Security Gap Analysis - Industrial Automation and Financial Sectors

Apala Ray
Mälardalen University
School of Innovation, Design, and Technology
apala.ray@mdh.se

ABSTRACT

The security of industrial plants has gained a lot of importance since last decade. The different components of automation systems have become inter-connected to support fast and cost effective decisions at the management level based on up-to-date information about the plant and the processes. This has posed many security challenges in this industrial segment. In addition to that, introducing wireless field devices in the plants also create new security threats. On the other hand, the financial sectors are another industrial segment where security is comparatively matured field. Although till today many security threats still exist in financial sectors. However, it would be beneficial to evaluate the security mechanisms in financial sectors if existing matured security solutions can be reused in the industrial automation domain. In this paper, the security requirements of industrial plants and financial sectors have been evaluated to understand the security gap so that we can identify the area where security needs of industrial plants to be improved and where some of the existing features from financial sectors can be reused.

Categories and Subject Descriptors

K.6.5 [**Management Of Computing And Information Systems**]: [Security and Protection]

General Terms

Security

Keywords

Industrial Automation, Security, Financial Application, Gap Analysis

1. 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) [16]. At the beginning, industrial plants were built as stand-alone systems, where specialized hardware and software were used in proprietary control protocols. These components were not fully connected with the outside world, so security had less attention. Therefore, these systems were built to meet performance, reliability, safety and flexibility requirement without secured 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 cyber threats. However, industrial systems have unique requirements of performance and reliability issues that are somewhat different from general information system security. The outputs of Control Systems have a direct impact on the physical environment. This leads to safety issues of humans and production environments [16]. Therefore, the most important requirement for industrial plants is safety and any loopholes in safety infrastructure may severely impact the system. The next prime requirement for industrial plants is availability. Many processes in industrial plants are continuous in nature and the expectation is that the plant system should be operational over extended period of time. Unexpected down-time is not acceptable as the plant down-time costs money. Therefore, the plant outage is generally planned and scheduled days/weeks in advance. However, 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 stop production in plants. Similarly, a system which requires authentication and authorization before emergency action is not suitable.

In financial sectors also the security is major requirement as they represent a vital component in critical infrastructure of a nation. To ensure seamless operation and maintain market trust, financial sectors require secure, resilient, and reliable systems. Therefore, there are lot of research work going on to develop advanced technologies for secured financial systems and assets. In addition to that, there are best practice guidelines and many standards for security. However, lot of security vulnerability still exists in financial sectors as attackers are also improving their technology to break the system.

In this paper, we have evaluated security requirements for both the industrial plants and financial sectors 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 from financial sectors can be reused. In this paper, section 2 discusses the related work. Section 3 presents the network architecture, security requirements and security threats for industrial plants. The financial sectors and the transactions using card reader and card is presented along with the security threats in section 4. In section 5, the assessment of security of industrial plants and financial sectors has been presented. Finally, the conclusions are presented in section 6.

2. RELATED WORK

To best of our knowledge there is no work done which compares the security mechanism available to financial sectors with industrial security requirements. However, there are many independent security analysis exist in both the domains. Since last decades the security for industrial plants has gained major attention. The National Institute of Standards and Technology (NIST) has provided recommendation to establish secure industrial control systems in [16]. In this document an overview of industrial control system and typical system topology along with identified threats and vulnerabilities and countermeasures has been presented. In [5], the communication security with security objectives, types of attack, cryptographic method, security in communication protocols and security best practices has been discussed. In [7], the challenges of SCADA system along with vulnerabilities in Profibus (industrial protocol) have been presented. On the other hand, the security in financial sectors 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) which was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally, provides a baseline of technical and operational requirements designed to protect cardholder data [13]. 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 [8]. However, the SET protocol failed to get acceptance, instead 3-D Secure protocol [17] to be an additional security layer for online credit and debit card transactions. It was initially developed by Visa [18] and later adopted by MasterCard [9], AMEX like financial service provider. While banks worldwide are starting to authenticate online card transactions using the "3-D Secure" protocol, the [10] claims this might be a textbook example of how not to design an authentication protocol. The "3-D Secure" protocol ignores good design principles and has significant vulnerabilities, some of which are already being exploited. 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 had been developed. The minimum security functionality required for cards and card reader terminals to ensure correct operation and interoperability is specified in [3]. The inherent advantages and disadvantages of credit card payments is explored in [15]. A Framework for Assessing Payment Security Mechanisms and Security Information on e-Commerce websites is presented in [1]. This study shows how online merchants can provide trust in the payment instrument options to potential customers by showing technical competence and ability to meet fiduciary obligations. The preliminary assessment was made using a selected number of Australian websites. In [12], the architecture of internet banking is assessed, focusing the cryptographic security controls implementation. In [2], the type of cybercrimes which poses threat to the banking industry and their mitigation solution is discussed. However, it is obvious that the industrial environment requires a security infrastructure and financial sector has some well-established security mechanism though there are not free from all security threats.

