Tufts University

COMP116 – Introduction to Computer Security

Recovery After Losing the Physical Device

Dec. 11th 2014

Author: Haoyang Mao Mentor: Ming Chow

Abstract

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards" says Prof. Gene Spafford. As the technology brings much joy to many people's lives, it also exposes ordinary citizens to a very dangerous yet not been emphasized threat: the cyber security. Although recently more and more algorithms and defenses have been developed to improve security in various aspects, recovery after losing physical devices has been largely ignored by the security communities. Many experts in security generally accept the idea that when a user lost its physical device, any security effort is useless. Due to this belief, very few people ever considered to enhance lost device security. However, is it really the game over moment for users when they lost their devices? I do not agree. In this paper, I will focus on the analyzing this problem by first explain what is the current conventional ways of recovery a lost device. Then I will discuss the importance of such recovery and my thoughts to the security community. Next, I will talk about my idea on this issue as well as some promising designs that would potentially tighten the security on this particular area. Lastly, I will make a closing conclusion.

1. Introduction

"Physical security is often overlooked and its importance underestimated in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware," said Margaret Rouse. Indeed, losing physical device is the most common security issue that an ordinary user would experience yet little attention has been distributed to it. According to Consumer Reports, 3.1 million American consumers were victims of smartphone theft. Unfortunately, large scale of loss of devices does not raise enough attention to improve the recovery mechanism. A survey conducted by Lockout Inc. stated "1 in 10 U.S. smartphone owners are victims of phone theft and 68 percent of victims were unable to recover their device after the theft occurred." All above statistics prove that the security community has not put enough efforts into security of lost devices.

1.1. Current Recovery Mechanisms

Recovery Mechanisms after losses of devices has two major forms: recovery applications that are built upon the application level and built in authentication mechanisms that are at the operating system level. Both forms of protection provide some extend of security to a lost device.

Currently, most recovery applications provide similar services. For example, *Find My iPhone* is a mobile application that protects and traces user's iOS devices. It provides services to physically locate the device and remotely wipe all the data in users' devices. Another mobile application *Prey* provides extra features such as recording devices' location when batteries are

running low and utilizing the devices' camera to capture images of the suspect thief when being in the lost mode.

Built in authentications across different computer systems have generally the same form but with various password complexity rules. For Windows XP operating system, an administration password is a string that must have minimum length of six characters and must not contain all part of the username. For Android users, mobile phone authentication is a user-defined sequence of connecting different dots.

1.2. Why Is Device-losing Recovery Necessary

Information stored in computer devices are highly valuable nowadays as online banking and e-commerce coming to people's lives. Data stored locally can sometimes be very sensitive information like the credit card number and medical records. Many insecure applications that store users identification information in plain text motivate the bad guys to steal even more. No one wants uninvited guests to be able to access his or her important data even if the device was stolen or lost. If users are not able to recover or wipe data on their lost devices, they might have to suffer more than just buying new ones.

1.3. Problem With Current Recovery

There are problems with existing recovery mechanisms in both application and operating system level. Both have serious setbacks, and both can be easily compromised with minor technical knowledge.

The biggest problem with recovery in the application level is that all security tools require Internet or cellular connections to be able to perform their services. *Find My iPhone* would not work at all if the iOS device is disconnected from the Internet. Attacker can take huge advantage of this connectivity requirement. By simply turning off the Wi-Fi and cellular services, an attacker is able to effectively compromise all existing security tools in the application level with no need for any further knowledge of the device.

At the operating system level, there are indeed many layers of defenses against external access. For instance, in most Linux distributions, there is a uniform set of discretionary access control (DAC) that sets up permission restrictions. However, most the authentication protections in the OS level are designed under the assumption that no attacker will ever have the physical access to the device. Therefore, they provide only very elementary security when attackers do get their hands on devices. Attacker can easily gain root access or administration privilege to a computer by entering the GRUB or service mood, prohibiting the system to enter default run-level and disabling any authentication protections with commands like "passwd". Also, with the help of directory traversal software like *iExplore*, attackers can bypass many authentication processes and access the file system of the device directly.

Another critical setback in current recovery tools in both OS and application level is that they both require some user efforts to set them up first before they can provide security services. Take a smartphone user as an example. This user would have to download the tracking application into his or her phone first and then register for an account to use the recovery service on the smartphone. This small but mandatory effort leads to a low rate of setting up protection. Even worse, entering a username and password can be seen as a troublesome process in many users' perspectives. In an article from the NBC, a survey "found that 34 percent of all

smartphone owners do absolutely nothing, not even a simple code to lock the screen." This high rate of no authentication protection or tracking application further endangers users when they lost their devices.

