A Risk Assessment of Logical Attacks on a CEN/XFS-based ATM Platform

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

Bernadette Gmeiner
Banking Automation
KEBA AG
Linz, Austria
email: b.gmeiner@outlook.com

Johannes Sametinger
Dept. of Information Systems
Johannes Kepler University Linz
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. For example, 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. This ATM platform is running in a real bank environment and is built on the CEN/XFS specification. The result of this assessment has revealed the main issues that are responsible for vulnerabilities of an ATM platform. The risk assessment has identified effective countermeasures and has additionally provided a prioritization of activities for ATM manufacturers.**

Keywords*— *ATM security; logical ATM attacks; XFS; embedded system security; risk assessment.

I. INTRODUCTION

This paper represents an extended version of a previously published article [1]. It provides more details about the risk assessment and discusses the findings in a broader sense.

Automated Teller Machines (ATMs) have their roots back in the late 1930s, but they began to revolutionize the banking environment in the 1960s [2]. 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 the operating system (OS) Windows [3]. On top of Windows, an 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 functionality of the platform. Besides Windows, ATMs use the Internet Protocol (IP) for communication in the banking network [4]. Consequently, the ATM network is part of the banking network, which in turn is part of the Internet. All in all, 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. Moreover, they are available around the clock and often located off-premises [5]. They have always been an attractive target for thieves and fraudsters [6]. Fraudulent activities are not only attracted by cash, but also by data that is required to conduct bank transactions. A further type of ATM attacks addresses malicious activities that impair the computer or the network of ATMs. Known as logical attacks, there is the common opinion that they are becoming more sophisticated and based on a well-organized execution. For example, representatives of malware, such as Skimer, Ploutus, or Stuxnet are indicators that these attacks bring up new challenges in securing ATMs and for providing secure banking environments. Furthermore, the XFS specification – see Section V – that represents the main reference for ATM engineers, is out-of-date and missing two-factor authentication for bank applications [7].

We will show an approach for the above mentioned problems and present additional details for implementing a risk assessment at an ATM. This risk assessment aims at providing information to select adequate countermeasures and controls for mitigating the likelihood or impact of risks. We have conducted the risk assessment concentrating on logical risks of an existing ATM platform. While the scope of the assessment is limited to logical risks, the used approach can easily be extended to physical risks and risks resulting from card and currency fraud. Early results of the risk assessment presented in this paper have been published previously at a conference [1]. Here, we provide a more detailed view on the conducted risk assessment including a broader discussion of the identified countermeasures. Besides, we use more recently published information on problems of the specification that is used by ATM manufactures.

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 prioritize these countermeasures and provide a guideline for those responsible for ATM security.

The remainder of the paper is structured as follows: Section II provides an overview of criminal activities in context of ATMs and discusses traditional attacks and countermeasures. Section III concentrates on logical ATM security. In Section IV, the used risk assessment approach is presented, which is then applied 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 [2]. 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. In other words, an ATM has to support synchronous or asynchronous electronic data processing operations in an online and real-time manner [2]. With these capabilities in place, ATMs have revolutionized the way of banking. Their widespread dissemination has grown to a worldwide use of around 2.8 million ATMs. This number is expected to reach 3.7 million by 2018 [8].

ATMs have always been an attractive target for thieves. This problem is reinforced by the fact that ATMs are typically available 24/7, often located off-premises, and vulnerable to cash thefts [5]. However, ATM crime, including ATM fraud, goes beyond stealing cash inside the safe. Illegally obtaining personal information of customers, such as bank account data, card number, or PIN is an additional security issue related to ATMs [5][7]. While these digital assets do not provide an immediate profit, they can be sold on illegal credit card data markets [10]. From a general viewpoint, there are three different types of attacks: card and currency fraud, physical attacks and logical attacks [11]. Various Information Technology (IT) security standards have been developed and vendors have recommended security concepts pertaining to ATMs [12]. 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: namely, card and currency protection, physical security, and logical security. The former two are briefly addressed in the next subsections. Logical ATM security is more important to the context of our work and follows 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 [13]. 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 [11]. 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 offsite ATMs that are open to the public, less protected and lighter compared to bank-located machines [14]. Physical security guidelines recommend seismic detectors, magnetic contacts, alarm control panels, access control and heat sensors as alarm equipment [15]. 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]. 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 [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 [4]. 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 [22]. 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 [22]. 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 [10].

