University of Victoria, Software Engineering

ABC Security Policy Case Study

Jordan Ell
V00660306

January 12, 2013

1 Information Security Policy Research

This document will outline background research and analysis performed in order to develop a policy to protect information on laptops against cold boot attacks with stolen laptops. This document will: analyze the issue (i), define the purpose (ii), identify and analyze risks (iii), search for policy and technical controls (iv), analyze impacts of controls (v), identify stakeholders (vi), and define compliance metrics (vii). The final policy developed from these findings can be found attached to this initial document.

1.1 Analyze The Issue

The prominent issue at hand is two fold. First off, the physical issue of laptops being stolen is a concern. While hard drive (HD) encryption prevents some forms of data loss, it in no way addresses the initial issue of laptops being stolen or misplaced by employees. The second issue is the HD encryption does not protect against cold boot attacks which are becoming a serious concern as these attacks are relatively cheap and quick to perform. Also, depending on how the company deals with the encryption keys, a single key being discovered may lead to further data loss on other systems.With these two issues, ABC faces great financial loss potential in both virtual data and physical property, both of which are damaging to the company's reputation and potential customers.

1.2 Define The Purpose

The purpose of this policy development task is to mitigate the loses outlined in the previous section. Trying to prevent laptop theft as well as HD encryption key discovery which may be a result of theft or carelessness. Both of these preventions are used to stop physical cost as well as potential data loss leading to large scale damage for financially and reputability of ABC.

1.3 Identify and Analyze Risk, Threats, and Vulnerabilities

The chief vulnerability of the cold boot attack is the access to a powered or recently powered laptop's DRAM. If the DRAM is accessible and is powered or recently powered, the HD encryption key and information inside of it can be stolen. There are multiple threats to this vulnerability both from stolen or unattended laptops. An external device may be plugged into the laptop such as an external HD or USB thumb drive which can be used for gaining access to the DRAM information. These type of threats can be done relatively quickly, so even an unattended laptop is a threat to this vulnerability. Laptop theft is another threat as with a stolen machine, the DRAM can physical be removed and cooled in order to allow the hacker more time and freedom when it comes to obtaining information from the device. The risk being run with these attacks are both physical cost to ABC with laptop replacements as well as potential data loss which could lead to enormous damage costs. These risks also scale with potential higher ranked employees as they may have access to higher levels of confidential information about the company or customers.

1.4 Identify and Analyze Risk, Threats, and Vulnerabilities

The chief vulnerability of the cold boot attack is the access to a powered or recently powered laptop's DRAM. If the DRAM is accessible and is powered or recently powered, the HD encryption key and information inside of it can be stolen. There are multiple threats to this vulnerability both from stolen or unattended laptops. An external device may be plugged into the laptop such as an external HD or USB thumb drive which can be used for gaining access to the DRAM information. These type of threats can be done relatively quickly, so even an unattended laptop is a threat to this vulnerability. Laptop theft is another threat as with a stolen machine, the DRAM can physical be removed and cooled in order to allow the hacker more time and freedom when it comes to obtaining information from the device. The risk being run with these attacks are both physical cost to ABC with laptop replacements as well as potential data loss which could lead to enormous damage costs. These risks also scale with potential higher ranked employees as they may have access to higher levels of confidential information about the company or customers.

1.5 Policy and Technical Controls

1. BIOS Password - Even though the system administration department does not agree, a BIOS password will ensure that the boot order of a laptop cannot be changed which would prevent the laptop from being powered on to an external HD.

2. High refresh DRAM - Ensuring that only high refresh DRAM is purchased and installed in laptops helps defeat the reboot style cold boot attack as the RAM will be cleared quicker upon power removal.

3. BitLocker DRAM Flush - If possible, ensure that BitLocker flushes the DRAM on laptop shutdown, this ensures the encryption key is removed from the DRAM and cannot be stolen on a quick reboot.

4. Laptop lock - Laptops must be tethered to an immovable object when being left unattended. This prevents laptop theft which can lead to data loss.

5. Laptop storage - Laptops must be in a locked cabinet or other closed storage device while being left unattended for short to medium periods of time. This prevents theft as well as external devices being attached for quick data theft of the DRAM.

6. Sensitive Data - Keep sensitive data off of personal laptops and only stored on authorized network storage. This keeps stolen encryption keys from being able to access local sensitive data.

7. Mandatory shutdown - If a laptop is not to be used for an extended period of time (end of the work day), it must be powered off. Being powered off prevents encryption keys from being in DRAM for very long.

8. Block ports - Physically block USB and other ports which would otherwise enable harmful devices to be attached to the laptop. This would stop attackers from running malicious hardware / software in an external fashion.

1.6 Analyze Impact of Controls

Out of the 4 technical controls listed above (1,2,3,6), BIOS password has the most inconvenience for the end user. As explained in the interview it would interrupt the current path management software as an employee must enter a password to allow patching as opposed to automation. High refresh DRAM and BitLocker flush would be hidden from the user but may cost slightly more money. Network storage for sensitive data may cause laptops users slight inconvenience as additional steps may have to be taken to access company data, as well as may lead to additional costs of server data farms and their security measures.

Out of the 4 policy controls listed above (4,5,7,8), mandatory shutdowns are potentially the most harmful. Depending on current boot times of the devices, having to power on a

laptop more than once a day can be a serious issue which may lead to less productivity of employees. Blocking physical ports can also be damaging depending on how currently move data from one device to the other. (The possibility of losing USB storage devices.) Laptop locks and storage should not damage the user's experience at all and should more or less just be considered responsible use of the laptops.

1.7 Identify Stakeholders

A stakeholder of this policy is anyone who can be affected positively or negatively by the new policy. Because of this, every employee at ABC who uses a laptop is labelled as a stakeholder of this new information security policy. Aside from laptop users, the IT department is also a large stakeholder as they will likely be in charge of ensuring technical controls are up to date and being administered properly. HR will likely play a large role in training and possibly enforcing policy controls company wide. The high level employees of ABC will be seen a large stakeholders as security is a business plan and must have "buy-in" from top level employees in order to be successful.

1.8 Define Compliance Metrics

In order to enforce the new information security policy, both the technical and policy controls must be in compliance with potential random spot checks as well as initial training and setup. The IT department can be tasked with ensuring both new and old laptops are installed or updated with new technical controls. These technical controls can also be enforced by conducting possible random checks of department laptops across ABC. A set of standard checks could be devised by which current laptops are tested. For policy controls, individual departments can enforced regulation by simply spotting non compliant procedures that happen from time to time by its workers. (Laptops being left unattended or not being properly secured with locks.) This ensures that departments and employees are self regulated which may cause greater awareness of security policy. The IT or HR departments may also wish to have meetings with other departments to go over new security policy or have refresher sessions.