Case Study : Develop a Policy To Protect Information On Laptops Against Attacks

Braden Simpson

January 20, 2013

1 INTRODUCTION

The ABC corporation is a multinational corporation with more than 30,000 employees in over 50 countries. ABC maintains tens of thousands of laptops and information loss from the these laptops is a serious problem to ABC corp. The Chief Information Officer of ABC has to develop a policy to protect against information loss on the laptops. Information loss is a problem for ABC corp, "... recent security report shows that over three hundred laptops were lost or stolen last fiscal year and ten information leakage incidents were related to the lost or stolen laptops".

From the case study, "... One of the incidents disclosed personal information of about 50,000 customers. These days, the average cost to deal with illegally disclosed information is about $90-$300 per record. Information Security Policy and International Standards This incident alone could potentially damage the corporation financially by about $7.5 million. The damage to the corporation's reputation can be enormous and irreparable."

ABC corp has issued Windows laptops, loaded with Microsoft Bitlocker, which protects the hard drive by encrypting all of the data on the hard disk with an encryption scheme. This is useful for stopping data from stolen laptops from being recovered and potentially lost or used for illegal purposes. However BitLocker still does have some issues, specifically, it isn't able to protect against cold boot attacks.[1].

[1] Attacks that are used by stealing the contents of RAM, containing the encryption key, then gaining access to the encrypted hard disk. http://en.wikipedia.org/wiki/Cold_boot_attack

2 Problem Analysis

The main issue in the case study is that the data on laptops might be important, and may contain confidential information, when stolen, the laptops can be broken into via the Cold Boot Attack method stated in Section 1, and have their encrypted contents decrypted and exposed.
In order to mitigate this issue, the Chief Information Officer at ABC has to explore potential policies, standards and training that could be implemented to ensure that data on the company laptops is not compromised.

2.1 Scale

ABC corporation is a very large company with over 30,000 employees, and over 50,000 customers. With a company of such scale, security policies are paramount, the problems that face enterprise security become much more difficult to address, and the training and policies require much more rigorous execution.

2.2 Interviews

The case study includes interviews with some of the people in the organization that have some input into the policies being created. These *stakeholders* are described in detail in section7. The following are a few excepts from the interviews that have an effect on the policy.

The System Adminstration and Operations Department really was opposed to a boot password because of the impact it has on the accessibility of a laptop when in critical situations. From the interview "For example, a court clerk cannot wait for a series of system updates when the court is about to begin within five minutes. The business impact of boot passwords is bigger than what you may imagine. We would like to avoid applying boot passwordâĂę"

The Information Security Department delcared that the probability of the attack succeeding is very small at the current time, but attacks become more likely as time goes on, and preparing for the future would be a smart idea.

3 Purpose

The purpose of the policy is to design a method of fullfilling the following :

1. To protect against cold boot attacks
2. Ensuring the employees know the risk of carrying important information
3. Preventing the theft of laptops

The policy will mitigate the risks of having important or confidential information on laptops that could potentially become compromised.

4 Threats and Vulnerabilities

The primary threat described in the video clip was that the attacker could try to get the contents of the laptops DRAM unencrypted before the memory is cleared. The fact that the memory is storing the encryption key of the hard drive is the largest vulnerability explored in the Princeton video clip and as long as the DRAM contains the encryption key, there will be a risk of the attackers obtaining it and using it for decrypting the hard disk.

The risk as defined by ISO 13335 as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization", is very very high in this case. As stated in Section 1 the business impact of a successful attack like this would be catastrophic and "unrecoverable", this makes the risk very high, especially because simply putting Microsoft BitLocker on a computer does not protect at all against the cold boot attack.

5 Policy and Technical Security Controls

There are both policy controls, controls that will be in place for employees to learn and adhere to, and security controls, controls which will be put in place to automatically mitigate some of the threats and vulnerabilities that exist.

Policy Controls

1. Avoiding laptop theft - Emphasize the importance of keeping the laptop in a safe place
2. Cable locks - Ensure that when leaving the laptop, it is locked to a secure location. Note that this doesn't fully protect against cold boot attacks, because the attacker may steal the contents of the ram on the victims computer. It does still help against some attackers.
3. Sensitive Data - Ensure that the employees know the risks of having sensitive data on their laptops. Educate them to delete the data as soon as it's no longer needed, and to only take the data that they need.