3. INDUSTRIAL PLANTS: THREAT ANALYSIS

In this section we have presented the architecture of industrial automation plants and summarized the security requirements and the security threats which are applicable to industrial plants.

3.1 Network Architecture

This section describes the network architecture of industrial automation which is based on a hierarchical topology system model as shown in Figure 1. This hierarchy is based on the requirements of categorizing 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 Control Network, which typically consists of controllers, connectivity servers and the top level is Plant/Server Network which consists of Operator Workplace, Engineering and Monitoring Stations, Servers. The Plant/Server network can be connected to internet for remote monitoring through firewall and virtual private network (VPN).

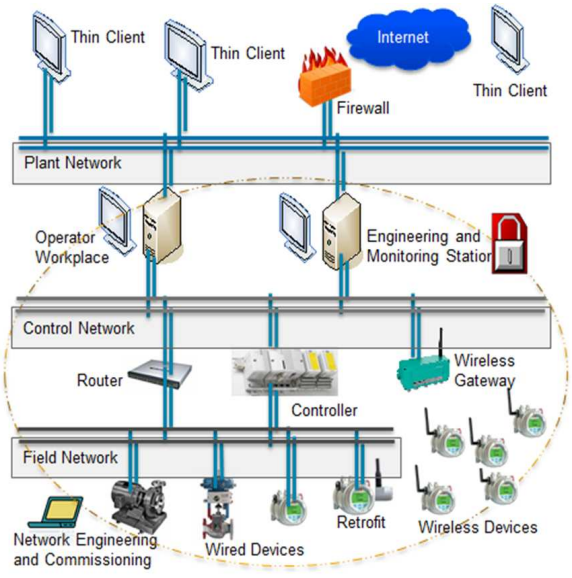

Figure 1: Industrial Automation Network

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.

3.2 Security Requirements

The industrial plants require deterministic responses and a high throughput is not a major importance for it. While the communication between Plant Network and Control Network has lesser stringent requirements on latency, real time properties; the Field Network has strict requirements on real time behavior, low latency and low jitter. The security objectives for industrial plants which provide a framework for categorizing and reviewing the threats involved are:

- Availability: During operational phase of industrial plant life-cycle, the data from the devices should be available to the operator work place or engineering or monitoring station within the update period as fixed by industrial application. Also during the maintenance phase of the plant life cycle, if a device needs to be replaced, the downtime should not be more compared to normal replacement time.
- Data integrity: For industrial plants, the sensor values or control commands should be prevented from undetected modification of information by unauthorized persons or systems, which imply that the data communication between device/sensor to controller and controller to devices should not be tampered with.
- Confidentiality: The information should be prevented from being disclosed to unauthorized persons or systems. The data should be encrypted such that no one should be able to read the content of the message that is transmitted in the wireless networks.
- Authentication: Authentication is related to determining the true identity of communicating parties. In industrial plants, the sensor device should receive data only from authenticated devices and vice versa.

