ATM Security

A Case Study of a Logical Risk Assessment

Johannes Braeuer
Dept. of Information Systems
Johannes Kepler University
Linz, Austria
email: johannes.braeuer@jku.at

Bernadette Gmeiner
Banking Automation
KEBA AG
Linz, Austria
email: gmb@keba.com

Johannes Sametinger
Dept. of Information Systems
Johannes Kepler University
Linz, Austria
email: johannes.sametinger@jku.at

***Abstract*—Automated Teller Machines (ATMs) contain considerable amounts of cash and process sensitive customer data to perform cash transactions and banking operations. In the past, criminals mainly focused on physical attacks to gain access to cash inside an ATM's safe. They captured customer data on the magnetic strip of an ATM card with skimming devices during insertion of the card. These days, criminals increasingly use logical attacks to manipulate an ATM's software in order to withdraw cash or to capture customer data. To understand the risks that arise from such logical attacks, we have conducted a risk assessment of an ATM platform that is running in a real banking environment. The result of this assessment has revealed the main issues that are responsible for vulnerabilities of an ATM platform. In this paper, we discuss the findings of our risk assessment as well as countermeasures to mitigate serious risks in order to ensure a secure banking environment. The risk assessment has revealed effective countermeasures and has additionally provided a prioritization of activities for ATM manufacturers.**

Keywords-automated teller machines; ATM security; embedded systems; risk assessment.

I. INTRODUCTION

Automated Teller Machines (ATMs) have their roots back in the late 1930s, but they began to revolutionize the banking environment in the 1960 [1]. With the integration of real-time terminals, ATMs have been developed to data processing units that contained commercially available computers. Today, almost all three million ATMs around the world are running on operating system (OS) Windows [2]. On top of Windows, the ATM platform controls all peripheral devices and uses the OS to communicate with device drivers. The ATM platform also provides an interface to multi-vendor ATM software, i.e., bank applications that utilize the platform's functionality. Besides Windows, ATMs use the Internet Protocol (IP) for communication in the banking network [3]. Consequently, the ATM network is part of the banking network, which in turn is part of the Internet. ATMs have developed from stand-alone equipment with simple cash dispensing capabilities to a network of connected devices for bank transactions. ATMs contain a remarkable amount of cash for their daily operation. Thus, they have always been an attractive target for thieves and fraudsters [4]. Also, they were available around the clock and often located off-premises [5]. Fraudulent activities are not only attracted by cash, but also by data that is required to conduct full bank transactions. Risk assessments provide information to select adequate countermeasures and controls for mitigating the likelihood or impact of risks. We have conducted such a risk assessment concentrating on logical risks of an existing ATM platform. The proposed method can easily be extended to physical risks and risks resulting from card and currency fraud.

In this paper, we will first provide an overview of attacks to ATMs as well as their countermeasures. We will then evaluate the countermeasures for logical attacks by a risk assessment. As a result, we can confirm that suggested countermeasures work for the identified risks. Additionally, we can prioritize these countermeasures and provide a guideline for those responsible for ATM security. The paper is structured as follows. In Section II, we describe criminal activities in the context of ATMs and discuss traditional attacks and countermeasures. Section III concentrates on logical ATM security. Section IV presents a risk assessment approach, which is then used in Section V to determine the risks of an ATM platform. Findings are discussed in Section VI. Related work and a conclusion follow in Sections VII and VIII, respectively.

II. AUTOMATED TELLER MACHINES

An ATM is a cash dispensing machine with the capability to credit or debit a customer account without human intervention [1]. The term ATM has been used synonymously for cash machines, cash dispensers or cash recyclers. However, the designation ATM is inappropriate when a machine cannot perform a complete financial transaction initiated by the customer. Thus, ATMs support synchronous or asynchronous electronic data processing operations in an online and real-time manner [1]. ATMs have revolutionized the banking sector. Their widespread dissemination has grown to a world-wide use of around 2.8 million ATMs. This number is expected to reach 3.7 million by 2018 [6]. ATMs have always been an attractive target for thieves [4]. Reinforced by the fact that ATMs are typically available 24/7 and often located off-premises, they are vulnerable to cash thefts [5]. However, ATM crime, including ATM fraud, goes beyond stealing cash. Illegally obtaining customer's personal information, such as bank account data, card number and PIN is an additional security issue that is related to ATMs [5][7]. These digital assets do not provide an immediate profit, but they can be sold on illegal credit card data markets on the Internet [8].

