Reusability assessment of financial card readers’ security mechanisms in process control devices

Apala Ray∗†, Johan Åkerberg††, Mikael Gidlund∗ Mats Björkman† and Christophe Tremlet†

∗ABB AB: Corporate Research
†Mälardalen University; School of Innovation, Design, and Technology
‡Maxim Integrated

Abstract—The security of industrial plants has gained a lot of importance since the last decade. The reason is that the different components from different network layers of automation systems have become inter-connected to support fast and cost-effective decisions at the management level. This inter-connectivity has posed many security challenges in this industrial segment. To achieve effective security mechanisms in industrial plants, there is a need to learn from other existing domains, matured in terms of security, whether existing matured security solutions can be reused in the industrial automation domain. The financial sector is a segment where security has been carefully managed since a long time, as security is very important for that sector. Therefore it would be beneficial to evaluate the security mechanisms present in financial card readers which are involved in financial transactions because these card readers have many similar characteristics with industrial process control devices. In this paper, the security requirements for both the field devices of industrial plants and card reader terminals of the financial sector have been evaluated to understand the security gap so that we can identify the areas where the security needs of industrial plants must be improved and where some of the existing security features of card reader terminals can be reused in field devices of industrial plants.

Index Terms—Industrial Automation, Security, Financial Applications, Gap Analysis

I. INTRODUCTION

Industrial plants like pulp and paper, water and wastewater, food and beverages, mining etc. generally include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC) [1]. At the beginning, industrial plants were built as stand-alone systems, where specialized hardware and software were used by proprietary control protocols. Many of these components were not connected with the outside world, so security had less attention. Therefore, these systems were built to meet performance, reliability, safety and flexibility requirements without much concern regarding secure communication capabilities. Over the last few years, low cost Internet Protocol (IP)-enabled devices have become popular in industrial segments, which raise the possibility of exposure to cyber threats since the Internet Protocol enables possibility of connectivity with the outside world. However, industrial systems have unique requirements in terms of performance and reliability that are somewhat different from general information systems. The outputs of control systems have a direct impact on the physical environment. This leads to safety issues of humans and production environments [1]. Therefore, one of the most important requirements for industrial plants is safety and any loopholes in the safety infrastructure may severely impact the system. Another prime requirement for industrial plants is availability, which is also a security property. Many processes in industrial plants are continuous in nature and the expectation is that the plant system should be operational over extended periods of time, for example 10 to 15 years. Unexpected downtime is not acceptable as the plant down-time costs money. Therefore, plant outages are generally planned and scheduled days/weeks in advance. As a result, the goals of safety and availability can sometimes conflict with the security design of plants. For instance, it is not acceptable to create a secure system which may require additional time to establish security and as a consequence disrupt production in plants. Similarly, a system which requires authentication and authorization before emergency actions is not suitable.

In the financial sector, security is a major requirement as the sector represents a vital component in the critical infrastructure of a nation. To ensure seamless operation and to maintain market trust, financial applications require secure, resilient, and reliable systems. Therefore, there is lot of research work going on to develop advanced technologies for secure financial systems and assets. In addition to that, there are best practice guidelines and many standards for security. However, some security vulnerabilities still exist in the financial sector as attackers are also improving their technologies to break the system. In spite of that, the existing security solutions in the financial sector might be good enough for industrial process control, which needs to be further investigated. The financial card readers are the components in the financial sector which share some common characteristics with industrial process control devices as both of them are low end embedded devices and prone to many security threats.

Contribution of this paper: In this paper, we have evaluated security requirements for both field devices of industrial plants and card reader terminals of the financial sector to understand the security gap between these two domains. The objective is to identify the area where the security of industrial plants is required to be improved and where some of the existing features of card reader terminals can be reused in field devices of industrial plants. The contribution of this paper is the reusability assessment and identification of technology areas, like key management, which can be adapted in industrial process control from the financial sector, whereas other areas
like tamper detection and memory erase need to be reevaluated before adapting to the industrial domain.

In this paper, section 2 discusses the related work. Section 3 presents the overview of industrial plants and the financial sector. In section 4, the assessment of security of industrial plants and the financial sector has been presented. Finally, the conclusions are presented in section 5.