3.3 Security Threats

Typically an industrial plant has a mix of different industrial communication protocols and these industrial protocols are almost common across several industries. The information of these protocols is also freely available. As a consequence, attackers may gain the knowledge of networks from open standards. In addition to that some protocols like Distributed Network Protocol 3.0 and Modbus were originally developed to run over serial connection. Later part of time, realizing the convenience and efficiency of LAN/WAN communication, these are adapted to run on top of TCP/IP stack as application layer protocols [14]. Therefore, many of these industrial and proprietary protocols lack proper security in terms of authentication or integrity checking and do not support any cryptography mechanism. There is also no homogeneous automated security policy which can be used across different protocols and systems. This in turn raises a threat of security gaps between industrial networks even if some protocols provide security mechanism. The vulnerabilities in industrial control systems have been broadly classified by NIST [16] in three categories such as policy related, platform related and network related vulnerabilities. In our classification, we have categorized the threats in four categories based on device compromise, communication medium compromise, security credentials compromise and physical attack. These threats are discussed in detail in the following section:

1. ***Devices are compromised:*** In an industrial plant, the devices are considered being compromised when an attacker is able to achieve the control for those devices. Once the device is compromised, the following threats arise.
   - *Data modification:* Once the device is compromised, it can intercept and modify the packets content to other device. This is problematic in an industrial plant when fake events are published, critical situation information is ignored or wrong control information is sent to other devices. *Data Injection* also falls under this category.
   - *Data replay:* In this scenario, the compromised devices reuse valid packets for malicious interest. It is done generally by first intercepting a valid packet and then retransmitting at later time. Now-a-days most of the advance industrial protocol protect against this type of attacks using nonce mechanism.
   - *Traffic analysis:* The compromised device can do the traffic analysis to find out the information which are getting exchanged in the network, the routing patterns and the network connectivity and as a consequence can compromise the communication medium. This type of attack can be either active or passive type of nature.*Eavesdropping* also falls under this category.
   - *Impersonate as field device:* In this scenario, a field device which is compromised by the attacker can impersonate itself and get entry in the industrial plant network. *Masquerading* is one way of impersonating as field device.
   - *Impersonate as controller device:* In this scenario, the attacker mimics as controller or gateway and may deceive the other devices to get controlled by it. *Masquerading* is one way to impersonate as controller device.
   - *Sybil:* This is a similar threat like *Masquerading* but here the device can create multiple fake identities.
   - *Deliberate exposer:* The compromised device can intentionally reveal critical data streams from that device. This is an active type of attack in industrial plants.
2. ***Communication medium is compromised:*** The communication medium is considered to be compromised if attackers are able to use the medium for communication. For wireless communication channel, this is a major threat as wireless is a broadcast medium.

The communication medium can be compromised if rogue devices are introduced inside industrial plants. Then the malicious devices can enter the network and gets hold of communication medium. The rogue devices may gain control in the network, using the impersonation attack. The inherent characteristics of some protocols also can be targeted by attackers to gain control over the network. Compromise communication medium raise the following threats.

- *Denial of Service:* In this scenario, the communication medium will be compromised by overloading the medium and thus disrupt the communication between legitimate device. Though this kind of attacks can potentially be detected once it happens, it will disrupt the communication for some times. This is not acceptable in industrial plants as communication between sensors, actuators, controllers are expected to be in real-time and this type of attack may prevent the system to perform the expected functions. In addition to that, it might cause malfunction to the process control and could lead to damage the plant equipment, safety of the plant and in turn create financial loss. This type of threat can happen in Physical Layer, MAC layer and/or IP layer of protocol stack. *Flooding* creates the threat of Denial of Service and *Jamming* generates high interferences in communication channels to disrupt the normal network traffic.
- *Sniffing:* The compromised devices can read the content of messages if the message is not encrypted. It can be passive type of attack as it might not influence the network behavior.
- *Man-in-the-middle:* If the compromised device is able to route the packets for other devices then it may read, modify and/or forward to a third party before it is sent to its original destination. This type of behavior is potentially hard to detect in the system.
- *MAC spoofing:* Protocols and systems which cannot authenticate the source or destination address can raise this type of threat and allow rogue devices to enter the network.
- *Routing attacks:* Using the security loopholes in the communication protocol, the attacker can redirect the traffic to other compromised device or server, which cause *Traffic redirect* or *Sinkhole Attack*. *Wormhole Attack* is also similar to Sinkhole attack but many devices are involved. The compromised device may not transmit the message to the next hop device, which is *Blackhole Attack* or may create *Selective forwarding*.
- *Session hijack:* If security credentials are compromised, exploiting the session key attacker can gain unauthorized access to the network.

