

Security Threats and Risk Mitigation in a Retail Network Environment

Columbitech, www.columbitech.com

Executive Summary

The global retail industry is facing a demanding challenge in terms of new security threats to both wired and wireless networks. Critical business assets and sensitive customer information, such as credit card information, are exposed to attackers due to the lack of vital safeguards.

The objective of this white paper is to provide a comprehensive overview of the security threats that exist in a global retail environment, and to describe different control mechanisms that can mitigate these threats. The most prominent safeguard technologies are described and analyzed. Pertinent standards, laws, and regulations are discussed and, in particular, the *Payment Card Industry Data Security Standard (PCI-DSS)* is analyzed against available security threats, control mechanisms, and safeguard technologies.

For several of the weak safeguards, such as the *Wired Equivalent Protocol (WEP)*, attack software is freely available on the Internet, rendering these technologies useless in practice. The successor technology *Wi-Fi Protected Access (WPA)* was designed as an interim solution to handle legacy devices, but has not proven to be secure over the long term. *WPA2 (802.11i)*, configured with strong authentication and Advanced Encryption Standard (AES), enables a powerful security framework for the *wireless local area network (WLAN)* but does not provide any protection for *wireless wide area networks (WWAN)* enabled devices using UMTS/3G, EV-DO and WiMAX. The WPA2 technology is still vulnerable to wired attacks, rogue devices, and rogue access points. Moreover, many retail environments have large numbers of *legacy devices*, for which no WPA2 upgrades are available.

It is concluded that the proven and mature safeguard technology of Virtual Private Networks (VPNs) covers both wireless and wired threats. Traditional wired VPNs (e.g., IPSec) mitigate the security threats and are, in contrast to WPA2 solutions, network agnostic and can be used with different carriers, such as UMTS/3G, EV-DO, and WiMAX. However, to be useable in a retail environment, a *mobile VPN* with support for session resume (due to out of coverage, hibernation, or network switching), is the recommended technology that both mitigates all security threats and enables convenience features, making it practically useable in a retail environment.

Table of Contents

1. INTRODUCTION	2
2. SECURITY FUNDAMENTALS	2
2.1 THE CIA TRIAD	2
2.2 ACCESS CONTROL	3
2.3 CRYPTOGRAPHY	3
2.4 RISK MANAGEMENT	4
3. ASSETS AND SECURITY THREATS	5
3.1 ROGUE DEVICES	6
3.2 MAN-IN-THE-MIDDLE	6
3.3 MASQUERADING ACCESS POINTS (APs)	6
3.4 WIRELESS EAVESDROPPING	6
3.5 WIRED EAVESDROPPING	7
3.6 FUTURE VULNERABILITY IN SAFEGUARDS	7
3.7 SPOOFING	7
3.8 STORED DATA MANIPULATION	7
3.9 LOST OR STOLEN DEVICES	7
3.10 WORLDWIDE DOS	7
3.11 HIJACKING – LEGACY PROTOCOL	7
4. CONTROL MECHANISMS	7
4.1 SERVER-SIDE AUTHENTICATION	7
4.2 STRONG USER AUTHENTICATION	8
4.3 SYSTEM AUTHENTICATION (PSK)	8
4.4 WIRELESS ENCRYPTION	8
4.5 WIRED ENCRYPTION	8
4.6 INTEGRITY PROTECTION	9
4.7 SEGMENTATION, PACKET FILTERING	9
4.8 SEGMENTATION, USER AUTHENTICATION	9
4.9 ROGUE DEVICE DETECTION	9
4.10 PUBLICLY REVIEWED SECURITY PROTOCOLS	9
4.11 AUTHORIZATION AND AUDIT LOG	9
4.12 POLICIES AND TRAINING	9
5. SAFEGUARD TECHNOLOGIES	9
5.1 WIRED VPN	10
5.2 MOBILE VPN	10
5.3 FIREWALL	11
5.4 WEP	11
5.5 DYNAMIC WEP	11
5.6 WPA-TKIP-PSK	11
5.7 WPA2-CCMP-PSK	11
5.8 WPA2-CCMP-EAP	11
5.9 SENSORS	12
6. STANDARDS, LAWS, AND REGULATIONS	12
6.1 PCI DATA SECURITY STANDARD	12
6.2 SARBANES-OXLEY AND HIPAA COMPLIANCE	12
7. CONCLUSIONS	12

1. Introduction

During the last decade, the retail industry has dramatically increased its productivity by making use of new wireless infrastructure. These include point-of-sale (POS) terminals, ruggedized PDAs with barcode scanners, wireless printers, and scales. A typical retail environment includes both modern devices and old devices that use legacy data communication protocols. Some devices and systems are supported by wireless network standards (e.g. 802.11b [7]), while others are connected by physical wires inside the store. This mosaic of different systems and technologies raises new challenges for retail enterprises when trying to secure their networks.

Unfortunately, the low level of security awareness and installed safeguards at many retail enterprises has led to many vulnerabilities, which have lately caused several major security breaches. In January 2007, the TJX security breach was first disclosed; it has lately been shown to be one of the largest worldwide security breaches ever [9]. During this incident, 45.7 million customer records were disclosed, containing sensitive customer information such as credit card numbers, names, addresses, driver's licenses, and military identifications. Other major breaches that have occurred within the last couple of years include the DSW shoe store theft, where 1.4 million credit card numbers were stolen [3], and the POS software flaw at Polo Ralph Lauren, leading to at least 180,000 compromised credit card numbers [11].

In reaction to these system vulnerabilities, a *Payment Card Industry (PCI) data standard security* [10] was developed. Furthermore, the obvious cost of disclosing business critical information and customer information and several laws and regulations, including the *Sarbanes-Oxley Act of 2002* and the *Health Insurance Portability and Accountability Act (HIPAA)*, force enterprises to reach a certain level of security to be compliant. If these regulations are not adequately managed, the enterprises risk both financial penalty and imprisonment for the CEO and CFO.

