Laptop theft: a case study on 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 physical assets. Of all physical assets, laptops are the probably the most troublesome to protect, since laptops are easy to remove and conceal. Organizations open to the public, such as hospitals and universities, are easy targets for laptop thieves, since every day hundreds of people not employed by the organization wander in the premises. The problem security professionals face is how to protect the laptops in such open organizations.**

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 biggest role in stopping theft. The results of this study are intended to aid security professionals in the prioritization of security mechanisms.

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

I. Introduction

Of all physical assets, laptops are particularly hard to protect. Laptops are mobile, easily concealable, there is a big market to sell the hardware and there can be hundreds 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: physical, technical and procedural mechanisms. Physical mechanisms, such as doors and cameras, physically isolate the thief from the laptop and/or identify her in case of an incident. Technical mechanisms such as laptop tracking and remote data deletion protect the laptop and the data in the laptop by using software. 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 contribution of this paper is evaluation of the existing 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. We look at all successful and unsuccessful laptop thefts and provide a guideline of which mechanisms should be considered first in implementing security mechanisms.

The outline of the rest of the paper is as follows. In section 2 we introduce related work. In section 3 we evaluate the logs of the laptop thefts and in section 4 we describe the penetration tests and the results from the tests. Section 5 summarizes our conclusions and suggests a guideline for which mechanisms should be considered first in adding security mechanisms. Section 6 concludes the paper.

II. Related Work

Protection against laptop theft is researched by the computer science and the crime science community.

In the computer science community, the accent is on protecting the data residing in the laptop and finding the location of the stolen laptop. Several security products, such as TrueCrypt[1] and BitLocker[2] provide encryption for the whole hard drive. A few manufactures even produce self-encrypting hard drives where the encryption key never leaves the drive [3, 4]. These approaches suffer from two problems. First, when the thief has physical possession of the laptop, she can always successfully

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.

[1] www.truecrypt.org
[2] blogs.technet.com/bitlocker

	Locked office (burglary)	Open office	Restricted location	Public location	No details	Total
Stolen laptops	18	11	2	27	1	59
Cut Kensington locks	1	5	0	1	0	7
Other physical damage	16	0	0	0	0	16

Figure 1. Information from the logs. The logs from both universities are merged to anonymize the data.

execute a number of attacks [5, 6, 7]. Second, these approaches seem to ignore the human element, or more precisely, induce performance overhead and decrease the usability of the laptop. A recent study by Panemon [8] shows that the majority of non-IT individuals, even when provided with an encrypted laptop, turn off the encryption software.

A number of tracking applications, such as Adeona [9] and LoJack [10], can track the location of the laptop they are installed on. In case of theft, these solutions use Internet to provide the owner with the current location of the laptop. These solutions suffer from two problems: (1) if the goal of the theft is obtaining data from the laptop, the thief might never connect the laptop to Internet and (2) the thief may remove the application by flashing the BIOS and/or formating the hard drive, making the tracking impossible.

The approach from the crime science community is more general, and considers the laptop *and* its environment. The goal in this field is to prevent a thief from stealing the laptop in the first place, by either changing the environment surrounding the laptop or by creating situations that will deter a thief [11]. Kitteringham [12] provides a a list of 117 strategies how to prevent a laptop theft. The strategies include implementation of physical, technical and procedural mechanisms. The list is quite elaborate, although the effectiveness of these mechanisms of each of them is unclear.

Willison and Sipnonen [13] use 25 techniques [11] on how the environment can reduce the risk of theft and link them with attack scripts. These results are used to understand how a specific class of attacks could have been stopped. Similarly, we also link these techniques with attack scripts, but we look at which mechanisms were in place and which failed to protect the laptops.

There are few reports which analyze laptop theft. These reports focus on the money loss from a stolen laptop [1] and the frequency of laptop theft and the most affected sectors [2]. Our results are complementary, and look at the effectiveness of conventional security mechanisms in stopping laptop theft.

III. Methodology

We used two approaches to look at the security mechanisms in use and their effectiveness.

First, we looked at logs of the laptop thefts in two universities in Netherlands. From the logs we got information about: the main reason for the laptop theft, alarms raised by the theft and the role of technical and physical mechanisms in securing the laptop and finding the thief, such as access control and surveillance cameras.