3. ***Security credentials are compromised:*** The confidentiality, integrity and user authentication are achieved through the secured credentials. These security credentials are considered to be compromised, if that information is leaked.
   - *Key compromise:* If the security key which is used for encryption or integrity check is compromised, it will create a threat in the plant network because it will be difficult to manage/upgrade/revoke keys for that particular system. Moreover, it will be hard to detect if the keys are compromised.
   - *Password stolen:* This is similar to key compromise, once the login information is stolen any person will be able to enter the network.
4. ***Physical attack:*** Generally first level of the 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 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. The physical attack raises the following threats.
   - *Physical theft:* If the plant is not protected, the hardware or device or equipment from the plant can be stolen.
   - *Physical damage:* If the plant is not protected, the hardware or device or equipment from the plant can be damaged or tampered.
   - *Change security environment:* After gaining entry inside the plant, the attacker might change the security settings and may allow attack from outside.
   - *Change network activity:* The attackers can manipulate the network activity. If the network is based on wired scenario, removing the cable can spoil the network connectivity.

From the classification, we can see that the categorized threats are inter-linked with each other. If the device is compromised, then there is a potential chance that the communication medium or security credentials will be compromised. Similarly, if the physical attack can happen, the device might be compromised and in turn communication medium will be compromised.

4. FINANCIAL SECTORS: THREAT ANALYSIS

In this section, we have discussed the transactions flow in financial sectors. The transaction can be done through a point-of-sale terminal, ATM or website. We have also summarized the security threats which are applicable to financial sectors.

4.1 Transactions Processes

This section presents the workflow in financial transaction using payment cards which is used involving Visa [18] and MasterCard [9] as service provider. The transactions steps involving payment card and card reader are presented in Figure 2. The transactions using card and card-reader terminal involve Consumer, Financial Institute, Merchant, and Financial Service Providers. The consumer is the user who is having payment card from his bank. The merchant is an entity who is doing business by selling goods or services

and accepts card for the financial transactions. The financial institutes are the banks who are responsible in money depositing and lending. Generally in traditional Four Party Payment System, the financial institutions that issue payment cards are called issuers and who have contract with merchants to accept cards are called acquirers. The Financial Service Providers, such as VISA or Master Card generally provide the networks between issuers and acquirers for processing payments.

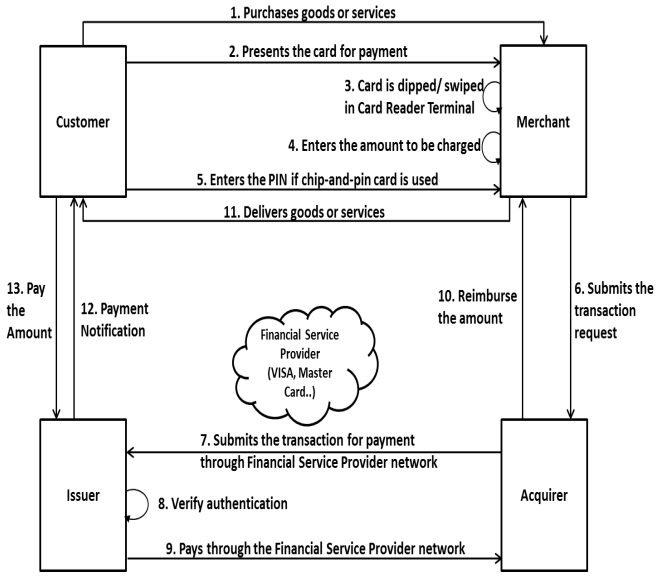

Figure 2: Transactions using Payment Card and Card Reader

The payment cards can have magnetic stripe or can be chip-enabled. When the consumer purchases goods or services from the merchant and uses his card for payment, there are two ways of using 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 acquirer and acquirer submits the transaction to 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 credit card, then issuer lends the consumers by paying the merchant acquirer through Financial Service Provider Network and 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.

The process of transactions when cards are used in automated teller machines (ATMs) is almost similar to the processes which are used in point-of-sale terminal/card reader. The typical workflow for ATM transaction is withdrawing money from an ATM. The bank's checking account verifies a consumer's authentication by 4-digit PIN entered by consumer. If the verification is satisfied and there is money in consumer's account, cash is issued. All of these workflows can be routed through one or more ATM networks. The consumer can withdraw money from a different bank's ATM if that bank is linked with the same ATM network as the bank of consumer.