II. RELATED WORK

To the best of our knowledge there is no work done which compares the reusability of security mechanisms of financial card reader terminals in industrial process control devices. However, there are many independent security analyses in both domains. In the last decade, security for industrial plants has gained major attention. The National Institute of Standards and Technology (NIST) has provided recommendations how to establish secure industrial control systems in [1]. In this document an overview of industrial control systems and typical system topologies along with identified threats and vulnerabilities and countermeasures has been presented. In [2], the communication security with security objectives, types of attack, cryptographic methods, security in communication protocols and security best practices has been discussed. In [3], the challenges of SCADA systems along with vulnerabilities in Profinet (industrial protocol) have been presented. On the other hand, the security in the financial sector is also a dominant research area, where the security mechanism in financial sector infrastructure is being scrutinized. The Payment Card Industry (PCI) Data Security Standard (DSS) and PIN Transaction Security (PTS) is developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally [4]. Secure Electronic Transaction (SET) was a standard protocol for securing credit card transactions over insecure networks such as the Internet. The SET protocol is presented in [5]. However, the SET protocol failed to get acceptance, instead the 3-D Secure protocol [6] has become an additional security layer for online credit and debit card transactions. It was initially developed by Visa [7] and later financial service providers like MasterCard [8] and AMEX adopted this. For authenticating credit and debit card transactions between payment card and card readers or automated teller machines (ATMs), EMV (Europay, MasterCard and Visa), a global standard has been developed. The minimum security functionality required for cards and card reader terminals to ensure correct operation and interoperability is specified in [9]. The inherent advantages and disadvantages of credit card payments are explored in [10].

III. OVERVIEW OF INDUSTRIAL PLANTS AND THE FINANCIAL SECTOR

In this section we present the communication architecture of industrial automation plants and the financial sector.

As shown in Figure 1, the hierarchical topology system model is based on the properties of different levels. Typically, the bottom of this hierarchy is the field network which consists of sensors and actuators, the next level is the control network, which typically consists of controllers, connectivity servers and the top level is the plant/server network which consists of operator workplaces, engineering and monitoring stations, and servers. The plant/server network can be connected to the Internet for remote monitoring through firewalls and virtual private networks (VPN).

Industrial plants have a mix of different industrial communication protocols and many proprietary protocols may exist on entire network levels as many of the devices are running for long time. To provide backward compatibility with those devices, the old proprietary protocols remain. In addition to that, there may be devices from different vendors and they may support some particular protocol. An important aspect for secured infrastructure inside the industrial plants is to provide a mechanism for secured and automated authentication of devices.

In Figure 2, the workflow in financial transaction involving payment card and card reader is presented. The transaction can be done through a point-of-sale terminal, ATM or website. The transactions using card and card-reader terminal involve consumer, financial institutes, merchant, and financial service providers. The consumer is the user who has a payment card from his bank. The merchant is an entity who does business by selling goods or services and accepts cards for the financial transactions. The financial institutes are the banks who are responsible for money depositing and lending. Generally in traditional Four Party Payment Systems as shown in 2, the financial institutions that issue payment cards are called issuers and those who have contracts with merchants to accept cards are called acquirers. The financial service providers, such as Visa [7] and MasterCard [8] generally provide the networks and services between issuers and acquirers for processing payments.

In card based financial transactions, the major components are payment cards and card reader terminals. The payment card
can have a magnetic stripe or can be chip-enabled. Magnetic strip enabled cards are capable of storing personalized data about the card holder by using the characteristic of magnetic particles on the stripe of the card. One of the major vulnerabilities is that it is easy to read the information from the cards and reproduce it. Therefore, in some scenarios customers are required to enter their 4-digit PIN number. However, most of the financial institutes are currently moving towards chip enabled cards which contain an integrated circuit (IC) chip to store data and provide secure authentication mechanisms to protect the information of the card holder. When the consumer purchases goods or services from the merchant and uses his card for payment, there are two ways of using the card. The first option is swiping the card in terminal if the card is not chip enabled and the second option is to dip the card into the card reader. The merchant enters the amount to be charged and consumer enters his PIN (personal identification number) if the authentication is required by the card readers. If the PIN is not required to be entered by terminal, the consumer needs to put his signature on the receipt from merchant. The merchant sends the transaction to the acquirer and the acquirer submits the transaction to the issuer for payment via the financial service providers’ network. After verifying authenticity the issuer pays the merchant acquirer through the financial service providers’ network. If the transaction is based on a credit card, then the issuer lends the consumers by paying the merchant acquirer through the financial service provider network and the consumer repays the issuer for the goods or services originally purchased from the merchant. If the transaction is based on debit or prepaid card, the funds are automatically withdrawn from the consumer’s account and transferred to the acquirer.

A. Comparison of workflow between financial card readers and industrial process control devices

In this paper, we consider the security requirements for entire plant life cycle, primarily commissioning, operational and maintenance. Availability is one of the most important requirements in industrial plants, followed by integrity and confidentiality. In [11], the problems that exist in the industrial plant workflow are captured in detail. It is found that an initial element which is going to be used in a key management system requires a trusted, or trusted and secured channel. Therefore, the bootstrapping of initial trust in the plant environment is still a challenge.