However, the logs provide limited information about the level of security awareness of the employees. In particular, the logs do not provide any information of possible violation of the procedural security mechanisms, such as letting strangers inside an office and sharing credentials between employees.

Therefore, as a second step, we orchestrated 14 penetration tests where we used social engineering to steal a laptop.

A. Log analysis

In a period of two years, the universities reported 59 laptop thefts (Figure 1 and 2). A sample log is shown in Appendix A. The logs from the thefts provide (1) the location from where the laptop was stolen, (2) protection mechanisms on the laptop, and (3) how the theft was discovered.

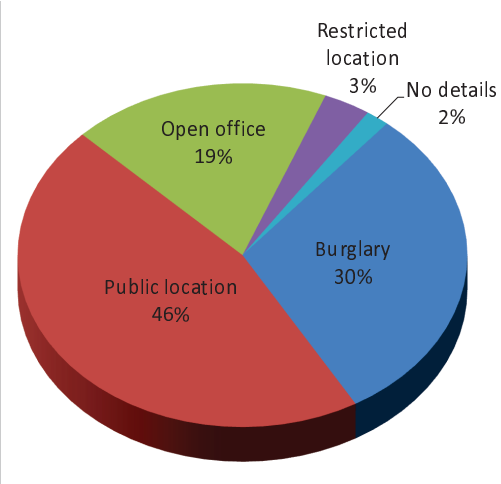

Figure 2. In majority of the cases, the theft occurred because the employee either left the laptop in a public location or forgot to lock the office door.

1) Location of the theft: 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 for a short period of time without locking the door.

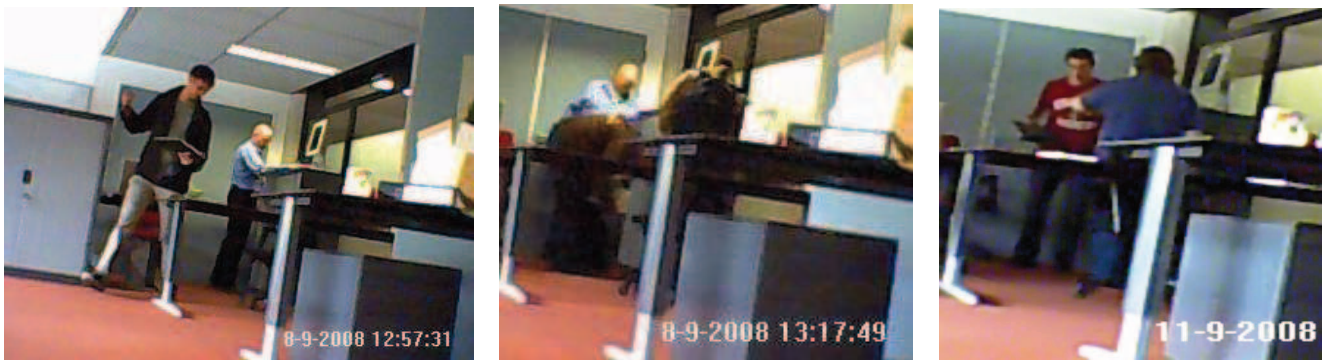

Figure 3. During three of the laptop thefts the students produced a fake e-mail giving them permission to take a laptop and went to the janitor. When the third team approached the janitor, he just gave them the keys and let the students go alone in the office.

In 30% of the thefts, the thief broke into a locked office either by forcing the door or breaking a window. In two of these burglaries there is no evidence of used force, and the guards assumed the thief used a master key or other credential to gain access. These two cases are targeted thefts, since the thief stole only a laptop and nothing else.

2) Protection mechanisms on the laptop: From the logs we could not deduce if any software protected the laptop.

In five of the thefts that occurred in an unlocked office, the laptop was locked with Kensington lock. Only one of the laptops stolen in a public location was locked with a Kensington lock.

3) Theft discovery: 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. In this case, the thief grabbed the laptop while the employee went to collect print outs and left through the fire door, triggering the fire alarm.

In all buildings, in both universities, there are surveillance cameras (CCTV) and either partially or fully centralized access control systems able to log access requests. Surprisingly, the systems provided no useful information in any of the thefts. These mechanisms are further analyzed in section IV.