There are three different types of attacks, i.e., card and currency fraud, physical attacks and logical attacks [9][10]. Various Information Technology (IT) security standards have been developed and vendors have recommended security concepts pertaining to ATMs [11]. The goal is to secure an entire ATM and its environment. Similar to ATM crime, ATM security can be divided into the three different core areas card and currency protection, physical security, and logical security. The former two will be described in the next subsections. Logical ATM security will follow in Section III.

A. *Card and Currency Fraud*

Card and currency frauds include direct attacks to steal cash or cards as well as indirect attacks to steal sensitive cardholder data that is later used to create fake cards for fraudulent withdrawals [10]. The target of these attacks is a single ATM, which may be physically manipulated for skimming, card fishing and currency trapping. Skimming is the approach to install an additional device, called a card skimmer, to capture the card's information on the magnetic strip. Lower tech card fishing and currency trapping focus on either card or cash capturing, typically using thin plates, thin metallic stripes, transparent plastic film, wires and hooks [5]. There are several security methods that deal with this threat category. Jitters, for example, vary speed and movement of cards or introduce motion. In other words, it distorts the magnetic stripe details and makes it difficult for the skimmer to read data while the card reader pulls the card into the ATM [12]. A further approach of an anti-skimming module is a jammer with the aim to disrupt a skimmer attached to the ATM dashboard. Instead of working on a mechanical level, a jammer uses an electromagnetic field to protect the cards' magnetic strips. Hence, the card reader can generate an error code that can be traced by remote monitoring tools [5].

B. *Physical Attacks*

Attacks that result in the physical damage of the entire ATM or a component thereof primarily focus on stealing cash from the safe [10]. But, some of these attacks are also conducted to prepare a further malicious activity on a single ATM. Vulnerable and easy targets for such attacks are off-site ATMs that are open to the public, less protected and lighter compared to bank-located machines [13]. Physical security guidelines recommend seismic detectors, magnetic contacts, alarm control panels, access control and heat sensors as alarm equipment [14]. Seismic detectors indicate abnormal vibrations and can cry havoc if an ATM is about to be raided. Heat sensors detect any form of unnatural temperature rise. Volumetric detectors on the wall can detect movements in the ATM's surrounding area. Intelligent bank note neutralization or degradation systems use bank note staining. A trigger becomes activated in case an inappropriate movement of the cassettes takes place. As a result, stolen banknotes get marked with a degradation agent or a dye.

III. Logical ATM Security

Logical attacks have become more sophisticated and their execution has typically been well organized [5][7][8][15]. Thus, recent examples, such as Skimer [16], Ploutus [17], Stuxnet [18] and a logical attack demonstrated at the chaos computing club congress [19] are indicators that these attacks bring up new methods and approaches to ATM crime. ATM malware is designed to steal cardholder data and PINs or to withdraw cash [9][13][15]. Typically, malware hides in the system to remain undetected as long as possible. It impairs confidentiality, integrity and authenticity of transaction data for its particular intention [5][10]. ATM networks are based on the Internet protocol and face the same attacks as other IP-related networks, e.g., denial of service (DoS), sniffing, man-in-the-middle attacks, or eavesdropping [3][10]. Communication between ATM and host can be used as entry point to launch remote attacks [5]. Even network devices like routers and switches can be targeted [3]. Logical security focuses on maintaining a secure network, protecting the OS and designing a system so that intruders cannot threaten cardholder's data and software components [5][10]. Subsequent subsections describe such measures.

A. *Cardholder Data Protection*

Sensitive data is the main target of logical attacks [20]. The Payment Card Industry (PCI) Data Security Standard (DSS) is for the protection of sensitive cardholder and authentication data. It proposes a set of twelve requirements divided into six areas [20]. Based on these requirements we have identified four security controls, which are needed to protect cardholder data:

- *Change control*, to guarantee that necessary and wanted changes are made only
- *Data masking*, to disguise cardholder data
- *User access control*, to restrict permsissions
- *Password policy*, to hamper password guessing

B. *Host-based Firewall*

To operate a secure ATM network, logical ATM security systems must be in place [5]. A firewall and a monitoring system to analyze and authenticate connection attempts are recommended in order to build such a layer of defense [5]. Instead of installing a central firewall, an integrated firewall on the ATM is feasible, controlling network communications on the processes, protocols and ports level [8].

C. *Application Control*

Traditional security software like antivirus software is used on desktop PCs to prevent unauthorized software execution. But, antivirus software requires processing power that often goes beyond the capabilities of an ATM and relies on a signature database that needs periodic updates. These updates can only provide protection against known malware. Consequently, malware prevention must operate within the limited resources and with a minimal "footprint" to avoid complications with ATM software [8]. Whitelisting restricts software running on an ATM to a known set of applications [8] that are tested and approved for execution. Unapproved software outside the list and malware are prohibited.

