Laptop Theft: A Case Study on the Effectiveness of Security Mechanisms in Open Organizations

Trajce Dimkov, Wolter Pieters, Pieter Hartel
Distributed and Embedded Security Group
University of Twente, The Netherlands
{trajce.dimkov, wolter.pieters, pieter.hartel}@utwente.nl

ABSTRACT

Organizations rely on physical, technical and procedural mechanisms to protect their IT systems. Of all IT systems, laptops are the probably the most troublesome to protect, since they are easy to remove and conceal. When the thief has physical possession of the laptop, it is difficult to protect the data inside. Organizations open to the public, such as hospitals and universities, are easy targets for laptop thieves, since every day many people wander in the premises.

In this study, we look at the effectiveness of the security mechanisms against laptop theft in two universities. We analyze the logs from laptop thefts in both universities and complement the results with penetration tests. The results from the study show that surveillance cameras and access control have a limited role in the security of the organization and that the level of security awareness of the employees plays the greatest role in stopping a theft.

Categories and Subject Descriptors: H.1.2 [User /Machine System]: Human factors

General Terms: Experimentation, human factors.

Keywords: laptop theft, case study, penetration tests, physical security, security awareness, social engineering.

1. INTRODUCTION

Of all IT systems, laptops are particularly hard to protect. Laptops are mobile, easily concealable, there is a big market to sell the hardware and there can be many of them in a single building. With the increased data storage capabilities of laptops, the loss of even a single laptop can induce dramatical costs to the organization [1]. Thus, although there can be a large number of laptops in an organization, losing even a single laptop may not be acceptable.

Organizations open to the public are particularly at risk from laptop theft. Hospitals and universities, for example, accept hundreds of people that can wander in the premises every day. Marshall et al. [2] stress that 46% of data breaches occur in institutions open to the public: education, health care and the government. Laptops containing sensitive medical or academic data become highly vulnerable in these environments.

The problem security professionals face is how to protect the laptops in such open organizations. There are three types of security mechanisms to secure laptops in a buildings: technical, physical and procedural mechanisms. Technical mechanisms such as laptop tracking and remote data deletion protect the laptop and the data in the laptop by using software. Physical mechanisms, such as doors and cameras, physically isolate the thief from the laptop and/or identify her in case of a theft. Procedural mechanisms such as organizational policies and rules decrease the number of mistakes by employees and increase the resilience of employees toward social engineering. The usage of technical mechanisms to protect laptops is elaborately researched by the computer science community [3, 4]. However, many of these mechanisms fail when the adversary has physical possession over the laptop [5, 6]. Interestingly, the role of physical and procedural mechanisms in protecting laptops is still not explored by the computer science community.

The main contribution of this paper is the evaluation of existing physical and procedural security mechanisms for protecting laptops based on (1) logs of laptop thefts which occurred in a period of two years in two universities in Netherlands, and (2) 14 penetration tests in the same universities, where the goal was to gain possession of a marked laptop from an employee unaware of the penetration test. To perform the physical penetration tests using social engineering, we devised a methodology which address the ethical and social implications of the tests.

In section 2 we evaluate the logs of the laptop thefts and describe the penetration tests. Section 3 summarizes our observations and section 4 concludes the paper.

2. METHODOLOGY

We use two approaches to look at the security mechanisms in use and their effectiveness. First, we look at logs of recent laptop thefts in two universities in Netherlands. From the logs we obtain information about the last control that failed before the laptop theft and alarms raised by the theft. However, the logs provide limited information about the level of security awareness of the employees. The logs do not provide any information on the possible violation of procedural security mechanisms, such as letting strangers inside an office and sharing credentials between employees. Even in case of a burglary, the logs do not provide any information how the thief reached the office.

Therefore, as a second step, we orchestrated 14 penetra-

This research is supported by the Sentinels program of the Technology Foundation STW, applied science division of NWO and the technology programme of the Ministry of Economic Affairs under project number TIT.7628.

CCS'10, October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

tion tests where we used social engineering to steal a laptop. Through the tests, we observed the security awareness of the employees as well as the effectiveness of the physical security mechanisms in both universities.

2.1 Log analysis

In a period of two years, the universities suffered from 59 laptop thefts. The logs from the thefts provide (1) the location where the laptop was stolen, (2) protection mechanisms on the laptop, and (3) how the theft was discovered.