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 [10]. Whitelisting restricts software running on an ATM to a known set of applications [10] 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 [23]. As a countermeasure, the ATM hard disk can be protected with full hard disk encryption [23]. 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 [11]. 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. Continuous patch management provides protection against viruses, worms and known vulnerabilities within an OS [24]. An example in this context is the Slammer virus, which was responsible for network outages of different systems, such as ATMs with Windows [24]. The incident could have been prevented because Microsoft had provided a patch covering the exploited vulnerability six month before the virus spread out [24]. 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 on OS level.

IV. Risk Assessment

Risks must be controlled by countermeasures or safeguards [25]. 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 [26]. Risk management must repeatedly be conducted in periodical time spans [27]. Each iteration begins with risk assessment, which is initiated at a predefined time, e.g., once a year or after a major IT transformation [28]. It results in the identification, estimation and prioritization of IT risks based on the security goals of confidentiality, integrity and availability [25]. The result represents a temporary view that will be used for further risk management decisions [27].

A. Risk Model

The risk model specifies key terms and assessable risk factors including their relationships [25]. 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 [29]. 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 [29], e.g., unauthorized modification, disclosure or destruction of system components and information. 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 [25]. A vulnerability is a weakness in the defense mechanism that can be exploited by a threat to cause harm to an asset [27][29]. This weakness can be related to security controls that either are missing or have been put in place but are somehow inefficient [25].

The likelihood of a risk consists of two aspects, i.e., the likelihood of occurrence (initiation of an attack) and the likelihood of success [25]. The likelihood of occurrence demonstrates the probability of a threat to exploit a vulnerability or a set of vulnerabilities [25]. 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 [25].

The impact describes the magnitude of expected harm on an organization [29]. 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 [25]. 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 [25]. Risk factors, such as threat, vulnerability, likelihood and impact determine the overall risk. Impact and likelihood are used to define the risk level [28].

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 [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 [25].

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 the daily operation of an organization [29].

2) Identification of Threat Sources and Events

Threat sources can be characterized based on their capability, intent and target to perform a malicious activity [25]. 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.

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 [29]. 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 [25]. In contrast, the likelihood of success is the probability that an initiated threat event results in an adverse impact [25].

5) Determination of Magnitude of Impact

It is necessary to determine the impact the event will have on the organization [29]. 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 [28].

6) Determination of Risk

The risk level is determined by combing impact and overall likelihood [27]. It shows the degree to which an organization is threatened [25]. 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 of risks faced by an ATM platform of a specific manufacturer. The applied approach identifies all threats, vulnerabilities and impacts that cause a potential risk to an ATM asset. The focus on the ATM platform limits our investigation to software aspects only. This is why the case study mainly concentrates on logical risks. We have to mention at this point that we 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.

A. System Characterization

From a general point of view, the logical system structure of an ATM consists of three layers as shown in Figure 1. On the bottom end of the structure is the operating system, which builds the base of all layers above. Hence, the ATM platform uses the functionalities of the operating system in order to communicate with the hardware components. To utilize the features that are implemented in the ATM platform, the ATM platform provides a public interface to multi-vendor ATM software and bank applications.

For providing a standardized interface to the layer above, the platform implements the eXtension for Financial Services (XFS) interface specification defined in CEN [31]. This programming specification has been published by the European Committee for Standardization (CEN) and is designed to control all peripheral devices of an ATM. 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.