For all these reasons, there is a concrete and urgent need for enterprises to mitigate the risk of attacks by purchasing safeguard technologies. However, without identifying the real security threats and understanding the whole picture and the underlying control mechanisms of various safeguard technologies, it is with major risk that companies invest large amounts of money in safeguards, while the networks may still be vulnerable to several forms of attacks.

The objective of this white paper is to explain and outline a comprehensive overview of security threats, control mechanisms, and safeguards in a re-

tail environment, with the aim of improving the fundamental understanding of security concerns in the retail industry, resulting in better basic data for decision making.

Paper Outline

The remainder of this white paper is organized as follows. Section 2 introduces fundamental information security concepts and terminology. Section 3 describes both wired and wireless network security threats that exist in a retail environment. In Section 4, these threats are mapped to different control mechanisms that can mitigate the risks and protect against these threats. Section 5 describes several safeguard technologies on the market. Each technology is mapped to the control mechanisms described in Section 4, including which solution addresses which threat(s). Section 6 discusses how several standards, laws, and regulations affect the threat/safeguard relationship described in previous sections. Finally, Section 7 provides concluding remarks.

2. Security Fundamentals

In this section, fundamental terms and concepts related to information security are explained and discussed. This information forms the basis for further discussions and analysis and serves as an introduction for the coming sections.

2.1 The CIA Triad

The main objective of information system security programs is to protect business critical information and other important resources according to three different concepts: *confidentiality*, *integrity*, and *availability*. These three parts are often summarized in the CIA or AIC triad, outlined in Figure 1.

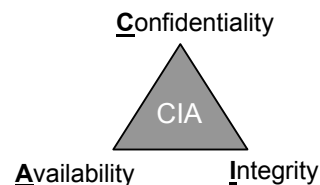


Figure 1. Outline of the CIA triad.

The meaning of the concepts is as follows:

- **Confidentiality.** Only authorized entities (people or systems) are allowed to *read* the critical information; the aim is to protect all data from unauthorized disclosure.
- **Integrity.** Only authorized entities are allowed to *create, modify, or delete* informa-

tion, providing protection from intentional or accidental changes.

- **Availability.** Authorized people and/or systems have access to information and systems when needed.

These three concepts affect each other and must all be considered when discussing a security solution. However, in some industries, one or two of the concepts are more important than others are. For example, in the military sector, confidentiality is vital, while in bank systems integrity can be considered the most important concept. It would be problematic for a bank if the balances of customer accounts were publicly exposed (confidentiality), but it would be devastating if unauthorized modification of account balances were possible (integrity).

The last concept, availability, is not uncommonly disregarded when discussing security solutions, even though it is often the most important aspect. Furthermore, availability has an important and sometimes inverse relationship to confidentiality. If critical information is encrypted and then the key is destroyed, full confidentiality is achieved, but authorized entities have no access to the information, which of course renders the procedure useless.

In the retail environment, the most focus has been on confidentiality issues, e.g., loss of customer information and credit card data. However, integrity and availability are perhaps even more important to consider in the long term. Hence, in the following parts of the paper we will consider threats, control mechanisms, and safeguards relating to all three concepts.

2.2 Access Control

A fundamental property when protecting assets such as sensitive information and computer resources is how to manage *access* to these resources, to control *who* has the rights to use *what*. Access control consists of three fundamental concepts:

- **Identification.** State who the entity (system or person) is; this usually expressed with a *user name*.
- **Authentication.** Verify the identification to make sure that the person or system is who he or she claims to be. Passwords, pass phrases, digital certificates, and physical tokens are examples of authentication data.
- **Authorization.** When the system knows who the entity is (identification + authentication), it must control what that entity can do (authorization).

Safeguard technologies typically provide different kinds of authentication mechanisms, which can be configured to fit the target organizations environment. This enables flexibility, but there is a risk that a secure product can be configured in a less secure mode and thus become able to be compromised. Hence, it is important to understand the different types of authentication mechanisms.

Authentication can be divided into three different factors or methods:

- Something you *know*, like a password.
- Something you *have*, like a hardware token, a one-time password (OTP), or a smart card.
- Something you *are*, for example the structure of your iris or your fingerprints.

If an authentication mechanism supports two or more of these factors, it is considered to be a *strong authentication*. So a system that asks for both a user name and password (something you know) and a one-time password (something you have) is considered to have strong authentication.

If a network enterprise has many different systems with different authentication mechanisms, a user might be forced to log in many times during a working session. This may lead the user to choose weaker passwords to overcome the hassle that the login process enforces. To remedy this inconvenience, a *single sign-on (SSO)* system may be implemented, enabling a user to authenticate only once for each session and still be able to access all systems.

2.3 Cryptography

Cryptography¹ is the study of using mathematical techniques to disguise information to ensure its integrity, confidentiality and authenticity. It provides the following:

- **Confidentiality.** Addresses unauthorized disclosure of information.
- **Integrity.** Addresses unauthorized modification of information.
- **Authentication.** Identifies and verifies an entity.
- **Non-repudiation.** Prevents an entity from denying previously performed actions.

The first three concepts were described in previous sections, while the fourth states that an entity should not be able to deny that an action was performed. For example, if a cashier confirms the account status

¹ If you are interested in an advanced introduction to cryptography, please read the entirety of this section. Otherwise, you can read the first paragraph and still be able to grasp the meaning of the rest of the document.

for a POS, he or she should not then later be able to deny that this confirmation was performed.

Confidentiality is achieved by using encryption algorithms to transform (*encrypt*) a *plain-text* into *cipher-text* by using a *secret key*. The reverse process of transforming a cipher-text into a plain-text is called *decryption*.

There are two basic types of encryptions:

- **Symmetric Key Encryption**, where a single secret key is used for both encryption and decryption. The algorithm can either be a *block cipher* that divides and encrypts the data in fixed sized blocks (examples include *advanced encryption standard (AES)* and *data encryption standard (DES)*) or a *stream cipher*, which encrypts a continuous stream of data without dividing into blocks (for example, algorithm *RC4*).
- **Asymmetric Key Encryption**, where each entity has a *public* and a *private* key. If a message is encrypted with the public key, only the corresponding private key can decrypt the message. Conversely, if the message is encrypted with the private key, only the public key can decrypt the message. Note that if the message is encrypted with the public key, the public key cannot be used for decryption.