In 46% of the thefts, the laptop was stolen when the employee left it unattended in a public location, such as a cafeteria or meeting room. In 19% of the cases, the theft occurred when the employee left the office without locking the door. In 30% of the thefts, the thief broke into a locked office either by forcing the door or breaking a window.

The majority of the thefts (93%) were reported by the laptop owner. In a few cases the report came from an employee who observed a broken door or window (5%). Only one of the thefts triggered an alarm.

2.2 The penetration tests

Before performing the tests we received permission for the penetration tests from the chief security officers in both universities. Only the chief security officers were aware of the tests. The tests were approved by the legal department of the universities.

To perform the penetration tests, we enlisted 45 master students in computer security who took the role of penetration testers. The students were divided in teams of three. The goal of each team was to steal a clearly marked laptop from an employee who was unaware of the penetration test. First, we did a pilot study with only three teams and three laptops. Based on the results and insights of the pilot study, we performed an additional 11 penetration tests the next year. The methodology used for performing the tests and the design decisions of the tests are thoroughly described in [7].

2.2.1 Setup of the environment

1. *Coordinator* - person orchestrating the penetration tests.
2. *Penetration tester* - person attempting to steal the asset.
3. *Contact person* - person who distributes the assets to the custodians.
4. *Custodian* - person at whose office the laptop is placed.
5. *Employee* - person with none of the roles above.

At the start of the study we used snowball sampling [8] to recruit a group of contact persons and custodians. We chose four acquaintances as contact persons, who in turn searched for other acquaintances willing to take part in the study as custodians. The custodians resided in two different universities in nine different buildings.

The contact persons asked the custodians to sign an informed consent form, and then distributed the 14 marked laptops, each with a web-camera and a Kensington lock. To steal any of the laptops, the penetration testers needed to circumvent three layers of access control: the entrance of the building, the entrance of the office where the custodian works and the Kensington lock.

The contact people provided the custodian a cover story stating that the study is focusing on the usability of the laptops where the level of satisfaction would be measured using motion detection web-cameras.

2.2.2 Execution of the penetration tests

After setting up the environment, we gave each of the penetration teams the location of a single laptop they should obtain. First, each team scouted their location and collected as much information as possible about the custodian and the security mechanisms at the location. Then, each team proposed a list of attack scenarios they wanted to conduct. After getting approval for executing the scenarios by the coordinator, the teams started testing.

The actions of the teams were logged using the web-cameras we positioned in the offices of the custodians and through recording devices carried by the teams during the attacks. We used such comprehensive recordings (1) to have a better overview of why the attacks succeeded/failed and (2) to be sure the employees were treated with respect by the penetration testers. The students were asked to try avoiding the CCTV cameras, to reflect the behavior of a real thief.

After each attempt, the teams provided an attack trace listing which mechanisms they circumvented and, in case of failed attempts, which mechanism caused the attack to fail. Figure 1 provides a summary of the successful approaches of teams and the disguises they used to obtain the laptop.

2.2.3 Closure

After all penetration tests were over, we debriefed the custodians and the contact people through a group presentation, where we explained the penetration test and its goal. All participants were thanked and rewarded for helping in the assessment of the security in their university.

2.2.4 Results

Surprisingly, *all* teams were eventually successful in stealing their laptop. Besides the 14 successful thefts, there were an additional 11 unsuccessful attempts.

The favorite approach of the teams was to confront the custodian directly and ask for the laptop. Nine of the teams took roles as service desk employees, students that urgently needed a laptop for a few hours or claimed that they were sent by the coordinator. Four teams used mobile phones or pocket video cameras to record the conversation with the employees.

Approach	Disguise	
Social engineered the custodian	as assistants	5
	as help desk	2
	as students	2
Social engineered the janitor	as students	4
Social engineered the cleaning lady	as PhD student	1

Figure 1: Approaches of the penetration testers

The resistance of the employees against social engineering varied. In six cases, the custodians gave the laptop easily after being shown a fake email and being promised they would get the laptop back in a few hours. In two cases the custodian wanted a confirmation from the coordinator. However, in five cases the students were not able to social engineer the custodian directly and were forced to look for alternative approaches. For example, in one of the cases the students entered the building before working hours. At this time a cleaning lady cleaned the offices, and under the

Figure 2: In five tests the teams social engineered an employee. In two of these cases the testers used a bolt cutter to cut the Kensington lock, and in three found the keys from the lock in the office.

assumption it was their office let the students inside. After entering the office, the students cut the Kensington lock and left the building before the custodian arrived.