The workflow of financial transaction using websites can also be fallen under this broad category though there are some extra components like web browser, web server and payment gateway. The payment gateway facilitates the transaction between a payment portal and acquirer. When the consumer selects the particular product or service what he needs to buy, he clicks on the pay button on the form of merchant website in the browser. The internet browser encrypts all the information sent by the user which is done through Secure Socket Layer (SSL) encryption. The merchant website receives the information from user and forwards to the payment gateway. The payment gateway can also be hosted separately. The rest of the process is similar to transaction using card reader. After verification, the response from bank is forwarded to the payment gateway and the payment gateway forwards the response to merchant webserver.

4.2 Security Threats

With the advancement of technologies, cyber criminals are significantly posing threats to the financial sectors. The attackers target this sector for the scope of large potential profits. The vulnerabilities in this sector has been identified by FBI (Federal Bureau of Investigation, US) in [6].

1. ***Devices are compromised:*** Often the devices which are used in financial transactions stay in open public places like ATM or shopping malls. These devices can be potentially compromised when an attacker is able to achieve the control for those devices. Once the device is compromised, the following threats arise.
    - *ATM skimming and POS skimming:* Attackers use a skimmer to the outside or inside of an ATM/ POS to collect card numbers and PIN codes. Bluetooth enabled skimmer is another threat which can read the information from a distance within the wireless range.
    - *Impersonating as valid hardware:* The attackers can mimic the security features of legitimate ATM/ POS hardware, so that the victim will not be able to identify a skimmer. *Phishing* is a similar type of attack using software.
    - *Payment processors are compromised:* When the network of large payment processors are compromised, the personally identifiable information (PII) of millions of individuals are also compromised. The attackers can use the stolen data to create fake debit cards and withdrew money.
2. ***Communication medium is compromised:*** The financial transactions are basically dependent on telecommunication or computer networks. There is a large potential threat that when transaction is happening over the internet, the communication medium is compromised and attackers are able to use that medium.

Compromise communication medium raise the following threats.

- *Telecommunication network disruption:* Generally, financial transactions are largely dependent on the availability of telecommunication infrastructure. Disruption in telecommunication network can create severe problem in financial transactions.
- *Telephone Denial of Service (TDoS):* The attackers can flood the victim's legitimate phone line with spam-like telephone calls. The banks or brokerage firms cannot contact the victim to verify whether the transactions were legitimate. The *Distributed Denial of Service (DDoS)* is also a similar type of attack.
- *Account takeovers:* This is an identity theft where attackers exploit online financial and market systems which are connected with the Internet, for instance, the Automated Clearing House (ACH) systems, card payments, and market trades. The attacker either creates another account or directly initiates a funds transfer masquerading as the legitimate user.
- *Man-in-the-middle:* The attackers can attack the user's mobile phone which is used sometimes for authentication purpose and forward the authentication information to a third party.
- *Sniffing:* The attackers can steal payment data when the information is sent from the POS terminals.

3. ***Security Credentials are compromised:*** Security credentials are very important for financial transactions to be secured.
   - *PIN disclosure:* If the PIN is compromised, it will create a threat in the financial transaction until or unless PIN is changed.
   - *Password stolen:* This is similar to PIN disclosure, once the login information is stolen any person will be able to do the transaction.
4. ***Physical attack:*** Though financial institutes are physically very secured but there are many components which reside in public place and not very protected. These can raise the following threats.
   - *Device tamper:* The ATM/POS devices can be tampered or skimmer can be attached by attackers.
   - *Supply chain infiltration:* ATM/POS can be delivered with malware installed on the systems, fake endpoints on the ATM networks can be created, or individuals can impersonate as ATM maintenance workers.
   - *Insider access:* Individuals with direct access to core processing centers of financial sectors may be in a position to steal intellectual property, insider information, or data.

5. ASSESSMENT OF FINANCIAL AND INDUSTRIAL SECURITY

This section assesses and compares the security features of financial transaction from the industrial automation security requirement point of view. The intention is to identify the area where industrial plant security needs to be improved and where some of the existing features from financial sectors can be reused. To achieve this, first of all, some major similarities and differences have been pointed out. After this, each component of financial transactions has been described with purpose, assumptions and security features to assess whether the security mechanism can be reused in industrial plants.