Symmetric encryption is generally much faster than asymmetric key encryption. For that reason, symmetric encryption is used for bulk data encryption. For example, in WEP, RC4 is used for bulk data encryption, while in transport layer security (TLS) AES can be used.

However, symmetric encryption requires that two communication entities share the same secret key. By generating, a random symmetric key and then encrypting that key using asymmetric key encryption the shared symmetric key can be securely exchanged. The generated symmetric key is encrypted using the public key and then decrypted using the private key. The asymmetric key encryption algorithm is used for exchanging the key for the symmetric encryption algorithm. *RSA* and *Diffie-Hellman* are example of algorithms that can be used for key exchange.

A *one-way hash function* is another type of cryptographic algorithm; it takes an arbitrary long message as input and creates a fixed-size digest as output. It is called one-way because it is efficient to produce the digest from the message, but computationally very hard to do the opposite. Examples of one-way hash functions are *secure hash algorithm (SHA-1)* and *message digest algorithm 5 (MD5)*.

Hash functions are used in many areas where one significant task is to provide integrity protection of messages. This technology is called a *message authentication code (MAC)*, where the MAC is produced by hashing the message together with a secret key. A common algorithm for performing this operation is the *hashed MAC algorithm (HMAC)*, which is based on a secure hash algorithm such as SHA-1 or MD5².

Authentication using cryptography can be accomplished by using asymmetric encryption (private key encryption and public key decryption) on a hashed message. The result of this process is called a *digital signature*. This technique can also be used to prevent an entity from denying that a certain message was signed. This enables non-repudiation. However, this technique assumes that the private key is kept intact and is not stolen.

The above-described cryptographic operations are commonly combined into standardized security protocols, such as the *transport layer security (TLS)*[2], *wireless transport security (WTLS)*[15], and *secure socket layer (SSL)*[4]. All these protocols make use of a common infrastructure for managing *digital certificates* called the *public key infrastructure (PKI)*. It is important to stress that if the cryptographic operations are used in an incorrect manner, their security functionality will be lost. It is therefore of great importance that the security protocols be standardized and open for public review.

2.4 Risk Management

Before discussing threats and what kind of safeguard are the best choices in specific circumstances, a necessary but often neglected step is the identification and assessment of *information assets*. This concerns questions like what information are we actually trying to protect? How much would it cost to replace it? How much would it cost to lose its confidentiality, integrity, or availability? For example, if certain important documents were destroyed it would cost a certain amount of money to reproduce them (loss of availability). How much would it cost if customer records and credit card numbers were exposed (loss of confidentiality)?

The process of *identifying, analyzing, and planning* for risks is called *risk management*. It has the objective of minimizing the cost associated with the loss of information assets. The risk analysis can be performed by using a *quantitative* or a *qualitative* approach. In the quantitative approach, objective numbers are assigned to the risk analysis. On the

² MD5 has a 128-bit digest (compared to SHA-1's 160 bits) output and it is possible to find collisions in the algorithm in a short time.

other hand, the qualitative approach does not assign numbers, but instead scenarios.

In the first part, the *identification of risks*, the objective is to answer the question “What could happen?” What are the potential *threat events* that could result in loss of the information asset?

The second part, *analyzing the risks*, asks the question “If it were to happen, how bad could it then be?” What is the *impact of the threat*? It is also interesting to evaluate “How often it can happen” and “What the likelihood that it will happen is?”

The third part, *planning for risks*, concerns doing something about it. There are several alternatives available:

- **Accept** the risk, i.e., do nothing.
- **Reduce** the risk, i.e., mitigate the risk (the likelihood that it would happen) or minimize the impact if it does happen.
- **Transfer** the risk, e.g., buy insurance.

Furthermore, if a quantitative risk analysis is performed, it is possible to estimate how much it would cost annually if the information were compromised. This estimated cost could then be compared to prices

for buying different *safeguard technologies* (products such as firewalls, VPNs, and wireless encryption technologies) to judge if the investment is cost effective or not. Such a cost/benefit analysis is important to perform at a high level, even though its result may have a high uncertainty.

3. Assets and Security Threats

A retail environment commonly includes several different network equipments and devices interconnected by both wired and wireless technology. This kind of network layout is at risk from classic network security threats available in regular IP networks, but also from specific threats associated with the store’s physical setup and the legacy devices commonly in use in retail stores.

A network is never stronger or more secure than its weakest link. Hence, the presence of legacy devices with insecure protocols, (e.g. Telnet and FTP) creates particular demanding challenges regarding a secure network design.