3. OBSERVATIONS

We observed three main security mechanisms in the universities: surveillance cameras, access control and a level of security awareness of the employees.

Surveillance cameras. Security officers do not use cameras as alarming mechanisms, but use recorded footages a posteriori, to identify an offender after an accident took place.

Even when used to identify the thief a posteriori, the cameras provide limited information about the thief. In none of the logs nor during any of the penetration tests the cameras provided enough information to reveal the identity of the thief. The CCTV system is providing limited help because (1) the cameras are not mounted in offices, (2) the thief can easily conceal the laptop and (3) thieves usually know the position of the cameras and obscure their face.

Access control. We spotted two weaknesses of the access control. Locks are usually bypassed because (1) they are disabled during working hours and (2) the doors and windows where the locks reside are easy to force.

Similarly to recordings from surveillance cameras, logs from the access control systems provide limited help in identifying the thief. The logs show whose credential was used to enter a restricted area at a specific time period. Since the credentials are easy to steal or social engineer and because there are many people entering and leaving the area where the theft occurs, it is hard to deduce the thief.

Security awareness of the employees. The level of security awareness of the employees plays a crucial role in success or failure of a theft. The human element is the main reason behind the success or failure of the laptop thefts. In 69% of the laptop thefts and 100% of the penetration tests, the theft occurred either because the employee left the laptop unattended in a public location or did not lock the door when leaving the office. Similarly, during the penetration tests, employees opened door from offices of their colleagues, shared credentials or handed in laptops without any identification. Therefore, even with strong access control in place, if the security awareness of the employees is low, the access control can easily be circumvented.

On the other hand, the human element is the main reason behind the failure of 67% of the penetration tests. In these cases, an employee informed the security guards for suspicious activities, rejected to open a door for the tester, rejected to unlock a laptop without permission or interrupted the tester during the theft. In these cases, the employees besides enforcing the access control mechanisms, also played a role as an additional surveillance layer around the laptop.

4. CONCLUSION

In this paper we evaluated the security mechanisms that influence laptop theft in organizations open to the public. We analyzed the logs of laptop thefts which occurred in a period of two years in two universities in Netherlands. We complemented the findings from these logs with 14 penetration tests, in which we used social engineering to gain possession of marked laptops. We observe that:

1. Access control mechanisms and CCTV are used to deter opportunistic thieves, but provide limited help against a determined thief.
2. The logs from the CCTV and the access control provide little useful information for identifying the thief.
3. Even if access control mechanisms are implemented, overall security will still strongly depend on security awareness of employees.

This is an exploratory study to explore the effect of physical security and procedural mechanisms in protection of laptops. In the future, we plan to repeat the penetration tests with a larger sample group and span them over a longer period of time. Such setup will provide statistically significant quantitative analysis of the results.

References

[1] L. Ponemon. Cost of a lost laptop. Ponemon Institute, 2009. communities.intel.com/docs/DOC-3076.

[2] M. Marshall, M. Martindale, R. Leaning, and D. Das. *Data Loss Barometer*. KPMG, UK, 2008. www.datalossbarometer.com.

[3] Wayne A. Jansen, Serban I. Gavrila, and Vlad Korolev. Proximity-based authentication for mobile devices. In *Security and Management*, pages 398–404, 2005.

[4] T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno. Privacy-preserving location tracking of lost or stolen devices: cryptographic techniques and replacing trusted third parties with dhts. In *SS'08*, pages 275–290, Berkeley, CA, USA, 2008. USENIX Association.

[5] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, and E.W. Felten. Lest we remember: Cold boot attacks on encryption keys. *USENIX Security*, pages 45–60, 2008.

[6] E.M. Chan, J.C. Carlyle, F.M. David, R. Farivar, and R.H. Campbell. Bootjacker: compromising computers using forced restarts. In *CCS'08*, pages 555–564, NY, USA, 2008. ACM.

[7] T. Dimkov, W. Pieters, and P. Hartel. Two methodologies for physical penetration testing using social engineering. Technical report, CTIT, December 2009.

[8] B.L.A. Goodman. Snowball sampling. *The Annals of Mathematical Statistics*, 32(1):148–170, 1961.