Similarities between industrial process control devices and financial card readers:

1) Industrial plants operate with embedded devices such as field devices. In the financial sector also the transactions involve embedded devices such as card readers or point-of-sale terminals.
2) To achieve a successful financial transaction an authentication mechanism is required. In industrial plants also, only authenticated devices are allowed to be part of the network.
3) Device compromise is a major threat in the financial sector and as well as in the industrial domain. Impersonating as a legitimate device should be detected.
4) Device tampering should be avoided in both the financial sector and the industrial domain.
5) Security credentials are required to be properly handled in both the financial sector and the industrial domain.
6) Denial of service attacks create severe threats in both the financial sector and the industrial domain. For financial transactions, the banks or brokerage firms will not be able to contact the victim to verify whether the transactions were legitimate. In worst case, the transactions will be lost. For industrial plants the availability is a major requirement and the denial of service will disrupt communication.

Differences between industrial process control devices and financial card readers:

1) Generally in an industrial plant, there is one plant owner who might be responsible for the whole plant operation though the hardware or software can come from different vendors. In financial transactions normally separate financial institutes are involved as separate independent entities.
2) In the operational phase of the industrial plant life cycle significant human intervention is not required, whereas financial transactions involve human intervention most of the time.
3) Security breaches in industrial plants cost not only large amounts of money, but may also impact the safety of human lives.
4) For chip-enabled cards, public key infrastructure are used in most of the places and the programming of keys in the card or terminal can be assumed to be

IV. ASSESSMENT OF REUSABILITY OF SECURITY FEATURES FROM FINANCIAL CARD READERS

This section assesses and compares the security features of financial transactions using card readers against the industrial automation security requirements. First of all, some major similarities and differences between financial card readers and industrial process control devices are pointed out. Then an applicability assessment of countermeasures in industrial plants form the financial sector is presented.
done in much more secured environment. Normally, the key is generated inside the chip and it never leaves the chip. This assumption might not be possible in industrial plants as industrial plants will not have a secured infrastructure similar to financial institutes. This is an issue for retrofitting the old devices and raises the challenge of the lifecycle management. For financial transactions, when a card or card IC is fresh out of the manufacturing plant, it is on purpose not usable and must go through a personalization stage before it is enabled and assigned to a unique bank account holder. For these financial transactions applications, the roles are very well defined between IC manufacturers, card manufacturers, banks, transaction acquirers and operators. In industrial infrastructures, there are different stakeholders like plant owners, equipment manufacturers and their subcontractors, infrastructure designers, companies providing operational and maintenance services etc. Enabling device authentication in industrial plants requires credential injection and lifecycle management, and roles have not been defined for that purpose yet.

5) The consumer in financial transactions is normally bound by laws and policies and the first level of authentication to open an account is done by physical verification like providing an identity card or passport. This is not exactly the same in industrial plant operation, where devices need to be authenticated to join the network.

6) The PIN which is the major key element for all financial transactions is sent to the customer by out-of-band communication (through postal mail) and each individual is responsible for keeping his PIN as secret. This is difficult to assume in an industrial plant scenario and a detailed analysis is captured in [11].

7) In industrial plants, it can be assumed that the authentication is required for devices to join the network. However, in financial transactions there are different levels of authentication between different entities such as, the consumer is required to be authenticated by bank, the card needs to be authenticated by card reader or POS terminal, the webserver needs to be authenticated, the consumer needs to be authenticated by merchants. For embedded devices in industrial plant, the concept of card is authenticated by card reader is interesting.

**B. Assessment of threats and countermeasures between financial card readers and industrial process control devices**

In this section, we discuss the threats that are applicable in both the industrial domain and the financial sector. Then we present an analysis of the applicability of probable countermeasures of the financial sector in industrial domain.

The industrial plants require deterministic responses but a high throughput is not a major importance for it. The vulnerabilities in industrial control systems have been broadly classified by NIST [1] in three categories such as policy related, platform related and network related vulnerabilities. On the other hand, with the advancement of technologies, cyber criminals are significantly posing threats to the financial sector. The attackers target this sector because of large potential profits. The vulnerabilities in this sector have been identified by FBI (Federal Bureau of Investigation, US) in [12].

In Table I, some major threats in both the financial sector and industrial plants have been presented with some probable countermeasures in the financial sector. These methods are assessed for applicability in the industrial segment. Many other threats may exist as well and the aim here is not to make this a complete list, but to provide an overview on reusability of security mechanisms of financial card readers in industrial process control devices.