Similarities:

1. Industrial plants operate with embedded devices like field devices. In financial sectors also the transactions involve embedded devices like point-of-sale terminals.
2. To achieve successful financial transaction the authentication mechanism is required. In industrial plants also, the authenticated devices are only allowed to be part of the network.
3. Device compromise is a major threat in financial sectors and as well as in industrial domain. Impersonating as a legitimate device should be detected.
4. Device tampering should be avoided in both financial sectors and industrial domain.
5. Security credentials are required to be properly handled in both financial sectors and industrial domain.
6. Denial of service attack creates severe threat in both financial sectors and 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. For industrial plants the availability is major requirement and the denial of service will disrupt communication.

Differences:

1. Generally in an industrial plant, there is one plant owner who might be responsible for whole plant operation though the hardware or software can come from different vendors. In financial transactions normally separate financial institute involve as separate independent entity. Therefore if remote monitoring is not enabled, we can assume one physical protection boundary for an industrial plant. Financial transaction should assume more than one physical security boundaries.
2. In the operational phase of industrial plant life cycle there is not significant human intervention is involved, whereas financial transactions involve human intervention most of the time.
3. Failed transactions in industrial plants cost not only huge money, but also safety of human lives.

4. During financial transactions, 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 done in much secured environment. This assumption might not be possible in industrial plants as industrial plants will not have a secured infrastructure like financial institutes.

5. Consumers in financial transactions are normally bound by laws and policies and the first level of authentication to open an account is done by physical verification like providing 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 industrial plant scenario.

7. In industrial plants, it can be assumed that the authentication is required for devices to join in the network. However, in financial transactions there are many authentication between different entity such as, 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.

In card based financial transactions, the major components are payment cards and card reader terminal. The payment cards can have magnetic stripe or can be chip-enabled. Magnetic strip enabled card is capable of storing personalized data of the card holder by using the characteristic of magnetic particles on the stripe of the card. One of the major vulnerability is that it is easy to read the information from the cards and reproduce. 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. In chip enabled cards the ICs are either secure memory ICs or 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 IC is 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.

On the other hand, the card reader terminals are required to read the payment card, perform transactions after authentication. Generally, there are three types of security architectures for the terminal. In first scenario, the terminal can use a security manager component to provide security in general purpose microcontroller by protecting security credentials and detecting tamper. In second scenario, the architecture is based on dividing the computing and security functions in microcontrollers. The general purpose microcontroller performs all non-security related tasks and the secure coprocessor controls security related activity. In third scenario, a single-chip architecture is used which incorporates a high-performance secure microcontroller.

EMV specification [3] 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 transaction there are three major steps, *card authentication*, *cardholder verification* and *transaction authorization*. The step on cardholder verification is done based on PIN which can be changed latter. Although, in [11] the authors have described and demonstrated a protocol flaw which allows attacker to use the card without entering any PIN and to remain undetected even when the merchant has an online connection to the banking network. Therefore, the card reader is not able to detect the consumer's authenticity.

To prevent the online banking fraud, the Chip Authentication Program (CAP) is initiated by MasterCard. CAP specifies a handheld device which is used together with the consumert's card to generate one-time codes for both login and transaction authentication. To make a successful transaction, CAP utilizes two-factor authentication as both a card and a valid PIN must be present. However in [4], authors present various weaknesses of this protocol. To secure the financial transactions over internet, Secure Electronic Transaction (SET) was suggested. Later, it is replaced by 3-D secure which provides an additional layer of security for financial transactions. This protocol covers the communication between the merchant, issuer, acquirer and payment scheme and leaves to the issuer the consumer verification. In [10], the authors have shown the poor authentication issues in this protocol.

Observation:

1. From the discussion, we can see that the security architecture of secure ICs used in the chip enabled card and card terminal may be a good option to explore in the next generation of field devices in industrial domain but the cost analysis and implication on backward compatibility with existing devices need to be done.

2. The mechanism of storing data in chip enabled card may be interesting to store secure credentials in the next generation field devices.