The information we obtained from the logs is limited. The logs provide information obtained after the theft took place, based on evidence found by the police and the security guards. The logs do not provide information on how the thief reached the location nor on whether the security awareness of the employees contributed to the theft. To check the effectiveness of the procedural mechanisms, we performed a set of penetration tests where we used social engineering as a means to obtain a laptop.

B. The penetration tests

To perform the penetration tests, we got help from 45 master students in computer security which took the role of penetration testers. Before performing the tests we informed and got permission from the chief security officers in both universities. We informed the officers exactly which locations we were going to test and the names of the staff and students involved. No other security person in the universities knew of the tests. The tests were approved by the legal department from the university.

The students were divided in teams of three. The goal of each team was to steal a clearly marked laptop from an employee who is 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 [14].

The rest of the section (1) defines the roles in a penetration test, describes the (2) setup, (3) execution and (4) the closure phase in the test, and discusses (5) the results and (6) the limitations of the tests.

1) Roles in the penetration test: We define five roles in the penetration tests.

1 *Coordinator* - an employee responsible for the experiment and the behavior of the penetration tester. The coordinator orchestrates the penetration tests.
2 *Penetration tester* - a student who attempts to gain possession of the asset without being caught.
3 *Contact person* - an employee who volunteers to distribute the asset to the custodians.
4 *Custodian* - an employee at whose office the laptop is placed.
5 *Employee* - person in the university who has none of the roles above.

2) Setup of the environment: At the start of the study, we chose four volunteers as contact persons, who in turn found custodians who volunteered to take part in the study. The selection of contact persons and custodians was pseudo-random. The common attribute among these participants was that the contact persons were

Figure 4. In nine of the tests the custodians willingly gave the laptop, either believing that the teams were from the help desk or that they were sent by the coordinator.

acquaintances to the authors, and the custodians were acquaintances to the contact persons.

After selecting the contact people and the custodians, we bought and marked the laptops that need to be stolen. The contact persons asked the custodians to sign an informed consent, and then distributed the clearly marked laptops, each with a web-camera and a Kensington lock. The custodians resided in two different universities in nine different buildings. 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 told the custodians the universities are doing a usability study on the new laptops, and thus they needed to measure the satisfaction level of the custodians. They informed the custodians that the level of satisfaction would be measured using motion detection web-cameras that would record the usage of the laptops. The data collected by the cameras was stored on a PC inside their office. Furthermore, for security reasons, the contact people instructed the custodians to lock the laptops with a Kensington lock and to leave the cameras recording at all times. bg The contact people also asked the custodians not to leave any private nor work related data on the laptops. With these measures, we tried to reduce the risk of data leakage and loss of productivity caused by any theft.

In a few cases a custodian asked a contact person what is precisely measured with the cameras. The answer was that the moment the contact person tells the custodian which behavior is measured, the custodian might change his behavior and invalidate the study.

3) Execution of the penetration tests: After setting up the environment, we gave to each of the penetration teams the location of a single laptop they should obtain. The penetration tests lasted for two weeks. In the first week, 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. A sample attack scenario is presented in Figure 6. During the second week of the test, after getting approval for executing the scenarios by the coordinator, the teams started testing.

1. Social engineer night pass from an employee.
2. Enter the building early in the morning.
3. Social engineer the cleaning lady to access the office.
4. Cut any protection on the laptop using a bolt cutter.
5. Leave the building during office hours.

Figure 6. Example of an attack scenario

The actions of the teams were logged using the CCTV system, 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 excessive 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.

After each successful or failed attempt, the teams provided an attack trace of which mechanisms they circumvented and, in case of failed attempts, which mechanism caused the attack to fail.

4) 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 custodians and contact people were thanked and rewarded for helping in the assessment of the security in their university.

5) Results: Eventually, *all* teams were 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 directly confront the custodian 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 they were sent by the coordinator. Four teams used mobile phones or pocket video cameras to record the conversation with the employees. In one case they took a professional camera and a cameraman, and told the custodian the recording is part of a study to measure the service quality of the service desk.