D. *Full Hard Disk Encryption*

Some logical attacks bypass security protection by booting the ATM from an alternative medium, such as a USB stick or CD-ROM. This circumvention provides the possibility to manipulate configurations or to put malware in place [21]. As a countermeasure, the ATM hard disk can be protected with full hard disk encryption [21]. In addition, it is recommended to encrypt data on an ATM's hard disk to make it unreadable in case of theft or unauthorized access [10]. Physically protecting the hard disk is an additional safeguard, because data access becomes more difficult.

E. Patch Management

Logical security includes the handling of software vulnerabilities by patch management to ensure the efficiency and security of ATMs in a timely and efficient manner [22]. Continuous patch management provides protection against viruses, worms and known vulnerabilities within an OS [22]. An example in this context is the Slammer virus, which was responsible for network outages of different systems, such as ATMs with Windows [23]. The incident could have been prevented because Microsoft had provided a patch covering the exploited vulnerability six month before the virus spread out [23]. Needless to say, precautions have to be taken to avoid malicious misuse of update mechanisms.

F. Device-specific Requirements

Depending on the actual installation of ATMs, additional security controls are required for a higher level of defense. Examples of countermeasures include secure test utilities and device controls. Test utilities that are built in an ATM platform must be protected via access control mechanisms. Externally available devices, especially USB ports, must be controlled on BIOS or OS level.

IV. RISK ASSESSMENT

Risks must be controlled by countermeasures or safeguards [24]. Risk management is an important part of an organization’s security program. It provides support in managing information security risks associated with an organization's overall mission [25]. Risk management must repeatedly be conducted in periodical time spans [26]. Each iteration begins with risk assessment [26], which is initiated at a predefined time, e.g., once a year or after a major IT change [27]. It results in the identification, estimation and prioritization of IT risks based on confidentiality, integrity and availability [24]. The result represents a temporary view that will be used for further risk management decisions [26].

A. Risk Model

The risk model specifies key terms and assessable risk factors including their relationships [24]. It defines all factors that directly or indirectly determine the severity and level of a particular risk, such as assets, threat source, threat event, likelihood, impact and countermeasure. Assets represent resources of value that need to be protected [28]. Thus, a person, physical object, organizational process or implemented technology can represent an asset. A threat is the potential for a malicious or non-malicious event that will damage or compromise an asset [28], e.g., unauthorized modification, disclosure or destruction of system components and information [24]. Depending on the degree of detail and complexity, it is possible to specify a threat as a single event, action or circumstance; or as a set of these entities [24]. A vulnerability is a weakness in the defense mechanism that can be exploited by a threat to cause harm to an asset [26][28]. This weakness can be related to security controls that either are missing or have been put in place but are somehow inefficient [24].

The likelihood of a risk consists of two aspects, i.e., the likelihood of occurrence (initiation of an attack) and the likelihood of success [24]. The likelihood of occurrence demonstrates the probability of a threat to exploit a vulnerability or a set of vulnerabilities [24]. Factors that determine this likelihood value are predisposing conditions, the presence and effectiveness of deployed countermeasures and the consideration of how certain the threat event is to occur. The likelihood of success expresses the chance that an initiated threat event will cause an adverse impact without considering the magnitude of the harm [24]. The impact describes the magnitude of expected harm on an organization [28]. To determine the impact, it is important to understand the value of the asset and the value of an undamaged system. Besides, it is advisable to consider an impact not only as a one-time loss because it can have relationships to other factors that cause consequential damage [24]. A risk is a combination of the likelihood that an identified threat will occur and the impact the threat will have on the assets under review [24]. Risk factors, such as threat, vulnerability, likelihood and impact determine the overall risk. Impact and likelihood are used to define the risk level [27].

B. Risk Assessment Process

Different risk assessment processes, frameworks and methodologies build on the same underlying process structure, which may vary in abstraction level and granularity [24][26]. These steps, which are listeted below, do not have to be strictly adhered to in sequential order. For example, it is useful to perform threat and vulnerability identification side by side to cover all risk possibilities. Also, some step iterations are necessary to get representative results [24].

1. *Definition of Assets* - No action can be taken unless it is clarified what the assets are. Asset definition seeks to identify the processes, applications and systems that are highly important and critical to an organization's daily operation [28].
2. *Identification of Threat Sources and Events* - Threat sources can be characterized based on their capability, intent and target to perform a malicious activity [24]. Once the list of sources is complete, threat events must be identified that can be initiated by a threat source. Predefined checklists are an easy way to verify whether the listed threat events can occur in the context of the assessment. But, an exclusive use of checklists can negatively influence the outcome because it may impair the free flow of creative thinking and discussing. An important step is the determination of the relevance of each threat event. If considered relevant, an event will be paired with all possible threat sources that can initiate it.