2. To the Community

Security community has been dealt with all kinds of attacks from the birth of technology. From fighting against the early MacMag virus to trying to stop modern DDOS attack, the community has focused its energy on defending from distant attacks. While it is important to keep investing time in mechanism to fight those attacks, the community has neglected the fact that a majority of people lost their data and sensitive information through losing their physical devices. In my opinion, it is not an excuse to not improve this particular area of security because of the false belief that losing physical device means no security at all. There are plenty improvements we can make to recover data and prevent sensitive information being stolen from users' lost devices

3. Defenses

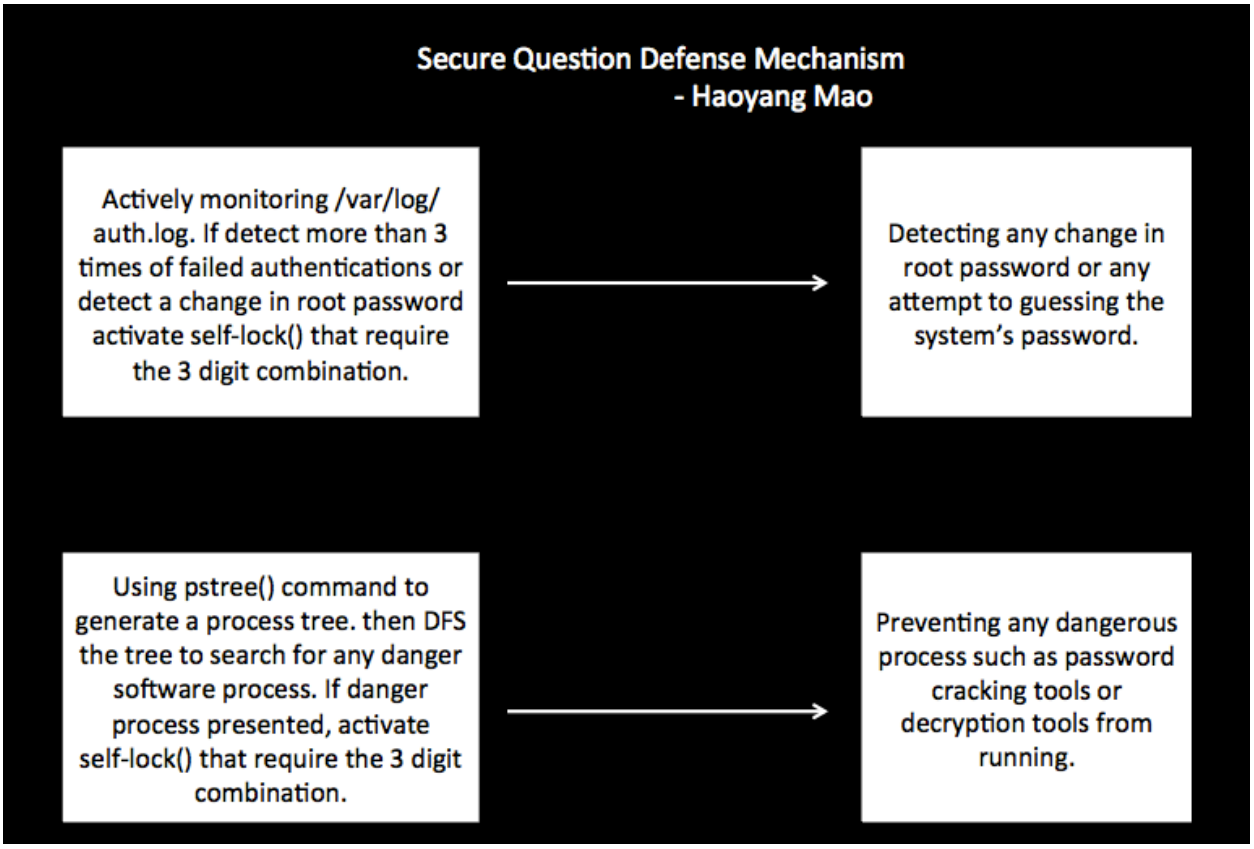
It is no question that extra protections are needed to lost devices. Some examples of this kind of protection are locking the device in the hardware level and automatically wiping the device when authentication is bypassed. Because of low levity and uncertainness of the devices when being stolen, protection should be emphasized on both software and hardware. In the following sections, I will first discuss my idea in a new software defense mechanism and then talk about other hardware security methods that are in the developing process. Lastly I will talk about some of the drawbacks in these defenses.