Figure 2 shows the XFS architecture that builds the foundation of the ATM platform. With reference to this illustration, the key element of XFS is the definition of a set of Application Programming Interfaces (APIs) and a

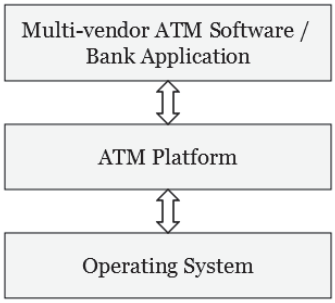

Figure 1. Logical System Structures of an ATM.

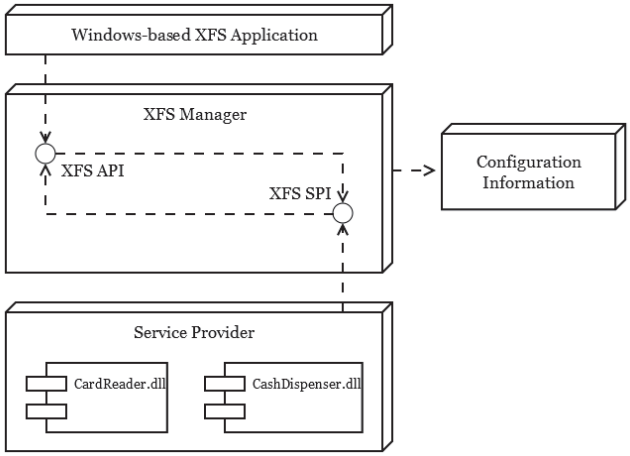

Figure 2. CEN/XFS Architecture.

corresponding set of Service Provider Interfaces (SPIs). The API provides access to financial services for Windows-based XFS applications. The SPI is similar to the API, even though it is utilized for the direct communication of vendor-specific service providers. Each of the service providers represents a peripheral device of the ATM.

1) XFS Manager

The heart of the XFS architecture is the XFS manager that handles the overall management of the XFS subsystem. This component is responsible for establishing and mapping the communication between API and SPI. In addition, the XFS manager is concerned about synchronously or asynchronously calling the appropriate service provider. For this task, a service provider is identified by a logical name parameter, which is unique within each workstation. As support, the XFS manager uses the configuration information component. This component stores the logical name parameter and defines the relationships between the Windows-based XFS application and service providers.

2) Service Providers

Either a vendor of a peripheral device or the ATM manufacturer has to implement the service provider in order to translate the device features into XFS services. Due to the fact that the peripheral devices differ in their capabilities and applications, service providers are grouped according to device classes. For example, the two service providers, Card Reader and Cash Dispenser represented in Figure 2, belong to the device class Identification Card Device (IDC) and Cash Dispenser Module (CDM). Regardless of the device class, a service provider is responsible for the functionality of translating the generic XFS request to commands that are native to the used device.

The main benefit of the XFS architecture is the fact that the XFS manager and the XFS applications are isolated from the communication between service providers and peripheral devices. As a result, vendors can individually develop their service providers, which are tailored to the devices and accessible through the XFS-API. Conversely, the XFS application that is using the ATM platform can be exchanged without changing the underlying implementation. While it would be desirable to not touch the ATM platform when changing the XFS application on the top, customizations are usually required due to some vague definitions in the XFS standard and different interpretations thereof.

B. Logical Risk Assessment

The risk assessment conducted in this case study is based on the risk assessment published in [25]. As defined in this document, the frst step focuses on the preparation of the assessment in order to establish the context. This includes the identification and definition of the purpose, scope, assumptions and the risk assessment methodology mentioned below.

1) Purpose

The purpose of this risk assessment is an implementation of an initial assessment to establish a baseline assessment of risks for the ATM platform. At the moment, the ATM manufacturer faces no security issues. This work is considered as preventive measure. In view of ensuring confidentiality, integrity and availability, the risk assessment identifies all logical threats, vulnerabilities and impacts to organizational operations, products and assets. This guarantees that the ATM manufacturer can offer a high level of software security. Additionally, the risk assessment must be reproducible, repeatable and extensible.