ISBN: 978-1-61208-438-1

3. *Identification of Vulnerabilities and Predisposing Conditions* - Next, we have to identify vulnerabilities that can be exploited as well as the conditions that may increase or mitigate susceptibility. Tool support is feasible for this task. For example, vulnerability scanners automatically test internal and external system interfaces in order to find known and obvious weaknesses.
4. *Determination of Overall Likelihood* - The overall likelihood represents the probability that the threat exploits vulnerabilities against an asset [28]. To get an adequate value and to keep focused on specific aspects, the overall value is divided into likelihood of initiation/occurrence and likelihood of success. These are an assessment of the probability that a non-adversarial threat happens or an adversarial threat source launches an attack [24]. In contrast, the likelihood of success is the probability that an initiated threat event results in an adverse impact [24].
5. *Determine Magnitude of Impact* - It is necessary to determine the impact the event will have on the organization [28]. For this task, the values of reviewed assets are an important input because they show the potential harm and the severity of the impact in case of a full or partial loss. The harm can be expressed in terms of monetary, technical, operational or human impact criteria [27].
6. *Determine Risk* - The risk level is determined by combing impact and overall likelihood [24][27]. It shows the degree to which an organization is threatened [24]. Formulas, matrices or methods that are used for merging likelihood and impact must be consistent and precisely defined.

V. CASE STUDY

The aim of this case study is a risk assessment to establish a baseline assessment of risks that are faced by an ATM platform of a specific manufacturer. Thus, the risk assessment identifies all threats, vulnerabilities and impacts that cause a risk to an ATM asset. The focus on the ATM platform limits our investigation to software aspects. Thus, we mainly focus on logical risks. We'd like to mention at this point that we have to refrain from describing attacks in too much detail, because this would provide valuable information to potential attackers. However, the given information is sufficient for readers to follow the conclusions that we will draw.

A. *System Characterization*

The logical system structure of an ATM consists of three layers as shown in Figure 1. On the bottom end is the OS, which is on top of the hardware layer (not considered here) and builds the base for all layers above. The second layer is the ATM platform that uses the functionalities of the OS in order to communicate with hardware components. The ATM platform provides a public interface to multi-vendor ATM software and bank applications that depict the third layer. The ATM platform is designed to run on various releases of Microsoft Windows. Some of these releases are optimized for point of sale solutions, i.e., Embedded POSReady. The ATM platform implements the eXtension for Financial Services (XFS) interface specification defined in [29]. XFS does not differ between a multi-vendor ATM software and a bank application, but considers both forms of an ATM software as a Windows-based XFS application [29]. The key element of XFS is the definition of an Application Programming Interface (API) and a corresponding Service Provider Interface (SPI). The API provides access to financial services for Windows-based XFS applications. The SPI is similar to the API, but is utilized for the direct communication with vendor-specific service providers. Each of the service providers represents a peripheral device of the ATM. The XFS manager handles the overall management of the XFS subsystem. Thus, this component is responsible for establishing and mapping the communication between API and SPI.

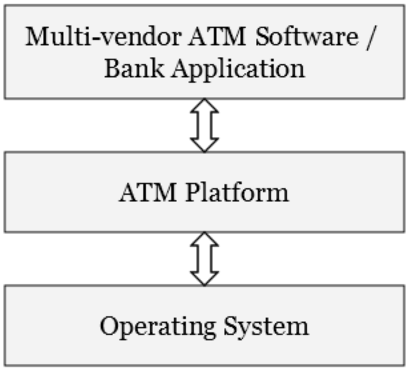

Figure 1. Logical System Structures of an ATM

B. *Logical Risk Assessment*

The risk assessment conducted in this case study is based on the risk assessment published in [24]. The focus of the assessment is on the ATM platform, i.e., from the ATM manufacturer's perspective. The operating system and any bank applications or other ATM software have not been considered in the evaluation (the bank's perspective).

1. *Assets* - The main assets are sensitive data, cash and the company's reputation. Cash can be more precisely defined as real cash represented by bills and coins as well as book money transferred from one bank account to another. The general term of sensitive data summarizes data and information that refers to an individual or is required to secure the system. For instance, card data, personal identification number (PIN), account data or secret keys belong to this category.
2. *Threat Sources and Events* - We have derived threat sources by interviewing ATM platform engineers and customer solutions employees. The resulting sources are: attacker (or hacker), thief, cash in transit (CIT) employee, IT specialist (in data center), bank clerk, helpdesk employee, service technician and employee of ATM manufacturer. Threat events were identified in form of brainstorming sessions. Threats were grouped to categories, which were derived from the primary objective of the threat events or an important key passage in an entire scenario:
    - *Denial of Service*, making the ATM platform unavailable to a customer by dominating some of its resources.