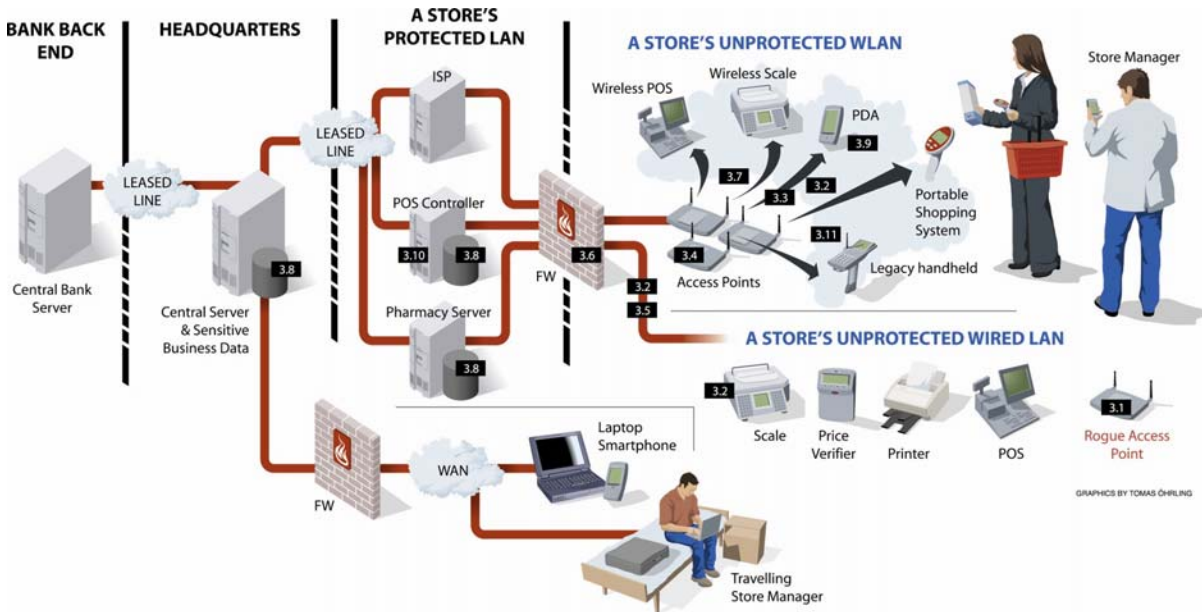


Figure 2. Outline of a retail environment, where the network is segmented into protected and unprotected LANs. Locations of potential threats are marked with a circle, where the number indicates the section number for the described security threat. To the right, the unprotected part of the network is divided into the WLAN for wireless devices and a LAN for wired devices. The central part shows the store’s protected LAN with local servers. The store’s network is typically directly connected to headquarter’s computers using a leased line. To the left, it is apparent that the central headquarter’s server is connected to external bank systems. At the bottom it is shown a future scenario for how management equipment within a store may be directly connected to headquarters using the Internet, using for example a wireless wide area network (WWAN).

This section describes and discusses the main assets in a retail environment and some of the most relevant security threats in such environments, where each threat is related to the asset that needs protection.

Consider Figure 2, which gives an overview of a retail environment, segmented into a protected and an unprotected LAN, where the unprotected part consists of both a wireless and a wired LAN. In this picture certain safeguards, such as firewalls (FWs) are already in use between the protected and unprotected parts. However, this is not always the case in real-life retail situations.

Besides the wireless and wired LANs located in the store, managers typically need to access servers both located at the headquarter and within the stores. Since the demand of mobility has increased in industry, a growing need for being able to access business critical data using wireless wide area networks (WWAN), such as UMTS/3G, EV-DO and WiMAX, are becoming more important. This add new demands on security solutions to enable secure remote access in a transparent way for the user.

The number of information assets that are vulnerable to attack varies. The following incomplete list shows some important assets (both system and information) and estimated costs due to loss of confidentiality, integrity, or availability.

- Stored and/or transmitted credit card data due to loss of confidentiality
- Sensitive company information, such as accounting and personnel information, due to loss of confidentiality
- Loss of the POS system's availability
- Loss of the price information database's integrity
- Unauthorized change in the balances on gift cards (loss of integrity)
- Loss of pharmacy information; represents both confidentiality and integrity

A number of potential security threats increase the risk of loss even above the aforementioned information assets. Note that these threats and attacks do not constitute a complete list, but they are examples of important threats common in a retail environment.

3.1 Rogue Devices

Rogue devices are unauthorized devices or systems (access points, laptops, and computers) that are intentionally or accidentally added to the network. A typical rogue device is a rogue access point located on the protected or unprotected LAN, allowing direct access to the network. Note that since many stores have a wired network available inside the

store where customers are located, an attacker may be able to install such a device without being discovered. Furthermore, it has been shown that most attacks are actually performed from inside, by employees who have access to both the protected and unprotected parts of the network. In some stores, power to electronic devices is delivered on the network cable, using power over Ethernet (PoE) technology, which makes it even more convenient to install rogue devices.

3.2 Man-in-the-Middle

A man-in-the-middle attack means that an attacker places himself between two parts of the network — a client and a server — intercepting communication without being detected. For example, if a rogue device is installed on the network, a man-in-the-middle attack can disclose the login session's username and password even if the session is encrypted. The client logs on to the attacker's node, which is pretending that it is the server. In this way, a secure connection is established between the attacker's node and the client, and between its node and the server. By using this attack strategy, the client and the server believe that they are talking to each other, but in reality the attacker stands in the middle and can read all transmitted traffic, such as login credentials. This information can then be used to log in to the system and perform malicious tasks, including manipulating customer records, changing balance status, or retrieving credit card data.

3.3 Masquerading Access Points (APs)

Unlike rogue access points that are located on the network, masquerading APs are APs that fool an authorized device into connecting to the masquerading AP instead of the real one. If the network environment's real network is successfully mirrored, the attacker may fool the user of the device into revealing his or her login credentials.

3.4 Wireless Eavesdropping

If the wireless network is open or has weak encryption, an intruder can perform wireless eavesdropping, sniffing, and reading all network traffic transmitted on the wireless network. This kind of attack can usually be conducted without even entering the store. To compromise certain insecure protocols, such as WEP, the attacker does not even need to be an expert, since attack tools are publicly downloadable on the Internet. Hence, confidential information such as personal records, credit card information, and even login information may be retrieved by a person who appears to be merely parked in the store parking lot.

3.5 Wired Eavesdropping

Due to the large wireless security breaches, such as the TJX breach, most focus has been placed on the confidentiality issues of wireless traffic. However, since most stores today have a large proportion of their devices connected using wired networks, wired eavesdropping is as dangerous as the wireless part. Rogue devices can enable wired eavesdropping, where the attack may go unnoticed for a long time.

3.6 Future Vulnerability in Safeguards

If a safeguard is chosen to address certain vulnerabilities and, therefore, mitigate the risk of an attack, there is of course no guarantee that no vulnerability will be found in the safeguard. An example where this threat became reality is the WEP protocol, which was initially assumed equivalent of the security of a wired network, but was later shown to be vulnerable to attacks on both confidentiality and integrity protection. Even when the security flaws in the protocol and algorithms were discovered, many networks have remained open for a long time due to the cost and complication of upgrading both software and hardware with new safeguards.