The first level of plant security comes from physical protection but this cannot eliminate the complete threat of physical attack if the attacker is an insider. However if the physical security in industrial plant is not available, attackers may get direct access to the plant server, database or devices. In addition to that, wireless devices create more challenges as those devices can be kept anywhere in the plant. Though financial institutes are physically much secured, there are many components which reside in public places and not very protected. However, in industrial plants we cannot assume a secured infrastructure similar to the financial sector.

The devices are considered being compromised when an attacker is able to achieve control of those devices. Once the device is compromised, it can intercept and modify packets content destined for other devices. In the financial sector also, attackers can use a skimmer to the outside or inside of an ATM or point-of-sale terminal to collect card numbers and PIN codes. A bluetooth enabled skimmer is another threat which can read the information from a distance within wireless range. Therefore, as per standard practice in financial sectors, in addition to electro-mechanical tamper detection mechanisms, the devices are required to be inspected regularly to detect any tamper.

**Reusable features of financial card readers in industrial plants:** This section captures the reusable features which have high applicability in industrial process control.

1) In practice confidentiality, integrity and user authentication are achieved through secured credentials. If that information is leaked, the security credentials are considered to be compromised. To mitigate this threat, the normal practice in the financial sector is to keep the user password secret and this is the responsibility of each user. Therefore, in transactions using a financial card reader, the authentication is based on the users’ trust. This concept can be reused in a plant environment where the commissioning or maintenance engineer can be trusted. The main point is that 2 factor authentication can be applied in device commissioning if the engineer has a smart card or security dongle with a chip that can be read by the machine used for commissioning to authenticate the engineer. The engineer needs to type his pin that is used by the dongle/smartcard for granting access to do the commissioning.
Table I
AN ASSESSMENT OF THREATS AND COUNTERMEASURES BETWEEN INDUSTRIAL PROCESS CONTROL DEVICES AND FINANCIAL CARD READERS

<table>
<thead>
<tr>
<th>Threats in industrial process control devices and financial card readers</th>
<th>Probable countermeasure in the financial sector</th>
<th>Applicability of countermeasure in industrial plants</th>
<th>Reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device compromised</td>
<td>Protection against physical tamper and complementary manual inspection of every device</td>
<td>Medium</td>
<td>Protection against device tampering is a good option but requires change in hardware, which might be difficult in an industrial plant which has working devices from the last 20 years. In addition to that, a plant owner may be responsible for entire industrial plant, whereas manual inspection is the individual responsibility of card reader owner in the financial sector. It is a non-trivial task for a commissioning engineer in an industrial plant to find the physical devices that are spread over large areas and not always visible.</td>
</tr>
<tr>
<td>Impersonation</td>
<td>Terminal authentication, manual inspection, awareness between users</td>
<td>Medium</td>
<td>The authentication mechanism can be imported in industrial plants though monitoring the device tampering requires manual intervention for industrial plants.</td>
</tr>
<tr>
<td>Processor compromised</td>
<td>Secured processor, Erasing memory</td>
<td>Medium</td>
<td>Secured processor is a good option but proposes change in hardware, which might be difficult in an industrial plant which has working devices from the last 20 years. Moreover, erasing keys from memory can create problem if attackers can erase the data to disturb or close down the plant.</td>
</tr>
<tr>
<td>Denial of Service Attack</td>
<td>Other communication like email, sms</td>
<td>Low</td>
<td>This kind of attacks can potentially be detected once it happens, however it will disrupt the communication for some time. Availability is most important in industrial plants as the plant down time costs money.</td>
</tr>
<tr>
<td>Sniffing</td>
<td>Protection against physical tamper and manual inspection of device</td>
<td>Low</td>
<td>Similar to device compromised.</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Cryptography</td>
<td>High</td>
<td>Some protocols in industrial plants can support cryptography but it requires to establish initial trust between communicating devices [11].</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>Encrypted session, encrypted communication channel</td>
<td>High</td>
<td>Some protocols in industrial plants can support cryptography but it requires to establish initial trust between communicating devices [11].</td>
</tr>
<tr>
<td>Security credential compromised</td>
<td>Manual inspection and the responsibility of user to keep Password secret for cards</td>
<td>Medium</td>
<td>During communication no human is generally involved in industrial plants, who will enter the PIN for communication bootstrap. In the operational phase of the industrial plant life cycle also no significant human intervention is involved.</td>
</tr>
<tr>
<td>Physical Theft or Damage</td>
<td>Protected environment</td>
<td>Medium</td>
<td>Industrial plants may have access control but it might not have a secured infrastructure like financial institutes. However, it might not be realistic to bring the security environment of an industrial plant to the level of a financial institution.</td>
</tr>
<tr>
<td>Change Security environment</td>
<td>Close and secure environment</td>
<td>Medium</td>
<td>Industrial plants may have access control but it might not have a secured infrastructure like financial institutes. However, it might not be realistic to bring the security environment of industrial plant to the level of a financial institution.</td>
</tr>
</tbody>
</table>