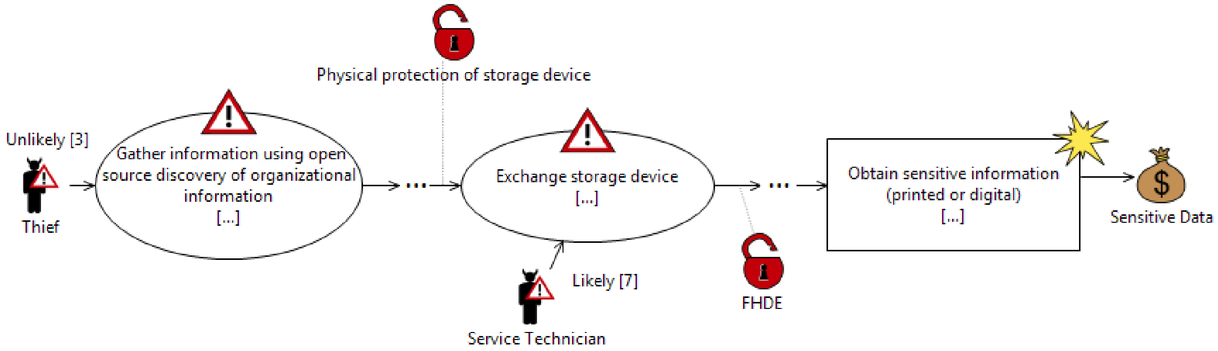
Physical protection of storage device
Unlikely [3]
Thief
Gather information using open source discovery of organizational information [...]
Exchange storage device [...]
Obtain sensitive information (printed or digital) [...]
Sensitive Data
Likely [7]
Service Technician
FHDE

Figure 2. Snippet from Threat Diagram: *Sensitive Data Disclosure*

- *Malicious Software Injection*, injecting malicious software, such as Trojan horses, viruses or worms at the OS level or the ATM platform level.
- *Sensitive Data Disclosure*, gathering unprotected cardholder data.
- *Configuration File Modification*, changing configuration files of the ATM platform.
- *Privilege Settings Modification*, modifying configuration files, focusing on the change of the user access control model to gain more privileges.
- *Software Component Modification*, modifying an executable or an assembly of the ATM platform, assuming the adversary can decompile the target file.
- *Test Utility Exploitation*, exploiting test utilities used by service technicians, IT specialists and ATM platform engineers for maintenance.

Eventually, the events were connected to threat sources and logically ordered to create entire scenarios. As a result, a directed graph was designed for each threat group. Figure 2 shows a snippet of the graph regarding the disclosure of sensitive data. With this graphical visualization on the table, the relevance of all threat scenarios was assessed and classified as either confirmed, likely, unlikely or not applicable. This is shown in Figure 2 by a label next to the threat source.

3. *Vulnerabilities* - In order to disclose vulnerabilities in the ATM platform, we have analyzed the threat scenarios based on countermeasures recommended in Section III. For instance, as is shown in Figure 2 by the second of the two lock symbols, missing hard disk encryption may allow a thief or service technician to access and read data on an ATM's hard disk.
4. *&* 5. *Likelihood and Magnitude of Impact* - We have derived the likelihood of occurrence from the characteristics of particular threat sources. These characteristics had been determined in discussions with employees from the ATM manufacturer and included capabilities of threat sources as well as intent and targeting, see (24). The likelihood of success has been determined by the vulnerabilities of the ATM platform. Results of threat scenarios, which were linked to the three assets of the ATM, were assessed as very high (10) or high (8), because they caused an immediate loss when they get stolen or damaged. Harm to the ATM manufacturer is evaluated as high (8) and the impact of indirect harm is considered as moderate (5). The latter is weighted as moderate because a further threat scenario is necessary to actually cause an impact.
6. *Risk* - Risk determination has the aim to aggregate all assessed aspects of the risk factors to the risk level. We have used a likelihood impact combination matrix for that purpose, see [24]. Table I shows the distribution of threat sources for risks assigned to the seven threat groups. The numbers do not represent individual scenarios, but threat sources of such scenarios. For example, in Figure 2 we have one threat scenario with two different threat sources, i.e., thief and service technician. Table II changes the perspective and shows how countermeasures affect risks of different risk levels. The Roman numerals I to VI on the left correspond to sections III.A through III.F as well as to sections VI.A through VI.F. Thus, this table helps in identifying security controls that are useful to mitigate multiple risks at once. Similar to Table I, the numbers do not represent single threat scenarios but threat sources.