2) Scope

The ATM manufacturer sells its banking products in a business area that underlies different regulations designed to protect cash and sensitive data. Equivalent to these regulations, the scope of this risk assessment focuses on the protection of the same assets including the reputation of the company. Latter is part of the risk assessment because security issues are highly correlated to the public image of the ATM manufacturer and its products.

3) Assumptions and Constraints

The risk assessment ignores countermeasures, security solutions and security processes a financial institute or an independent ATM deployer has in place. Moreover, when evaluating risk factors such as threat sources, threat events, likelihood or impact, decisions are based on the worst case scenario.

4) Information Sources

Within the scope of the risk assessment, the ATM manufacturer provides security-related documents. These documents describe the platform architecture, planned and already implemented security mechanisms and possible threat scenarios. We use additional sources like ATM security guidelines [12] and best practice approaches for ATM security [30]. Besides this kind of explicit knowledge, the risk assessment is supported by expert interviews. The experts are employed at the ATM manufacturer and are divided into two groups. The first group contains technical staff with knowledge in developing the ATM platform. The second group has a deep understanding in operating the ATM platform for a financial institute or an independent ATM deployer.

5) Risk Assessment Process

The utilized risk assessment process takes its cue from the process recommended by NIST. A difference to the proposed process is that the definition of assets is in front of the threat source and threat event identification. Although NIST defines asset identification as part of the preparation, this task is added as an additional step in order to point out the assets that are worthy to protect. Consequently, the applied risk assessment process consists of the following six steps:

a) Definition of 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.

b) Identification of 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.
- *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, we have designed a directed graph for each threat group. For the graphical representation of the threat events, CORAS, a model-based method for security risk analysis [31], is used. By using this graphical approach, the risk assessment benefits from several advantages.

For instance, CORAS improves the communication and interaction between the involved parties. Therefore, it provides a precise description of the system including its security features in a simple format. Additionally, CORAS provides a tool to support the risk assessment team in documenting, maintaining and reporting the assessment result and assumptions [31]. Figure 3 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 3 by a label next to the threat source.

c) Identification of 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 3 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.

d) e) Determination of Overall 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