2) The EMV specification [9] specifies mechanisms to authenticate both the card and the card holder through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In EMV transactions there are three major steps, card authentication, cardholder verification and transaction authorization. The cardholder verification step can be done based on a PIN that can be changed latter. The offline dynamic data authentication can be very useful in industrial plants when public key certificates are used.

3) In chip enabled cards, the Integrated Circuits (ICs) are secure microcontrollers which are claimed to be designed and manufactured to protect the data and enable secure transactions. These cards are also claimed to be tamper resistant. Secure memory ICs are primarily used for data protection by preventing writing or erasing data or restricting memory read access. Secure microcontrollers can enable secure data transactions, where the data stored on the card cannot be retrieved if the microcontroller cannot authenticate the system.
Generally, there are three types of security architectures for the terminal. In the first type, the terminal can use a security manager component to provide security in a general purpose microcontroller by protecting security credentials and detecting tampering. In the second type, the architecture is based on dividing the computing and security functions in microcontrollers. The general purpose microcontroller performs all non-security related tasks and a secure coprocessor controls security related activities. In the third type, a single-chip architecture is used which incorporates a high-performance secure microcontroller. This concept of storing the secured data may be interesting for next generation devices in industrial plants though it requires a migration policy for existing set-ups.

4) In the financial sector the security best practice guidelines address the security threats in consumer security. The best practice guidelines can be easily reused in industrial plants to have a secured solution.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we have discussed the security requirements for both field devices of industrial plants and card reader terminals of the financial sector. From the discussion, we can see that the security architecture of secure ICs used in the chip enabled card and card terminals may be a good option to explore in the next generation of field devices in the industrial domain but the cost analysis and implications of backward compatibility with existing devices need to be done. In addition to that, the mechanism of storing data in chip enabled cards may be interesting to store secure credentials in the next generation field devices. However, this requires new hardware, which might be difficult in industrial plants due to pre-installed base. The cost issues of replacement difficulty or retrofit for working devices which are working since last 20 years is too high. The terminals erase data stored in memory when any tampering is detected as one of the mechanisms. This mechanism can also be useful in industrial domains but this feature can create problem if attackers can erase the data to disturb or close down the plant. So this should be evaluated before accepting in industrial plants.

On the other hand, the authentication mechanism by card readers is basically dependent not only on keys and certificates but also on consumer’s confidential PIN. When a consumer receives an ATM/debit/credit card from the bank, he is given a 4-digit number as PIN. This is separately mailed to his personal residential address which he has given during the account opening procedure. Moreover, when a consumer is required to be authenticated by the bank, typically the bank authenticates financial transactions by consumer’s confidential PIN and other details which the consumer has given to the bank during account opening. Therefore, a major step of secret bootstrapping between consumer and bank comes from an out-of-band channel secret key distribution. This involves human intervention to memorize and keep PIN secret. The problem in bootstrapping trust in industrial plants is already discussed in [11]. Therefore, entering PIN code manually for every data communication will not be applicable in industrial plants as the devices are the entry point of the communication, not the human entity. In order to enable a consistent credential injection in industrial devices for further authentication, roles of various stakeholders as well as procedures have to be defined, and secure infrastructures are required to be built. In industrial plants, there is a need to have some mechanisms which can bootstrap the trust in the network. Once the device is trusted in the network, the security architecture of the device can manage the secured transactions. The 3-D secure or SET protocol might not be relevant in industrial communication unless the remote monitoring facilities are enabled. Therefore we can conclude that in the financial transaction best practice guidelines, the security architecture and the authentication based on user trust can be utilized in industrial segments though the plant infrastructure needs to support public key cryptography and an initial trust between the communicating devices. The flaws which has been found in financial transaction mechanisms need to be avoided, so that the same mistakes are not made when a security workflow for industrial segments is proposed. Such scenarios will be considered in our future work in the area of secured industrial communication.

ACKNOWLEDGMENT

This work has been supported by the Swedish Knowledge Foundation (KKS) through ITS-EASY, Embedded Software and Systems Industrial Research School, affiliated with the School of Innovation, Design and Engineering (IDT) at Mälardalen University (MDH, Västerås, Sweden) as well as by the ABB Industrial Communication and Electronics Program.

REFERENCES