Approach	Disguise	
Social engineered the custodian	as coordinator helpers	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 7. From 9 of the teams that social engineered the custodian, 5 as a people sent by the coordinator, 2 of the teams took a role as help desk employees and 2 as students. 4 teams approached the janitor as students that needed to pick up a laptop, with a fake email as a proof, and 1 team took a role as a PhD student who forgot the key to his office

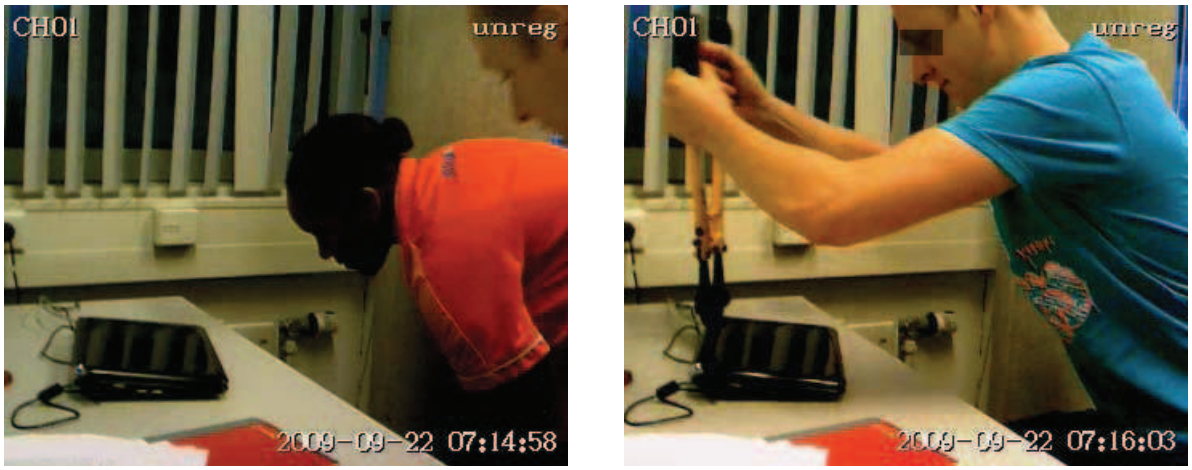

Figure 5. In five tests the teams social engineered a person other than the custodian. In two of these cases the students used a bolt cutter to cut the Kensington lock, and in three found the keys from the lock in the office.

The resistance of the employees 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. The teams succeeded in the attempt because the custodian called a number provided by the penetration testers. Needless to say, the number was of another team member pretending to be the coordinator. In one case a colleague of the custodian got suspicious and sent an email to campus security. Since only the chief security officer knew about the penetration test, in a few hours the security guards all over the campus were all alerted and started searching for suspicious students.

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 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. On the way out, they even asked the same cleaning lady to lock again the office door.

6) Limitations of the test: During the analysis of the recordings from the tests, we observed that a few custodians were easily persuaded to hand in the marked laptop. The reason might be that employees are less reluctant to give in a temporary laptop than their own laptop.

Another limitation of the test might be the high self-confidence of the testers. The security guards were not aware of the penetration test. If caught, the identification process would be unpleasant experience for the testers. Nevertheless, they knew they will not go to jail for their actions. A thief might rather wait for the laptop to be left unattended than approaching an employee directly and asking for their laptop.

The results of the test are based on only two universities and their security mechanisms. Other institutions might have different specter of mechanisms for protecting their laptops.

IV. Observations

The observations presented in this section focus on the effectiveness of security mechanisms in two open institutions to protect laptops. The observations should probably apply also to any mobile asset, such as medical equipment, beamers and mobile phones.

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

A. Surveillance cameras

Security officers do not use cameras as alarming mechanisms, but use them a posteriori, to identify an offender after an accident has taken place. The security officers cannot afford to monitor all surveillance cameras. The cameras work only when a motion is detected, and automatically store the recording in a back end server. The delay between the occurrence and report of the theft gives the thief sufficient time to leave the building.

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 cameras are not able to identify the thief because (1) they 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.

The cameras are not mounted in offices. All penetration tests and 49% of the thefts took place in an office. Cameras are not mounted in offices to preserve the privacy of the employees and because mounting cameras in every office is not cost effective. Without surveillance

in these offices, it is impossible to identify a thief during the act.

Instead of in offices, the cameras are usually mounted on entrance doors. Many people pass through the entrances with bags, and each of the bags might conceal the stolen laptop. Even if there are only two persons observed by the camera, if the persons are not caught on the spot and challenged by the security guards, the evidence from the surveillance camera can not be used against them.