3.1. Software Defenses

There are a lot measures that can be made to secure a lost device in the software level. A research that I have done showed that security question mechanism could be a very trust-worthy option. The security questions mechanism serves as an extra password that protects the system's password. It is semantically very simple and works in three stages. Firstly, when the device was booting up for the first time, security questions are required to be answered by the user.

```
void squestion(int secure_question[]) {

    /* all three answers are stored as int */

    /* question 1 */
    printf("Q1: Please enter the last digit of your birth year\n");
    scanf("%d", &secure_question[0]);

    /* question 2 */
    printf("Q2: Please enter 1 if you are a male, 0 if you are a female\n");
    scanf("%d", &secure_question[1]);

    /* question 3 */
    printf("Q3: Please enter the first digit of your mother's birth year\n");
    scanf("%d", &secure_question[2]);

    setupdone = 1;
}
```

These questions are very easy to answer, which require very little effort from the user side. The answers of these questions then form a three digits combination that would be stored encrypted in a file called init_config. Correctly inputting these three digits would be required to access init_config file in any way. Secondly, if the system detects situations including entering many time the wrong password, changing the root password or running potential dangerous software, it then activates self-lock() that requires whoever is in control of the device to enter the three digits combination.



Thirdly, if the wrong three digits combination were entered many times, the system would then erase the hard drive completely. Although not a perfect solution, the security questions would provide an extra layer of defense independent of the system's passwords.

3.2. Hardware Defenses

Hardware defenses have a few charming advantages over software protections. Because of the low levity, any sort of hardware protection would be automatically resistant to most attacks in the application level. Here are several new hardware designs that would increase the security of the device significantly.

Self-destruct hardware is an emerging technology that provides solid defenses for the data on lost devices. Developed by a British company called Secure Drive, Autothysis series hard drives are the first SSDs that would physically destruct all its data if it receives a special

SMS message or if it is physically removed from the original motherboard. In addition, the hard drive consists a built-in GSM access unit. If it cannot receive any GSM signal for a reasonable long period, it would delete all its content as well. By deleting, this secure piece of hardware not only erases all the bits but also physically breaks its NAND chips, electronic controller as well as other parts of the SSD to ensure that data recovery conducted by the attacker is not possible.

Hardware encryption is also a brilliant idea that has been put forward recently. Instead of encrypting data using software that depends heavily on CPU performance and system memory capability, hardware encryption are totally transparent to the operating system. This low level of encryption lowers the risk of data being decrypted, because the encryption process happens inside the hard drive, which immunes the drive from many kinds of attacks used to compromise software encryption. Various companies have been developing encryption hardware. A leader in this industry is Toshiba, who recently introduced a family of hard drives that would automatically self-encrypt its content using a strong AES-256 encryption. In addition, the hard drive would keep track of its owner's system configuration as well. When connected to an unknown host, the hard drive would prevent any data access.

In the hardware design level, examples of security thinking has proven to be extremely effective when it comes to protecting lost devices. A great example is the new generation of iPhone 5s and iPhone 6 developed by Apple. One of the essential steps of disassembling an iPhone is to separate the screen and the main logical board, which are connected by a group of special wires. This kind of wires are made of a unique synthetic rubber that would break apart easily when applying force to them. This intentionally easy-to-break design increases the chances that unauthorized person who is not familiar with the design would tear the wires and thus secure the data inside. While this design is mainly to prevent unauthorized person from

disassembling iPhones, I believe it illustrates how hardware design can serve as a kind of device self-defense.

3.3. Drawbacks

Unfortunately, the proposed defenses above are not perfect. Security questions are great protection to the system. Nevertheless, when the attacker power off the machine, software protections collapse. Although the self-destruct and self-encrypted hard drive will protect the information in any circumstances, such hardware is surprisingly expansive. Only a very limited group of people is willing to afford such prices. The rest users would still suffer critical losses of information in the event of losing physical devices. In addition, secure hardware design has not been seen in many devices. Instead, modern design choices are often made based on company's profitability instead of users' information security

4. Conclusion

Protecting the physical device is very important. All of user's data will be exposed if there is no way to recover after losing the device itself. The security community has not put enough effort in this side of the problem. We should devote more energy to create better mechanisms that protects the informational safety. In addition, as the informed ones, we have the responsibility to raise the general citizens security awareness.

References

1. *3.1 Million Smart Phones Were Stolen In 2013, Nearly Double the Year Before,* http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html

2. *Phone Theft In America*, https://www.lookout.com/resources/reports/phone-theft-in-america

3. *Windows XP Password Complexity Requirement*, https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/504.mspx?mfr=true

4. *Most Americans don't secure their smartphones*, http://www.cnbc.com/id/101611330#

5. *These solid state hard drives will self-destruct if you text them*, http://www.theverge.com/2014/10/1/6877217/autothysis-solid-state-hard-drives-will-self-destruct-if-you-text-them

6. *Toshiba to launch self-erasing hard drives*, http://www.cnet.com/news/toshiba-to-launch-self-erasing-hard-drives/

7. *How to Hack Your Own Linux System*, http://www.tecmint.com/how-to-hack-your-own-linux-system/

8. *Security Hard Drives*, http://storage.toshiba.com/storagesolutions/trends-technology/security-hard-drives

9. *Physical Security*, http://searchsecurity.techtarget.com/definition/physical-security