3. To avoid device tampering, the terminals erase data stored in memory when any tampering is detected. This mechanism can also be useful in industrial domains. Although in industrial plants it should be considered that the erasing memory features should not affect the availability of the plant.

4. On the other hand, the authentication mechanism by card reader is basically dependent on consumer's confidential PIN. When a consumer receives 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 consumer is required to be authenticated by bank, typically the bank

authenticates financial transaction by consumer's confidential PIN and other details which consumer has given to bank during account opening. Therefore, the first 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. This mechanism will not applicable in industrial plants as the devices are the entry point of the communication, not the human entity.

5. 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 device can manage the secured transactions.

6. The use of CAP enabled one time code generator might not be applicable in industrial domain as it requires PIN and human intervention to enter the one-time code for login or authentication.

7. The 3-D secure or SET protocol might not be relevant in industrial communication unless the remote monitoring facilities are enabled. Moreover the industrial plants generally do not involve many different financial institutes like acquirer, merchant, service provider. Therefore the 3-D secure type mechanism might not be applicable in industrial domain.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we have discussed the security requirements and threats for industrial automation and evaluated the security mechanisms which are already available in the financial sectors and the corresponding threats. In financial transaction the authentication means are card (in case of point-of-sale transaction), card number (in internet banking), PIN, one-time password by handheld reader, password, 3D secure phase etc. In most of the scenario the consumer is the entry point of the financial transactions, which is different in industrial communication. In industrial plants the devices are the entry pint in communication. However, the best practice guidelines and the security architecture can be utilized in industrial segments. This may require plant infrastructure to support public key cryptography and an initial trust between the communicating devices. Moreover, the flaws which were found in financial transaction mechanism need to be avoided, so that the same mistake cannot happen 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.

7. ACKNOWLEDGMENTS

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, Västrås, Sweden) as well as by the ABB Industrial Communication and Electronics Program.

References

[1] M. Ally, Mustafa A. and Toleman. A Framework for Assessing Payment Security Mechanisms and Security Information on e-Commerce Web Sites. In *PACIS*, page 101. AISeL, 2005.

[2] D. M. Bhasin. Mitigating Cyber Threats To Banking Industry. Technical Report April, 2007.

[3] I. C. Card. *EMV Book 2 - Security and Key Management*. Number November. 2011.

[4] S. Drimer, S. J. Murdoch, and R. Anderson. Optimised to Fail: Card Readers for Online Banking. *Financial Cryptography and Data Security*, (February):1–17, 2009.

[5] D. Dzung, M. Naedele, T. P. V. Hoff, and M. Crecatin. Security for industrial communication systems. *Proceedings of the IEEE,*, 93(6):1152–1177, 2005.

[6] FBI. Cyber security threats to the financial sector. `http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector`. Last visited on 06-Nov-2012.

[7] V. M. Igure and R. D. Williams. Security and SCADA Protocols. In *5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface (NPIC and HMIT 2006)*, pages 560–567, 2006.

[8] Y. Li and Y. Wang. Secure Electronic Transaction (SET protocol). Technical report, 2001.

[9] MasterCard. MasterCard website. `http://www.mastercard.com/index.html`. Last visited on 06-Nov-2012.

[10] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. *Financial Cryptography and Data Security*, (January):25–28, 2010.

[11] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and PIN is Broken. *2010 IEEE Symposium on Security and Privacy*, pages 433–446, 2010.

[12] E. Parkin. Cryptographic Key Management Principles Applied In South African Internet Banking. Technical Report 0, 2005.

[13] Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Technical Report October, 2010.

[14] H. Security. Cyber Security Assessments Of Industrial Control Systems A Good Practice Guide. Technical Report APRIL, 2011.

[15] U. Shankar and M. Walker. A survey of security in online credit card payments. Technical report, 2001.

[16] K. A. Stouffer, J. J. A. Falco, and K. A. Scarfone. Guide to Industrial Control Systems (ICS) Security. Technical report, Gaithersburg, MD, United States, 2011.

[17] Visa. 3D Secure. `http://www.3dsecurempi.com/`. Last visited on 06-Nov-2012.

[18] VISA. VISA website. `http://corporate.visa.com/index.shtml`. Last visited on 06-Nov-2012.