Cameras positioned to monitor public locations, such as cafeterias, halls and reception desks can record the thief during the theft. The logs show that 46% of the laptop thefts happened in public locations. During the penetration tests we noticed that these cameras are usually set on motion detection, and are not actively monitored by the security guards. A careful thief would obscure her face from the cameras using a hat, a hood or just covering her face with her hands before she steals the laptop. In one of the penetration tests, three penetration testers wandered with newspapers on top of their faces through the building without being challenged by anybody.

In conclusion, the surveillance system provides no help in stopping the theft and has limited usage in identifying the thief a posteriori.

B. Access control

The security logs and from the penetration tests show that although there are multiple layers of access control in both universities, it is still possible to steal a laptop.

We spotted two weaknesses on the access control in the universities. 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.

The access controls on the entrances of the building are easily bypassed because they are disabled during working hours and because there are too many people with credentials that can open the door. From the 14 penetration teams, 13 bypassed the entrance locks by attacking during working hours and one team social engineered credentials from an employee to enter the building out of working hours.

Another attack vector for stealing a laptop is to force a door or a window. The penetration teams were not allowed to damage any property of the universities except cutting the Kensington locks. However, the logs from actual laptop thefts show that in 30% of the thefts, the thief broke a door or a window to get access to the office.

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 very hard to deduce which person is the thief.

In conclusion, the typical access control mechanisms deployed in the universities are mainly used to deter opportunistic thieves, but provide no help against a determined thief.

C. 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 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 all failed 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 from the custodian 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.

Employees are usually considered as the weakest link in the security of an organization [15]. We observe that employees can also be the strongest link in the security of open organization. A proper security education of employees increases the employee's resistance to social engineering, and increases effectiveness of the other security mechanisms.

V. Conclusion

In this paper 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 which we conducted in the same universities.

Based on the logs and the penetration tests, we conclude that physical security mechanisms provide deterrent rather than protective security role in laptop theft in open organizations. Security awareness of the employees is the main element which determines if a theft will be successful or not and influences the effectiveness of the other security mechanisms.

In the future we plan to repeat the penetration tests. This time, to make the penetration tests more realistic, we plan to randomly select of contact persons and custodians and give the laptops to the custodians few months before the start of the tests.

References

[1] L. Ponemon. Cost of a lost laptop. Technical report, Ponemon Institute, April 2009.

[2] M. Marshall, M. Martindale, R. Leaning, and D. Das. *Data Loss Barometer*. September 2008.

[3] Seagate Technology. Can your computer keep a secret? 2007.

[4] Seagate Technology. Drivetrust technology:a technical overview. 2007.

[5] P. Kleissner. Stoned bootkit. In *Black Hat USA*, 2009.

[6] Ellick M. Chan, Jeffrey C. Carlyle, Francis M. David, Reza Farivar, and Roy H. Campbell. Bootjacker: compromising computers using forced restarts. In *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*, pages 555–564, New York, NY, USA, 2008. ACM.

[7] Sven Türpe, Andreas Poller, Jan Steffan, Jan-Peter Stotz, and Jan Trukenmüller. Attacking the bitlocker boot process. In *Trust '09: Proceedings of the 2nd International Conference on Trusted Computing*, pages 183–196, Berlin, Heidelberg, 2009. Springer-Verlag.

[8] L. Ponemon. The human factor in laptop encryption. Technical report, Ponemon Institute, December 2008.

[9] Thomas Ristenpart, Gabriel Maganis, Arvind Krishnamurthy, and Tadayoshi Kohno. Privacy-preserving location tracking of lost or stolen devices: cryptographic techniques and replacing trusted third parties with dhts. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 275–290, Berkeley, CA, USA, 2008. USENIX Association.

[10] Absolute Software. Lojack for laptops www.lojackforlaptops.com.

[11] D.B. Cornish and R.V. Clarke. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, 16:41–96, 2003.

[12] G. Kitteringham. Lost laptops = lost data: Measuring costs, managing threats. Crisp report, ASIS International Foundation, 2008.

[13] R. Willison and M. Siponen. Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM*, 52(9):133–137, 2009.

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

[15] N. Barrett. Penetration testing and social engineering hacking the weakest link. *Information Security Technical Report*, 8(4):56–64, 2003.