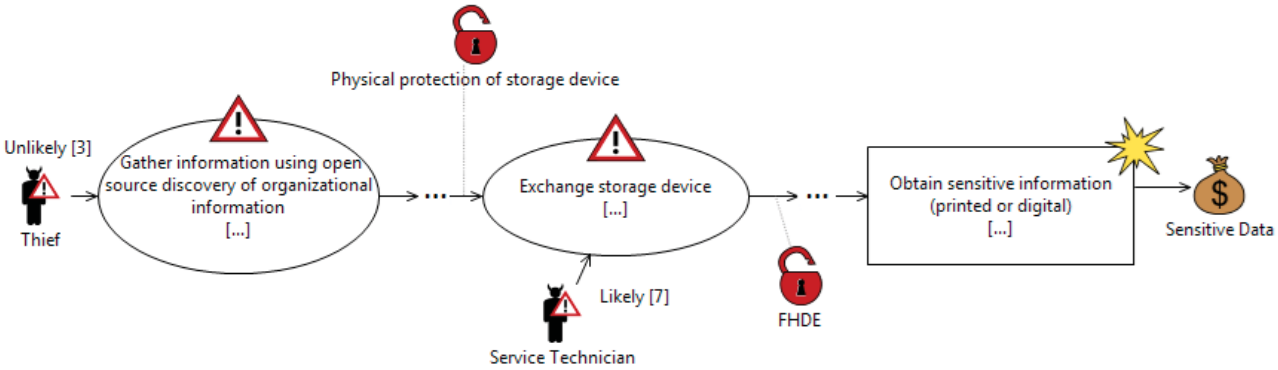

Figure 3. Snippet from Threat Diagram: *Sensitive Data Disclosure.*

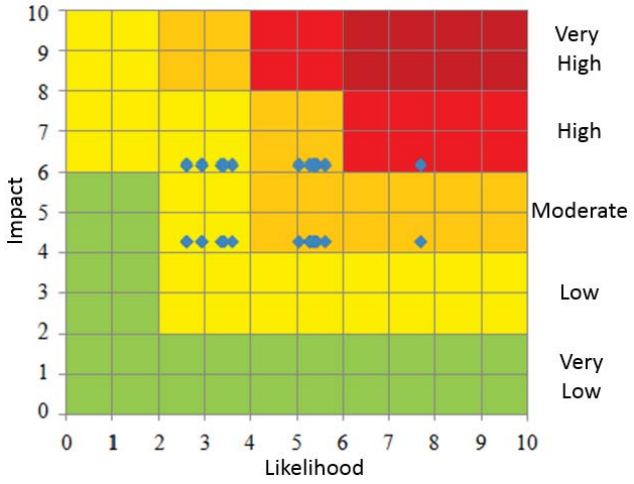

Figure 4. Likelihood Impact Diagram.

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. After the identification of both likelihood aspects (i.e., occurrence and success) they were combined to the overall likelihood of the threat scenario.

The magnitude of impact is expressed by the final result of a threat scenario. Scenarios that were linked to the three assets of the ATM have been assessed as very high (10) or high (8) since 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 damage.

f) Determination of Risk

Finally, the last step of the risk assessment is the risk determination. The risk determination has the aim to aggregate all assessed aspects of the risk factors to a single value. Therefore, we have used a likelihood impact combination matrix as proposed by NIST; see in [25] on page I-1 of the appendix. According to this matrix the level of impact is heavier weighted than the likelihood. This idea is also applied in this case study because interview partners considered the impact as dominant determinant of the risk level.

Based on the previous assessments of the overall likelihood and magnitude of impact for each threat scenario, both determinants have been combined according to the matrix. As a result, a likelihood impact diagram illustrates the risks of each category, as shown by the example in Figure 4. The coloring of the diagram is based on the likelihood impact combination matrix and represents the five areas in which a risk can fall. For clarification, the ten-step scale on both axes is divided by five with the consequence that two steps count for one qualitative value. In the diagram a risk (caused by a single threat scenario) is indicated through a dot. The position of this dot is horizontally defined by the estimation of its likelihood and vertically by its impact.

The determination of the risk has been conducted for all seven threat groups by simply combining likelihood and impact. As a result, Table I shows the distribution of risks across the seven threat groups. The numbers do not represent individual scenarios, but threat sources of such scenarios. For example, in Figure 3 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 letters A to F on the left correspond to Sections III.A through III.F as well as to Sections VI.A through VI.F. 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.

TABLE I. DISTRIBUTION OF RISKS.

Threat Group	Risk Level				
	very high	high	mod-erate	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-erate	low	very low
A	Change Control	1	7	13	7	-
	Data Masking	-	1	3	-	-
	User Access Con-trol	-	1	15	14	-
	Password Policy	-	1	3	-	-
B	Host-based Fire-wall	2	6	4	1	-
C	Application Con-trol	1	9	38	-	-
D	Full Hard Disk Encryption	-	9	55	19	-
E	Patch Management	-	2	9	7	-
F	Securing Test Utilities	-	4	8	-	-
	Device Control (for USB Port)	-	2	1	6	-

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 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 should work on the level of protocols, ports and processes. In other words, the configuration of the firewall must specify the protocol and port that can be used by a particular process for establishing an outgoing connection. The same applies for processes that are receiving incoming traffic. All ports and protocols that are not in use must be blocked by default.

By configuring the firewall for each process and closing all other connections, it is unlikely that an adversary can discover an unauthorized port or protocol. Moreover, it is not possible to open a connection to transmit sensitive data over the network. So, malware that collects data on an ATM platform cannot communicate with a receiving service due to the exclusive utilization of open ports and protocols.