3.7 Spoofing

Spoofing is the technique of masquerading as a certain IP address or MAC address, with the intent of accessing a system. For example, several APs use access control based on MAC addresses, which are vulnerable to spoofing.

3.8 Stored Data Manipulation

Several of the attacks and threats described so far enable the attacking individual to gain access to the private network system. If an attacker can retrieve login credentials for one system, he or she may then be able to perform another attack. For example, by manipulating stored data, the integrity of price information or private customer information may be compromised. Furthermore, if the attacker is able to gain access to the headquarters database, data manipulation may affect all stores in the enterprise. For example, he or she could install malicious software in software installation packages that will then be spread to all connected stores.

3.9 Lost or Stolen Devices

Since many devices are portable and use a wireless network, they may be lost or stolen. If this theft goes unnoticed, an intruder may use the service without being disturbed. Even if the applications available on the devices are not directly useful to an attacker, credential information stored on the device can be

used for performing other kinds of attacks directed to other services on the network.

3.10 Worldwide DoS

One of the most important security issues regarding an enterprise is *denial of service (DoS)*, shutting down its retail capabilities. A worldwide interruption of business would lead to large costs. If an intruder manages to gain access to the headquarters and from there manipulates the database or software updates and makes *point of sale (POS)* controllers malfunction, a worldwide DoS may be the result.

3.11 Hijacking – Legacy Protocol

Retail enterprises commonly have a large base of legacy devices, such as DOS terminals using *telnet protocols* for terminal emulation. For such legacy protocols, there are well-known and publicly available tools to perform a hijacking attack, taking over a session from another user. By doing so, the attacker can, for example, perform different actions, such as changing the password for the account or installing malicious software.

4. Control Mechanisms

The described security threats and attack risks can be mitigated by different kinds of control mechanisms. The different controls are often categorized into three distinct areas, depending on the nature of the control mechanism.

- *Physical Control* – prevents unauthorized persons from physically accessing computer resources.
- *Technical (Logical) Control* – the most common mechanism type, which includes software and hardware systems that prevent attacks.
- *Administrative Control* – the policies, training, and procedures for mitigating the risks and effects of security threats.

This section describes and discusses different control mechanisms that can reduce the threats described in the previous section. The relation between the control mechanisms and threats described in this section are illustrated in Table 1, where the intersection in the table states the level of protection given for each mechanism.

4.1 Server-Side Authentication

While user authentication makes sure that the user of the client is who he or she claims to be, it does not give any guarantees that the client is connecting to the right server. Hence, without this control mecha-

nism, the network is vulnerable to the man-in-the-middle attack, as described in Section 3.2.

If the server authenticates itself to the client, the client can be sure that it is talking to the right server. This technique is commonly achieved by making use of server-side certificates and PKI infrastructure.

When both server-side and client-side authentication are used, a *mutual authentication* is established. This technical control mechanism does not only prevent man-in-the-middle attacks, but also masquerading APs and rogue devices, since the application on the client device will notice if it is not communicating with the right server.

4.2 Strong User Authentication

If strong user authentication, using more than one method of authentication, is required, the threat associated with lost or stolen devices is mitigated. Mere physical access to a device does not allow that device to be used. Strong authentication disables rogue devices from gaining access to network resources, and prevents stored data manipulation.

4.3 System Authentication (PSK)

If unique users (persons) do not have separate identifications, some control mechanisms, such as a *pre-shared key (PSK)* on all devices can give system authentication capability. However, compared to user authentication, this does not prevent an attack if a device is stolen, since the attacker in this case pos-

sesses the secret information, which may go unnoticed by the network administration.

4.4 Wireless Encryption

If the wireless network is encrypted using a strong symmetric encryption algorithm, the wireless traffic is not vulnerable to eavesdropping. However, the algorithms in use must be strong enough resist attacks. AES is considered state of the art in symmetric encryption and currently gives strong protection. However, care must be taken so that keys are managed in a secure manner. If symmetric keys are transported between the peers in an insecure manner, the encrypted traffic itself may be compromised.

4.5 Wired Encryption

Since great emphasis is put on the wireless protection, it is easy to forget that most wired traffic is transported unencrypted. This is not a problem if it is possible to guarantee that no one can access the wires. However, since the wires are often available in the stores, and since employees are a common source of attacks, this assumption can lead to devastating consequences. Wired traffic should always be encrypted.

Control Mechanisms	Threats										
	Rogue devices	Man-in-the-middle	Masquerading APs	Wireless eavesdropping	Wired eavesdropping	Future vulnerability	Spoofting	Stored data in safeguards	Lost or stolen device	Worldwide DoS	Hijacking - legacy protocol
Server side authentication	3	3	3								
Strong user authentication	3						2	3	2		
System authentication (PSK)							1		1		
Wireless encryption			3								2
Wired encryption				3							3
Integrity protection						3	3				3
Segmentation - packet filtering							2		2		
Segmentation - user authenticated							3		3		
Rogue device detection	2										
Publicly reviewed security protocols					2						
Authorization and Audit Log							2	2	2		
Policies and Training	2							2			

Table 1. Control mechanisms in relation to potential security threats in a retail environment. Each intersection indicates the level of risk mitigation/protection of the given control mechanism. 3 = strong protection, 2 = acceptable protection, 1 = weak protection, and an empty cell indicates no protection or risk mitigation of the given threat.

4.6 Integrity Protection

Protection of the integrity of transmitted traffic (both wired and wireless) can be accomplished by using message authentication codes (MACs). If such a mechanism is implemented in a security protocol, spoofing and hijacking can be avoided, since the receiver can verify that the data has not been altered during transmission.

4.7 Segmentation, Packet Filtering

In Figure 2, the network was shown segmented into protected and unprotected parts using a firewall. The firewall then decides what types of packets are allowed to pass. This kind of safeguard is commonly installed at stores, even if it is not true for all environments. However, the use of segmentation using firewalls only, can give a false feeling of security, since some traffic is still allowed to pass. For example, if legacy protocols are allowed to pass through the firewall, attacks such as session hijacking could render the firewall protection useless.