VI. Discussion

The discussion about countermeasures in the literature reflects the result of the assessment in our case study. The case study additionally highlights security approaches and technologies, which were identified as most appropriate for dealing with logical ATM risks.

A. *Cardholder Data Protection*

We have identified change control and efficient user access control as most appropriate for protecting cardholder data and also for threat scenarios that focus on settings changes or software components of a running ATM platform. The main purpose is to guarantee that neither unnecessary nor unwanted changes are made. A change control system also supports the documentation of modifications, ensures that resources are used efficiently and services are not unnecessarily disrupted. With reference to ATMs, it can be additionally applied for ensuring PCI compliance because the change control system provides an overview of software that is deployed within the ATM environment. Although data masking is activated by default by the investigated ATM platform, there are threat sources capable to disable this

TABLE I. DISTRIBUTION OF RISKS

Threat Group	Risk Level				
	very high	high	mod	low	very low
Denial of Service	-	-	-	2	-
Malicious Software Injection	-	7	40	19	-
Sensitive Data Disclosure	2	8	13	-	-
Configuration File Modification	1	7	13	7	-
Privilege Settings Modification	-	1	15	14	-
Software Component Modification	1	7	37	-	-
Test Utility Exploitation	-	6	12	-	-

TABLE II. DISTRIBUTION OF COUNTERMEASURES

Countermeasure		Risk Level				
		very high	high	mod	low	very low
I	Change Control	1	7	13	7	-
	Data Masking	-	1	3	-	-
	User Access Control	-	1	15	14	-
	Password Policy	-	1	3	-	-
II	Host-based Firewall	2	6	4	1	-
III	Application Control	1	9	38	-	-
IV	Full Hard Disk Encryption	-	9	55	19	-
V	Patch Management	-	2	9	7	-
VI	Securing Test Utilities	-	4	8	-	-
	Device Control (for USB Port)	-	2	1	6	-

feature. Consequently, the approach of obfuscating data becomes inadequate if user access control is not in place. The most efficient way of implementing a user access control mechanism is by applying the user management that comes with the OS. Not a technical but an organizational countermeasure is the implementation of a password policy, which enforces a periodical change of passwords that are either used for locking user accounts or for switching to the maintenance mode of the ATM platform.

B. *Host-based Firewall*

Malicious use of the network interface can be mitigated through a host-based firewall. Such a firewall has to work on the level of protocols, ports and processes, i.e., the configuration of the firewall must specify protocols and ports that can be used by a particular process for outgoing connections. The same applies for incoming traffic. All ports and protocols that are not in use must be blocked by default.

C. *Application Control*

Protection against unauthorized software on ATMs has to focus on whitelisting, where the execution of applications and executables is limited to a predefined set. This set includes files that are required to run the OS and the ATM platform. All other executable files not in the whitelist cannot be launched, even if not malicious. As a consequence, threat scenarios that install known or tailored malware on the ATM platform fail in the execution of the malicious software. Whitelisting solutions offer a simple device control by removing the device’s driver from the whitelist.

D. *Full Hard Disk Encryption*

Hard disk encryption is a powerful countermeasure against alternatively booting the system for malicious activities. Several threat events require access to an ATM's computer to boot the system from an alternative medium. Although launching an alternative OS would work because the environment is running in the RAM, access to the encrypted hard disk fails. As a result, an adversary is not able to search for sensitive data, to drop malicious files, to collect executables and dynamic link libraries from the ATM platform or to change the privileges of restricted objects. Hard disk encryption tones down threat scenarios that concentrate on stealing or exchanging a hard disk as encrypted hard disks cannot be used on another system. A Trusted Platform Module (TPM) chip, which is mounted on a computer's main board, can be used to establish this connection. Other approaches do not require additional hardware, but can compute the encryption key based on unique characteristics of installed hardware components or network location of the ATM.

E. *Patch Management*

A fundamental base for an effective patch management is appropriate hardening of a system. Compared to a firewall that works at the network side, system hardening focuses on the OS level and removes or disables all unnecessary applications, users, logins and services. For instance, non-essential applications, which may offer useful features to a user at a workstation, must be removed because they could provide a backdoor to an ATM environment. Next to hardening, a rule policy with defined user privileges must be in place. The reason is that managing a distributed system like an ATM network still provides a vector for the installation of malware by maintenance staff. Based on that groundwork, a continuous patch management allows a financial institute to provide protection against known viruses, worms and vulnerabilities within an OS.