C. Application Control

Other threat events are focused on installing malicious code on the ATM platform. After the infection of the target, this malware hides in the system and can be activated through an adversary. Examples of such malware are discussed in Section III. In order to deal with this type of threat, a countermeasure must be in place that detects and avoids the execution of unauthorized software. In a workstation environment an antivirus solution should be utilized for this purpose. At these endpoints normally an Internet connection is available for regularly updating the signature database or transferring behavior-based malware data to an Internet service for further investigation. However, at an ATM the concept of a blacklist is inappropriate as mentioned in Section III. Consequently, the protection against unauthorized software on an ATM must change the perspective and should focus on whitelisting.

When establishing a whitelisting solution on an ATM, the execution of applications and executables is limited to a known set. This set includes files that are required to run the operating system and ATM platform. All other executable files that are not within the whitelist, even though they are not malicious, cannot be started. As a consequence, threat scenarios that install known or tailored malware on the ATM platform fail in the execution of the malicious software. In more detail, an adversary can apply different approaches to store the malicious file on the system without facing a restriction from the control of a whitelisting solution. However, the security protection raises an alert and stops the execution process when calling the executable.

Additionally, threat scenarios with the attempt to use a modified software component of the ATM platform fail to execute the prepared file. The reason is that almost all whitelisting solutions calculate and store the hash value of a whitelisted executable in order to ensure integrity of the file. Hence, a slight modification can be detected because the difference in one bit results in another hash value. In case the hash values do not match, the executable is considered as untrusted and is prevented from running on the system. As an add-on to hash values, solutions make use of software certificates, trusted publisher or trusted directories. Latter can be a security weakness when a user has write permission on the directory.

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.

Furthermore, hard disk encryption tones down threat scenarios that concentrate on stealing or exchanging a hard disk inasmuch as an encrypted hard disk is linked to the computer and cannot be used on another system. A Trusted Platform Module (TPM) chip, which is mounted on the main board of the computer, 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. Consequently, exchanging the hard disk is useless as long as the surrounding environment cannot be made available.

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

This section highlights related work in the area of ATM security. Financial institutions argue that releasing any technical information about the implementation of an ATM would threaten the security of the devices. Consequently, it is difficult to find work that deals with the risk assessment of ATMs. Notwithstanding, some publications discuss security challenges in operating an ATM.

A. Card and Currency Fraud

In the summary of an ATM risk assessment, DeSomer demonstrates card skimming as the highest ATM risk [32]. 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. Furthermore, the article provides recommendations for choosing a nonmanipulated ATM and for using the ATM card in a secure manner.

With focus on installed ATMs in Minna, Nigeria, Adepoju and Alhassan show the result of their empirical research, which analyzes the ATM usage in combination with fraudulent activities in this area [33]. The authors come to the conclusion that most of the fraudulent activities are skimming attacks and PIN thefts by various means. Moreover, they point out that fraudsters are able to keep on track with the further development of ATMs, but banks do not install adequate countermeasures to deal with these types of threats.

By conducting an additional survey about ATM security in Nigeria, Adesuyi et al. derive a similar result like Adepoju and Alhassan [34]. They highlight that some of the security measures of an ATM are obsolete and inadequate. Fraudulent activities on can be easily performed on an ATM. In order to overcome this problem, the work proposes improvements in the authentication process by installing a finger vein technology or a facial recognition system.

B. Logical ATM Attacks

A work that investigates the security of ATMs from a logical viewpoint has been conducted by Bradbury in 2010 [21]. According to this study, logical fraud activities on ATMs are increasing and executed as organized and highly sophisticated attack. Besides, adversaries are capable to manipulate the software inside of ATM to directly withdraw money. The severity of this issue is underlined by the fact that both banks and customers are facing heavy losses.