4.8 Segmentation, User Authentication

With this control mechanism, arbitrary packets selected on just protocol types are not allowed to pass through the firewall. Instead, a session that is authenticated using a strong user authentication mechanism is used, so only authenticated users are allowed to transmit data. This control mechanism together with integrity protection and server-side authentication enables the possibility to achieve *perimeter security*, where only authenticated users can access the private part of the network.

4.9 Rogue Device Detection

If a rogue device, such as a rogue access point, is available on the network, this device can illegally be transmitting data using another wireless network. Control mechanisms are available that detect these APs using wireless sniffers and probes installed at the store. The challenge for these kinds of control mechanism is to not only detect but also to decide if a specific access point is rogue or not. Moreover, to be complete, all potential kinds of communication media need to be covered, including normal cellular communication links such as GSM.

4.10 Publicly Reviewed Security Protocols

In Section 3.6 we described how future possible vulnerability in existing safeguards can lead to un-

expected security threats in a previously secure infrastructure. All safeguards have vulnerabilities, regardless if they are known or unknown. However, if a control mechanism and thus the safeguard is based on publicly reviewed security protocols, it is less likely that the vulnerabilities will pass unnoticed compared to if the protocol was developed within an organization or in a closed community.

4.11 Authorization and Audit Log

By enabling not only strong user authentication but also an authorization mechanism, the enterprise can implement need-to-know privileges (giving each user the least possible privileges). Hence, even if an attacker gains access to a user account, he will only be allowed to perform the actions available to this particular user. Moreover, if an audit log is available, actions performed by an intruder can be traced, which does not prevent the intrusion but may mitigate the risk of the same breach occurring again.

4.12 Policies and Training

Finally, by implementing administrative controls, such as constructing and enforcing policies and training, the risk that employees will deploy rogue devices or that existing devices will be lost can be reduced, but of course will not be eliminated. Note that writing security policies and performing security awareness training should not be considered as an optional control mechanism, but something that all retail enterprises do.

5. Safeguard Technologies

The control mechanisms described in the previous section mitigate and give various levels of protection against different threats. These control mechanisms are not normally implemented in isolation, but are usually part of a commercial product that implements a certain safeguard technology.

This section gives an overview of the most common categories of safeguards that can give protection to a retail environment. Table 2 shows how these safeguard technologies relate to the earlier described control mechanisms and security threats. It also outlines a number of business benefits and convenience features that are important to consider when comparing different safeguard technologies.

	Safeguards									
	Wired VPN	Mobile VPN	Firewall	WEP	Dynamic WEP	WPA-TKIP-PSK	WPA2-CCMP-PSK	WPA2-CCMP-EAP	Sensors	
Control Mechanisms										
Server-side authentication	3	3			3	2		3		
Strong user authentication	3	3			3			3		
System authentication (PSK)	3	3		2	2	3	3			
Wireless encryption	3	3		1	1	2	3	3		
Wired encryption	3	3								
Integrity protection	3	3				2	3	3		
Segmentation, packet filtering			3							
Segmentation, user authentication	3	3								
Rogue device detection									3	
Publicly reviewed security protocols	3	3				1	3	3		
Authorization and audit log	2	2			2	1	1	2	2	
Policies and training										
Business Benefits and Convenience Features										
Hardware future proof	3	3		2	2	2	2	2		
Network future-proof	3	3								
WAN support	3	3								
Session resume		3		2	2	2	2	2	N/A	
Data compression	2	3							N/A	
Threats										
Rogue devices	3	3			2	2		2	2	
Man-in-the-middle	3	3			2	2		2		
Masquerading APs	3	3			3	2		3		
Wireless eavesdropping	3	3		1	1	2	3	3		
Wired eavesdropping	3	3								
Future vulnerability in safeguard	2	2				1	2	2		
Spoofing	3	3		1	2	2	3	3		
Stored data manipulation	3	3	2	1	1	2	2	2	2	
Lost or stolen device	3	3			3		2	3	2	
World-wide DoS	3	3	2		2		2	2	2	
Hijacking - legacy protocol	3	3		1		2	2	2		

Table 2. Control mechanisms, business benefits, convenience features, and threats in relation to available safeguard technologies. The intersections indicate to which level a safeguard includes a particular control mechanism, business benefit, or convenience feature, where 3 = full, 2 = partial, and 1 = marginal support. The lower part shows the security threats described in Section 3 in relation to the safeguards. The intersections outline a summary of the level of protection a specific safeguard gives to a threat, where 3 = strong protection, 2 = acceptable protection, 1 = weak protection. An empty (white) cell indicates no protection or risk mitigation of the given threat or that no relation exists between a safeguard and a control mechanism.

5.1 Wired VPN

A wired VPN is commonly based on the IP Security (IPSec) standard, which was originally designed specifically for wired VPNs. The IPSec protocol operations at the network layer in the OSI model. The protocol supports mutual authentication and can operate in two distinct modes: transport mode and tunneling mode. In the former, only payload data is encrypted and authenticated, while in the latter the entire IP packet (both data and message header) is encrypted and authenticated.

5.2 Mobile VPN

Mobile VPN has generally the same security functionality as wired VPN, in terms of mutual authentication, secure key exchange (using RSA) and strong symmetric encryption (AES). However, depending on the vendor used, the actual protocol used could be TLS, SSL, or WTLS, or some proprietary protocol. It should be noted that if the product is using a nonstandard publicly reviewed protocol, there might be vulnerabilities in the protocol due to design flaws.

The main aspect that differentiates mobile VPNs from wired VPNs (such as IPSec VPNs) is the convenience of use in a retail environment. In particular,

the ability to resume sessions is vital, since devices are often hibernated due to limited battery lifetime, or a device goes out of the coverage area, or because of network switching. If session resumption is not available in the safeguard, the user needs to log in each time the device hibernates or goes out of coverage.