F. *Device-specific Requirements*

For dealing with the potential danger arising from test tools used by ATM platform engineers, service technicians and IT specialists, it is important that these tools function only under certain circumstances. Especially, when the ATM is in maintenance mode, the tools should support the activities on the ATM. But, in all other cases they must be disabled. Device control comes into play when the USB ports of an ATM represent possible entry points for a malicious activity. Similar to the concept of application control, device control can be implemented by whitelisting solutions too. Instead of blocking an application, a whitelisting solution can block the USB driver resulting in disabled USB ports.

VII. Related Work

DeSomer demonstrates that card skimming provides the highest ATM risk [30]. In order to detect a card skimming device or the installation of a camera for PIN capturing, the author highlights risk mitigation measures, such as jitter devices, lighting improvements or fraudulent device inhibitors. A survey about ATM security highlights that some of the security measures are obsolete and inadequate [31]. Thus, fraudulent activities can be easily performed on an ATM. The work proposes improvements in the authentication process by installing a finger vein technology or a facial recognition system. Bradbury has conducted ATM security from a logical point of view [15]. He concludes that logical fraud activities on ATMs are increasing and executed as organized and highly sophisticated attacks. Adversaries are capable to manipulate the software inside of ATMs to directly withdraw money. The severity of this issue is underlined by the fact that both banks and customers are facing heavy losses. Rasiah discusses the topic of ATM risk assessment from the same perspective as we did [32]. The author adapts a non-technical approach and investigates risk management and controls by defining general ATM security goals. The paper provides a general overview on ATM risk related topics.

VIII. Conclusion

We have discussed various aspects of ATM security, i.e., card and currency fraud, physical attacks as well as logical attacks. Logical risks of a specific ATM have been assessed in a case study to evaluate and prioritize appropriate countermeasures. The risk assessment has provided information about countermeasures in general and their importance in particular. This allows the ATM manufacturer to better plan resources for security and concentrate on the most important countermeasures first. Also, we have found out that countermeasures suggested in the literature are effective for the identified risks. By multiplying risk levels and the number of threat sources of Table II, we have identified application control, full hard disk encryption, and user access control to be most effective, as they provide protection to most identified risks. A host-based firewall is also a must for ATM security, as it protects against very high risks.

Reference

[1] B. Batiz-Lazo and R. Reid, “The Development of Cash-Dispensing Technology in the UK,” IEEE Ann. Hist. Comput., vol. 33, no. 3, 2011, pp. 32–45.

[2] T. Kaltschmid, “95 percent of ATMs run on Windows XP,” heise online. [Online]. Available: http://www.heise.de/newsticker/meldung/95-Prozent-aller-Geldautomaten-laufen-mit-Windows-XP-2088583.html [retrieved: 08, 2015].

[3] C. Benecke and U. Ellermann, “Securing ’Classical IP over ATM Networks’,” presented at the Proceedings of the 7th conference on usenix security symposium (SSYM ’98), Berkeley, CA, USA, 1998, pp. 1–11.

[4] R. T. Guerette and R. V. Clarke, “Product Life Cycles and Crime: Automated Teller Machines and Robbery,” Secur. J., vol. 16, no. 1, 2003, pp. 7–18.

[5] Diebold, “ATM Fraud and Security,” Diebold, 2012. [Online]. Available: http://www.diebold.com/Diebold%20Asset%20Library/dbd_atmfraudandsecurity_whitepaper.pdf [retrieved: 08, 2015].

[6] RBR, “Global ATM Market and Forecasts to 2018,” Retail Bank. Res., 2013.

[7] ENISA, “ATM Crime: Overview of the European situation and golden rules on how to avoid it,” 2009.

[8] GMV, “Protect your automatic teller machines against logical fraud,” 2011. [Online]. Available: http://www.gmv.com/export/sites/gmv/DocumentosPDF/checker/ WhitePaper_checker.pdf [retrieved: 08, 2015].

[9] R. Munro, “Malware steals ATM accounts and PIN codes,” theInquirer, 2009. [Online]. Available: http://www.theinquirer.net/inquirer/news/1184568/malware-steals-atm-accounts-pin-codes [retrieved: 08, 2015].

[10] S. Chafai, “Bank Fraud & ATM Security,” InfoSec Institute, 2012. [Online]. Available: http://resources.infosecinstitute.com/bank-fraud-atm-security/ [retrieved: 08, 2015].

[11] PCI, “Information Supplement PCI PTS ATM Security Guidelines,” PCI Security Standards Council, 2013. [Online]. Available: https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines _Info_Supplement.pdf [retrieved: 08, 2015].