C. ATM Risk Management

In the article titled ATM Risk Management and Controls, Rasiah discusses the topic of an ATM risk assessment like this paper. But in contrast to our technical perspective, Rasiah adapts a non-technical approach and investigates the risk management and controls by defining general ATM security goals [35]. At the beginning, the work highlights the main points of ATM crime and ATM security as mentioned in Sections II and III, respectively. Without going into details, the work provides a general overview on ATM risk related topics. For instance, it provides recommendations for handling stolen cards and for mailing the PIN to the customer. As a conclusion, the author points out that these issues have become a nationwide problem and banks must meet certain standards to guarantee a secure banking environment.

VIII. Conclusion and Future Work

Automated teller machines have become indispensable in today's banking environment. Although customers primarily use ATMs for withdrawing money, the further development in this area has integrated additional features for other banking activities. This further development is the reason that an ATM is widely accepted and considered secure. However, it is also an attractive target for criminals especially because it processes financial customer transactions and contains real cash. In order to protect the money and customer data inside an ATM, it is essential to understand the threats and their risks.

In this paper, 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 ap-

plication 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.

Future work should focus on the consideration of additional adversarial threat sources, such as cyber criminals or cyber terrorists. Compared to the threat sources discussed in this work, these groups represent structured organizations with advanced skills for conducting sophisticated attacks. In the subject area of ATM security it is commonly accepted that these groups are gaining power. Another category of threat sources, which we did not consider in this paper, is the group of competitors in the field of ATM development. Threats outgoing from competitors are interesting for investigation because they would primarily focus on disturbing the availability of the targeted ATM in order to damage the manufacturer's reputation. Furthermore, this risk assessment is limited to the operating system and ATM platform. Consequently, future work could consider the entire software stack including multi-vendor ATM software or a bank application on the top of the ATM platform. When a risk assessment contains multi-vendor ATM software, the main attention should concentrate on the interface to the ATM platform. The reason is that the interface can contain an unclosed entry point for malicious software. This vulnerability can be unknowingly exploited, even though both the ATM platform and multi-vendor ATM software are functioning correctly.

ATM frauds not only cause financial loss to financial institutes or independent ATM providers, but they also undermine customers' confidence in the use of ATMs. In order to deal with this issue and to provide a secure environment for the installed ATMs, it is important to understand the associated risks. A contribution to this challenge is made by this work, which emphasizes the consideration of ATM fraud from a logical perspective. This should help to integrate adequate countermeasures in order to make it difficult to conduct and successfully complete an attack.

REFERENCE

[1] J. Braeuer, B. Gmeiner, and J. Sametinger, "ATM Security: A Case Study of a Logical Risk Assessment," ICSEA 2015, Tenth International Conference on Software Engineering Advances, 2015, pp. 355–362.

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

[3] T. Kaltschmid, "95 Prozent aller Geldautomaten laufen mit Windows XP," *heise online*. Available: http://www.heise.de/newsticker/meldung/95-Prozent-aller-Geldautomaten-laufen-mit-Windows-XP-2088583.html. [Accessed: 14-Nov-2016].

[4] C. Benecke and U. Ellermann, "Securing Classical IP over ATM Networks," in *Proceedings of the 7th conference on usenix security symposium (SSYM '98)*, Berkeley, CA, US, 1998, pp. 1–11.

[5] Diebold, "ATM Fraud and Security," *Diebold*, 2012. Available: http://securens.in/pdfs/KnowledgeCenter/5_ATM%20Fraud%20and%20Security.pdf. [Accessed: 14-Nov-2016].

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

[7] Kasperksy Lab, "Jackpot am Geldautomaten: Wie man mit oder ohne Malware zu Bargeld kommen kann - Securelist," *SecureList*, 07-Feb-2016. Available: https://de.securelist.com/analysis/veroffentlichungen/71316/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/. [Accessed: 14-Nov-2016].

[8] RBR, "Global ATM Market and Forecasts to 2018," *Retail Bank. Res.*, vol. 2013.

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

[10] GMV, "Protect your automatic teller machines against logical fraud," 2011. Available: http://www.gmv.com/export/sites/gmv/DocumentosPDF/checker/WhitePaper_checker.pdf. [Accessed: 14-Nov-2016].

