This employee was not seeking any monetary gain. [2] explains that this insider's reason for the attack was to cause deliberate harm because of a dispute over the employee's bonus.

This situation (where money is not the gain) is another perfect area for Keyboard Acoustic Emanations attacks. Confidential data is exchanged on a daily basis between employees of a company by email or through confidentially printed documents. In email,

many companies are utilizing encryption routines such as PGP [6] in their email systems to protect confidentiality from outsiders. Using these encryption techniques, sending an email becomes a chain of events. The user types the email, then encrypts it by whichever encryption they are using. The encrypted email is then sent to the receiver who can then decrypt it to view it. For a hacker trying to intersect an email between the sender and receiver, this is an effective technique, but with Keyboard Acoustic Emanation attacks these encryption techniques are worth nothing. Using Keyboard Acoustic Emanations, insiders can attack the very beginning of the chain mentioned above and learn the information inside the email before it has even been encrypted. Using the system provided in [5], we can get email replication up to 96% accurate. In an email, the remaining 4% of characters recognized incorrectly will be insignificant and the email will still be readable. The same is applicable for confidential documents. These can be recognized while being entered into the computer.

Previously I explained how insider attacks are not always for financial gain. However, a lot of the time this is the reason. 81% of the time in fact (according to [2]). Another possible area where Keyboard Acoustic Emanations could cause extreme harm to a company is attacking their financial assets. It is very common for a company to have a bank account with “loose” funds for petty cash, paying suppliers, etc. To have access to this account, an employee must be very high up on the company hierarchy. Not only will it require another specific password, but will also require the bank account number and/or a login name different to any normal user login. This is done to limit which employees are allowed access to these funds. This extra login will not stop attacks when facing a Keyboard Acoustic Emanations attack. By ‘eavesdropping’, and calculating the login, password and bank account number, the insider can potentially transfer money from the company account to any account in the world.

Because of the nature of Keyboard Acoustic Emanations attacks, tracking an insider using this method would be extremely difficult. They come in no contact with the person they are attacking, so can not be caught easily at this stage. Once they log in using a password they may have learned it might be easier for this individual to be caught. If the

individual's goal, however is only to steal confidential information (as described above) then it becomes extremely difficult to catch the insider in the act.

Discussion

The paper "Insider Threat Study: Illicit Cyber activity in the finance and banking sector" [2] was crucial for the argument of this paper. They took a sample of insider attacks and brought up striking conclusions about the commonalities of these attacks. The paper however does not go into detail in all areas of the paper. For example a broad statement in [2] states "Most of the incidents examined in the banking and finance sector were not technically sophisticated or complex." This does not give any detail about the number of incidents where this was actually the case. From my point of view it seems that this paper was made more for less technical personnel. Their argument is still relevant and significant in demonstrating insider commonalities.

"Keyboard Acoustic Emanations" [1] had definite flaws in their system, which they pointed out in their paper. For example, when training the system on one keyboard and then testing the results on another keyboard, the system was only 52% accurate when looking at the four top nodes output from the Neural Network. For password sniffing, this is incredibly inaccurate. [5] tackles the same problem found in [1] but by a different approach, achieving much more convincing results. For example, after listening to the victim type in English for ten minutes, the system can now analyze and calculate what is being typed in real time to a very high standard. Though some results from [1] were less than convincing, some results did enforce the topic of the paper, that Keyboard acoustic emanations was a plausible method of gaining information from another individual's computer. Some good results were achieved from their testing as shown in Figure 1 in a previous section. The results from both these papers prove that an attack by Keyboard Acoustic Emanations is not just a far away worry for future generations, but the threat is knocking on our doorstep. To effectively combat this form of attack by insiders, companies need to focus on countermeasures to nullify this attack method.

[1] lists some possible countermeasures that could be taken to reduce the likeliness of being attacked by this method. Let me first explain that in [1] they only believe that they know what causes a keyboard key press to be unique. They deduced that this assumption could be true but did not rule out all other possibilities entirely. This means that their suggested countermeasures may not be effective at stopping a Keyboard Acoustic Emanations attack.

Countermeasures that are suggested include keyboards that don't have a base plate in them (so the keys won't make a sound). However, in many companies, employees take their work home with them on their laptops and work on both their laptop and work computer during the work day. A possible countermeasure not discussed in either [1, 5] that I suggest is interfering with the attacking microphones to distort the signal that the attacking computer is receiving, giving them inaccurate results. However, this could affect work progress with employees in the company by distractions such as background noise. Another method would be to create artificial keyboard clicks that are played by the computers sound card when a key is pressed. This would confuse the attacking system as all keys would sound the same, meaning each key would be indistinguishable. Without doing appropriate investigations, we can not resolve whether either of these methods would be appropriate in a work environment.

Before this paper, the idea of insider attacks using Keyboard Acoustic Emanations had not been conceived. Throughout the body of this paper I have aimed to emphasize how Keyboard Acoustic Emanation attacks could be used by an insider to gain restricted access or cause intentional harm with less possibility of being caught than previous insider techniques. The discussed results of [1] and [5] have confirmed that this kind of attack is a serious security threat, demonstrating the need for companies to be wary of this attack by monitoring the physical domain. Unlike many current insider attack dilemmas, Keyboard Acoustic Emanation attacks are based in the real world and not through the network. Because of this, companies need to adopt appropriate countermeasures to monitor or nullify this assault.

References

[1] Asonov, D., Agrawal, R. "Keyboard Acoustic Emanations" *Symposium on Security and Privacy*. IEEE,
February 2004.

[2] Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., Moore, A., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector"
August 2004

[3] Investopedia.com – Your Source for Investing Education
http://investopedia.com/

[4] The Spy Store.com - Microphones
http://www.thespystore.com/microphones.htm

[5] Zhuang, L., Zhou, F., Tygar, J. "Keyboard Acoustic Emanations Revisited" *To appear in Proceedings of the 12th ACM Conference on Computer and Communications Security*
November 2005

[6] PGP Corporation – Home Page
http://www.pgp.com/

[7] Strategies & Issues: Thwarting Insider Attacks
http://www.itarchitect.com/article/NMG20020826S0011

[8] Chinchani, R., Iyer, A., Ngo, H.Q., Upadhyaya, S., **"**Towards a Theory of Insider Threat Assessment" *Dependable Systems and Networks*
June 2005