[12] F. Lowe, “ATM community promotes jitter technology to combat ATM skimming,” ATMMarketplace, 2010. [Online]. Available: http://www.atmmarketplace.com/article/178496/ATM community-promotes-jitter-technology-to-combat-ATM-skimming [retrieved: 08, 2015].

[13] T. Kitten, “ATM Attacks Buck the Trend,” BankInfoSecurity, 2010. [Online]. Available: http://www.bankinfosecurity.com/atm-attacks-buck-trend-a-2786 [retrieved: 08, 2015].

[14] ATMSWG, “Best Practice For Physical ATM Security,” ATM Security Working Group, 2009. [Online]. Available: http://www.link.co.uk/ SiteCollectionDocuments/Best_practice_for_physical_ATM_security.pdf [retrieved: 08, 2015].

[15] D. Bradbury, “A hole in the security wall: ATM hacking,” Netw. Secur., vol. 2010, no. 6, 2010, pp. 12–15.

[16] DrWeb, “Trojan.Skimer.18 infects ATMs,” Doctor Web. [Online]. Available: http://news.drweb.com/?i=4167&c=5&lng=en&p=0 [retrieved: 08, 2015].

[17] J. Leyden, “Easily picked CD-ROM drive locks let Mexican banditos nick ATM cash,” BusinessWeek: Technology. [Online]. Available: http://www.theregister.co.uk/2013/10/11/mexico_atm_malware_scam/ [retrieved: 08, 2015].

[18] Metro, “Stuxnet worm ‘could be used to hit ATMs and power plants,’” Metro. [Online]. Available: http://metro.co.uk/2010/11/25/stuxnet-worm-could-be-used-to-hit-atms-and-power-plants-591077/ [retrieved: 08, 2015].

[19] 30C3, “Electronic Bank Robberies - Stealing Money from ATMs with Malware,” presented at the 30th Chaos Communication Congress (30C3), 2013.

[20] PCI, “PCI DSS - Requirements and Security Assessment Procedures,” PCI Security Standards Council, 2013. [Online]. Available: http://de.pcisecuritystandards.org/_onelink_/pcisecurity/en2de/minisite/en/docs/PCI_DSS_v3.pdf [retrieved: 08, 2015].

[21] J. J. Leon, “The case of ATM Hard Disk Encryption,” RBR Bank. Autom. Bull., vol. 318, 2013, pp. 11–11.

[22] Diebold, “Patch Management Considerations in an ATM Environment,” Diebold, 2012. [Online]. Available: http://www.diebold.com/Diebold%20Asset%20Library/dbd_softwaredatamanagement_whitepaper.pdf [retrieved: 08, 2015].

[23] H. Cavusoglu, H. Cavusoglu, and J. Zhang, “Economics Of Security Patch Management,” in Proceedings of the The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, United Kingdom, 2006.

[24] “NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments,” National Institute of Standards and Technology, 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/ 800-30-rev1/sp800_30_r1.pdf [retrieved: 08, 2015].

[25] G. Stoneburner, A. Y. Goguen, and A. Feringa, “SP 800-30. Risk Management Guide for Information Technology Systems,” National Institute of Standards & Technology, Gaithersburg, MD, United States, 2002.

[26] R. K. Rainer, C. A. Snyder, and H. H. Carr, “Risk Analysis for Information Technology,” J. Manag. Inf. Syst., vol. 8, no. 1, 1991, pp. 129–147.

[27] ENISA, “Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.,” 2006. [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools [retrieved: 08, 2015].

[28] T. R. Peltier, Information Security Fundamentals, Second Edition. Boca Raton, FL, USA: CRC Press, 2013.

[29] CEN, “Extensions for Financial Services (XFS) interface specification Release 3.20 - Part 1: Application Programming Interface (API) Service Provider Interface (SPI) Programmer’s Reference.,” European Committee for Standarization, 16-Apr-2014. [Online]. Available: ftp://ftp.cenorm.be/PUBLIC/CWAs/other/WS-XFS/CWA16374/CWA16374-1-2011_December.pdf [retrieved: 08, 2015].

[30] F. DeSomer, “ATM Threat and Risk Mitigation,” Thai-American Business, vol. 2, 2008, pp. 28–29.

[31] F. A. Adesuyi, A. A. Solomon, Y. D. Robert, and O. I. Alabi, “A Survey of ATM Security Implementation within the Nigerian Banking Environment,” J. Internet Bank. Commer., vol. 18, no. 1, 2013, pp. 1–16.

[32] D. Rasiah, “ATM Risk Management and Controls,” Eur. J. Econ. Finance Adm. Sci., vol. 21, 2010, pp. 161–171.