Another property that distinguishes wired and mobile VPNs from other wireless security protocols such as WPA2 is the ability to communicate not only over LAN but also over *wide area networks (WANs)*, e.g., the Internet. This includes not only wired networks, but also *wireless WAN (WWAN)* technologies, such as UMTS/3G, EV-DO, and WiMax. At the bottom of Figure 2, an example is shown of how a store manager may connect directly to headquarters using a remote VPN. By using this path via the Internet, instead of going through the store, a manager is given greater flexibility to work while traveling or from home.

5.3 Firewall

Firewalls are powerful safeguards that can consist of different functionality. The earliest generation of firewalls could only handle simple packet filtering, while today almost all modern firewalls manage stateful inspections and certain levels of *application-layer firewalls*, or *proxy-based firewalls*. However, although this safeguard is powerful and addresses some sorts of DoS attacks, it does not help against man-in-the-middle attacks, rogue devices, or wireless and wired eavesdropping. Hence, a firewall should not be seen as the only security safeguard, but one component that can be used in conjunction with (for example) a VPN.

5.4 WEP

The *wired equivalent protocol (WEP)* was the first attempt to provide a security-layer protection to wireless networks. However, due to flaws in both the encryption and integrity checking part of the protocol, WEP is now considered non-secure, since it can be broken within minutes by downloading and executing tools freely available on the Internet. Unfortunately, WEP is still used in many enterprises, providing a false sense of security.

5.5 Dynamic WEP

One of the flaws in WEP is its ability to provide only system authentication and not user authentication. During the years before an alternative to WEP appeared, vendors started to create propriety products where WEP was combined with the 802.1X standard, which is used for authentication. This approach of combining WEP with 802.1X [8] is com-

monly called “*Dynamic WEP*.” Here, the ability of mutual authentication in 802.1X in combination with dynamic key management reduces the exposure to key attacks. However, the approach is still vulnerable to other attacks such as replays [12].

5.6 WPA-TKIP-PSK

To overcome the vulnerability of the WEP protocol, in October 2003 the Wi-Fi Alliance launched a new protocol called Wi-Fi Protected Access (WPA), which is based on drafts of the IEEE 802.11i specification [5]. WPA can be configured in a personal mode. The encryption algorithm used is called TKIP, which is an improvement of the WEP algorithm, where still RC4 is used as the encryption algorithm. Message integrity checks are performed by the protocol message integrity code (MIC). In the personal mode, all devices are configured with a pre-shared key (PSK) instead of 802.11X/EAP. This enables a simple setup, but the whole security solution breaks down if a device is lost or stolen, since dictionary attacks can then be applied on the pre-shared key. The TKIP protocol is considered a weak algorithm, even though it is not yet broken. Since it is built on technology derived from WEP, it is not unlikely that cryptographic attacks will in the future be discovered for the WPA protocol.

5.7 WPA2-CCMP-PSK

The TKIP protocol was designed so that only software upgrades were needed when upgrading from WEP. However, to enable stronger encryption algorithms and better integrity checks, more computation power is normally needed. Hence, the next generation, called WPA2 (based on IEEE 802.11i), includes the ability to use *Counter-Mode/CBC-MAC Protocol (CCMP)*, which is the new symmetric encryption protocol replacing TKIP. CCMP uses advanced encryption standard (AES) for both encryption and message integrity. In this configuration, WPA2 and PSK are used for authentication. Note that legacy devices can seldom be upgraded to WPA2, due to its increased demand on computational resources.

5.8 WPA2-CCMP-EAP

If the product is configured in WPA2’s enterprise mode, authentication is conducted using 802.1X and EAP. This enables the possibility to perform mutual authentication and support for PKI infrastructure. This mode of WPA2 enables strong authentication, mutual authentication, and a strong encryption and integrity protection for wireless traffic. However, this safeguard is only valid for wireless traffic and cannot be implemented on the wired part of the net-

work. Therefore, this solution is not network agnostic, since the security protocol is strongly connected to the wireless communication standards. Hence, this safeguard is not capable of securing a wireless wide area network (WWAN), such as UMTS/3G and EV-DO.

5.9 Sensors

Finally, sensors can be used for intrusion detection and detection of rogue devices and APs. However, even if these safeguards detect and report some rogue devices and access points, they cannot guarantee that a rogue device that is not detected does not do any harm.

In contrary to technologies such as VPNs and WLAN security protocols (e.g. WPA2), sensors do not prevent an attack using access control mechanisms. Instead, the main purpose is to discover an intrusion, to report it, and to react rapidly. Although e.g. VPNs also mitigates some of the threats generally targeted for sensors (e.g. rogue APs), these safeguards should not be seen as competing technologies. Instead, these solutions may be used in parallel for maximal risk mitigation.

6. Standards, Laws, and Regulations

In the following section, some of the most important standards, laws, and regulations that affect a retail enterprise's security policy and implementation work are discussed.

6.1 PCI Data Security Standard

One of the most important standards relating to retail security work is the *payment card industry (PCI) data security standard* [10]. This standard includes 12 informally described requirements, divided into six different areas. Several important threats and countermeasures discussed earlier in this paper are also requirements in this standard. Hence, many of the control mechanisms described are actually enforced by PCI's data security standard, if the retail enterprise wants to use credit cards in its business.

However, there are several areas where the specification are vague and open to interpretation. For example, it states that WEP can be used in a retail environment, *if* it is used in conjunction with other safeguards, such as IPSEC, TLS, or WPA.

Other parts put stronger requirements on authentication, for example, that user authentication requires at least one factor on the LAN and at least two factors for remote access. Therefore, WPA-TKIP-PSK and WPA-CCMP-PSK would not be legal configurations according to PCI. Moreover, the

standard requires the ability to implement authorization, giving a tool to enforcing a need-to-know basis.

If retailers use the strongest safeguard technologies discussed in this paper, they will be compliant with the PCI standard. However, the converse is not true; merely by following the PCI standard, not all of the threats discussed in this paper will be covered. In particular, wired networks are not discussed in the PCI standard, and failure to require mutual authentication may make the network vulnerable to both man-in-the-middle attacks and rogue devices.