Technical Controls

1. Higher DRAM refresh rates - Upgrade the DRAM to require a higher refresh rate. This means that it will make the laptop harder to attack due to the reduced timeframe for the attacker.
2. BIOS password - This was noted as not a suitable option from the Systems administrator in Section 2.2, but it would protect against the attacks.

3. Encryption key FOB - This is a very viable method, and is used in many systems worldwide (Luxury cars[2], Google Authenticator[3] etc)

4. Physically block ports - This method would actually physically disable the external USB ports and CD-ROM drive, as well as any other methods of booting externally.

5. Disallow external boot devices from BIOS - This method is a software method to block external boot systems. Essentially disabling the attackers ability to boot, similar to blocking the ports physically.

6. Physically Seal DRAM - Weld or modify the laptops so that the RAM could not be removed. This combined with another technical control such as technical control 4 or 5 would be a whole solution.

6 IMPACT

Policy Controls

1. Avoiding Laptop Theft - This will produce very little negative impact, a simple internal advertising campaign, and some training sessions would help. It also is not a complete solution, but would likely reduce the number of stolen laptops, reducing the risk.

2. Cable Locks - Low impact, low cost. Would reduce the number of stolen laptops, and would require simple advertising and reminders to the employees.

3. Sensitive Data - This would require training, and reminders, as well as discipline on the part of the employees. Reducing the time that sensitive data sits on the hard disks of employees laptops reduces the risk of a catastrophic leak.

Technical Controls

1. Higher DRAM refresh rates - This would make the attacks harder perform, but not impossible. Also this would require a hardware upgrade on all laptops, which would be costly and time-expensive.

2. BIOS password - This requires an update to each computer, and even after the update is performed, in order for each employee to start their computer, there is extra time spent entering a bios password. This was noted as a problem in Section 2.2, and would negatively impact the employee productivity, even though it would be a solution to the cold boot attacks.

3. Encryption key FOB - There would have to be a FOB handed to each employee, which is expensive, however it would add another layer of security against cold boot attacks. In order for the attacks to succeed, the attacker would have to steal both items, FOB and laptop, which would be separated.

[2] Rolling codes http://www.burningimage.net/rke/
[3] Google authenticator http://support.google.com/a/bin/answer.py?hl=en&answer=1037451

4. Physically Blocked Ports - This requires IT to modify all the laptops, and it means that the employees can longer use the ports. This will stop the attacker from using other boot media to extract the information off the DRAM, blocking most cold boot attacks. Only making the cold boot attack viable if the RAM could be physically taken out of the laptop and put into an attackers laptop before the memory fades.

5. Disallow external boot devices from BIOS - This would require IT to apply the settings to the BIOS for each of the employees laptops, but would require no extra work once it is applied. It has a low impact and would protect against cold boot attacks, unless the RAM is physically taken out of the laptop.

6. Physically seal DRAM - This requires a physical modification to the laptops and would be expensive to perform, but it means that the attackers cannot physically take the DRAM out of the laptop and attack it from their own machines.

7 STAKEHOLDERS

The stakeholders in this policy are

1. Security Sponsor

   - Helps influence the security policies

   - Takes ultimate responsibility when security policy flaws are detected, or breaches are made

2. Security Team

   - Actually writes the policies

   - Educates all the teams on how to implement the policies

3. IT department

   - Dictates how fast the implementation of technical controls is done.

   - Responsible for the robustness of the technical controls listed in Section 5

4. Every Employee of ABC

   - They use the laptops after the controls are put in place, and they implement the policy.

   - Responsible for following all rules and regulations dictated by the policy.

5. Attackers

   - The attackers choose which types of attacks to use, and how to perform these attacks. This influences how the security team needs to respond, as security is usually done in response to attacks.

8 COMPLIANCE METRICS

The compliance metrics for a policy require that the effectiveness of a policy can be tested at times to ensure that the security measures are implemented correctly. In order to do this, the company must have regular methods for reporting discrepancies in the system (BIOS passwords disabled when they should be enabled, people unblocking their USB ports, etc).

As well there should be regular checks for policy controls, for example checks for unlocked laptops, laptops unattended, encryption key FOBS attached to the laptop, people leaving sensitive data on the laptops unnecessarily, etc. The IT department may be able to do routine checks on the laptops after they implemented the technical controls to check if they are still secure. Regular sessions to reinforce the security policies are recommended, to ensure all employees comply with the policy.