[11] S. Chafai, "Bank Fraud & ATM Security," *InfoSec Institute*, 2012. Available: http://resources.infosecinstitute.com/bank-fraud-atm-security/. [Accessed: 14-Nov-2016].

[12] PCI, "Information Supplement PCI PTS ATM Security Guidelines," *PCI Security Standards Council*, 2013. Available: https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf. [Accessed: 14-Nov-2016].

[13] F. Lowe, "ATM community promotes jitter technology to combat ATM skimming," *ATMMarketplace*, 2010. Available: http://www.atmmarketplace.com/article/178496/ATMcommunity-promotes-jitter-technology-to-combat-ATM-skimming. [Accessed: 14-Nov-2016].

[14] T. Kitten, "ATM Attacks Buck the Trend," *BankInfoSecurity*, 2010. Available: http://www.bankinfosecurity.com/atm-attacks-buck-trend-a-2786. [Accessed: 14-Nov-2016].

[15] ATMSWG, "Best Practice For Physical ATM Security," *ATM Security Working Group*, 2009. Available: http://www.link.co.uk/SiteCollectionDocuments/Best_practice_for_physical_ATM_security.pdf. [Accessed: 14-Nov-2016].

[16] DrWeb, "Trojan.Skimer.18 infects ATMs," *Doctor Web*. Available: http://news.drweb.com/?i=4167. [Accessed: 14-Nov-2016].

[17] J. Leyden, "Easily picked CD-ROM drive locks let Mexican banditos nick ATM cash," *BusinessWeek: Technology*. Available: http://www.theregister.co.uk/2013/10/11/mexico_atm_malware_scam/. [Accessed: 14-Nov-2016].

[18] Metro, "Stuxnet worm 'could be used to hit ATMs and power plants,'" *Metro*. Available: http://metro.co.uk/2010/11/25/stuxnet-worm-could-

be-used-to-hit-atms-and-power-plants-591077/. [Accessed: 14-Nov-2016].

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

[20] R. Munro, "Malware steals ATM accounts and PIN codes," *theInquirer*, 2009. Available: http://www.theinquirer.net/inquirer/news/1184568/malware-steals-atm-accounts-pin-codes. [Accessed: 14-Nov-2016].

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

[22] PCI, "PCI DSS - Requirements and Security Assessment Procedures," *PCI Security Standards Council*, 2013. Available: http://de.pcisecuritystandards.org/_onelink_/pcisecurity/en2de/minisite/en/docs/PCI_DSS_v3.pdf. [Accessed: 14-Nov-2016].

[23] J. J. Leon, "The case of ATM Hard Disk Encryption," *RBR Bank. Autom. Bull.*, vol. 318, pp. 11–11, 2013.

[24] 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, UK, 2006.

[25] "NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments," *National Institute of Standards and Technology*, 2012. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. [Accessed: 14-Nov-2016].

[26] 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, US, 2002.

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

[28] ENISA, "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.," 2006. 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. [Accessed: 14-Nov-2016].

[29] T. R. Peltier, *Information Security Fundamentals, Second Edition*. Boca Raton, FL, US: CRC Press, 2013.

[30] "Best Practices for ATM Security," GRGBanking, May 2011.

[31] F. Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based Security Analysis in Seven Steps — a Guided Tour to the CORAS Method," *BT Technol. J.*, vol. 25, no. 1, pp. 101–117, Jan. 2007.

[32] F. DeSomer, "ATM Threat and Risk Mitigation," *Thai-American Business*, vol. 2, pp. 28–29, 2008.

[33] A. S. Adepoju and M. E. Alhassan, "Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria - A Case Study of Selected Banks in Minna Metropolis," *J. Internet Bank. Commer.*, vol. 15, no. 2, 2010.

[34] 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, pp. 1–16.

[35] D. Rasiah, "ATM Risk Management and Controls," *Eur. J. Econ. Finance Adm. Sci.*, vol. 21, pp. 161–171.