6.2 Sarbanes-Oxley and HIPAA Compliance

Today, several laws and regulations impose additional security requirements on the retail industry. The *Health Insurance Portability and Accountability Act (HIPAA)* is a recent federal regulation that has put into place requirements on transmitting and storing medical information and health care data. Any retail store offering pharmacy services must comply with HIPAA. If a company violates the standards stated by HIPAA, it may be given large monetary penalties, even if the noncompliance was the result of a mistake.

The *Sarbanes-Oxley Act* (also called *SOX*) from 2002 is a U.S. federal law that is a reaction to a number of accounting scandals. The law does not explicitly state any requirements on information security, but puts great responsibility on CIOs and IT departments to efficiently control their environments. By following good information security practice, analyzing, and managing threats in the environment, such as the ones described in this paper, the fundamental security infrastructure should be compliant to the Sarbanes-Oxley Act.

7. Conclusions

Information system security is a critical area in modern retail network environments, due to the high proportion of business-critical software systems within the stores. Important information and system assets need protection from the loss of confidentiality, integrity, and availability. Important assets that are especially sensitive to security threats are credit card information, private customer records, and the risk that business-critical systems such as POS controllers could go out of service.

Several of the threats the retail environment are facing are not covered by standard technologies offered on the market. For example, the threat of disclosing wireless information is not covered by WEP technology due to its weak protocol, and successor technologies such as WPA and WPA2 only handle the wireless part of the network infrastructure.

Wired threats and rogue devices cannot be covered by these safeguards.

VPNs, on the other hand, do cover both the wireless threats and the wired ones, using one solution for all devices. By regarding all devices on the network as remote clients, the same access control mechanism can be used; including mutual authentication. The solution is network agnostic, enabling the possibility to change wireless and wired infrastructure without the need to reinvest in a new security solution.

Traditional wired VPNs using IPSec are efficient on pure wired LANs, but lack the possibility for session resumption, which is an important aspect in a retail environment. Session resumption is one of the features that distinguish mobile VPNs from IP-Sec VPNs. Moreover, mobile VPNs can achieve better performance in a wireless environment, due to lossless data compression.

Taken together, strong wireless protocols (e.g., WPA2 with CCMP) can achieve good protection against wireless threats. However, to also cover wired threats and rogue devices, VPNs should be used as safeguards. Finally, mobile VPNs share the same security protection mechanisms as traditional VPNs, but also include support for convenience aspects such as the capability to resume sessions.

Be Fearless and Unleash the Power of Wireless

To find out how Columbitech can help you to secure your wireless infrastructure and ensure PCI compliance, visit www.columbitech.com

+1 212 946 4820 (U.S. Sales Office)
 + 46 8 556 08 100 (European Headquarters)
info@columbitech.com

Acronyms

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AP	Access Point
CCMP	Counter-Mode/CBC-MAC Protocol
DES	Data Encryption Standard
DoS	Denial-of-Service
DOS	Disk Operating System
EAP	Extensible Authentication Protocol
FW	Firewall
GSM	Global System for mobile communication
HMAC	Hashed Message Authentication Code
HIPAA	Health Insurance Portability and Accountability Act
IPSec	Internet Protocol Security
ISP	In Store Processor
LAN	Local Area Network
MAC	Message Authentication Code <i>or</i> Media Access Control
MIC	Message Integrity Code
OTP	One-Time Password
OSI	Open System Interconnection Basic Reference Model
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PoE	Power over Ethernet
POS	Point of sale
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RSA	Rivest, Shamir, and Adleman (<i>asymmetric encryption algorithm</i>)
SSL	Secure Socket Layer
SSO	Single Sign-On
TLS	Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTLS	Wireless Transport Layer Security

References

- [1] B. Aboba et.al. (2006). "Extensible Authentication Protocol (EAP)." RFC 3748.
- [2] T. Dierks and E. Rescorla. (2006). "The Transport Layer Security (TLS) Protocol. Version 1.1." RFC 4346.
- [3] DSW (2005). "Press Releases Customer Alert – April 18, 2005." Available from: <http://www.dswshoe.com/pressRelease.jsp> [Last accessed November 27, 2007].
- [4] Alan O. Freier, Philip Karlton, and Paul C. Kocher. (1996). "The SSL Protocol Version 3.0." Transport Layer Security Working Group, INTERNET-DRAFT.
- [5] IEEE. (2004). "IEEE Std 802.11i™-2004." ISBN 0-7381-4074-0. The Institute of Electrical and Electronics Engineers, Inc. New York, USA.
- [6] IEEE. (2000). "IEEE Std 802.11a-1999 (R2003)." The Institute of Electrical and Electronics Engineers, Inc. New York, USA.
- [7] IEEE. (2000). "IEEE Std 802.11b-1999 (R2003)." ISBN 0-7381-1812-5. The Institute of Electrical and Electronics Engineers, Inc. New York, USA.
- [8] IEEE Computer Society (2004). "IEEE Std 802.1X-2004." The Institute of Electrical and Electronics Engineers, Inc. New York, USA
- [9] Dawn Kawamoto. (2007). "TJX says 45.7 million customer records were compromised." CNET News.com, March 29, 2007. Available from: http://www.news.com/TJX-says-45.7-million-customer-records-were-compromised/2100-1029_3-6171671.html [Last accessed November 27, 2007].
- [10] PCI Security Standards Council. (2006). "Payment Card Industry (PCI) Data Security Standard." Version 1.1. Release September 2006. Available from: <https://www.pcisecuritystandards.org/>.
- [11] Jaikumar Vijayan. (2005). "Update: Scope of credit card security breach expands – HSBC Bank is just one of several institutions whose customers may be affected." Computerworld Security, April 15, 2005. Available from: <http://www.computerworld.com/securitytopics/security/story/0,10801,101101,00.html> [Last accessed November 27, 2007].
- [12] Wi-Fi Alliance (2003). "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks," April 29, 2003, Available from: <http://www.wi-fi.org/> [Last accessed November 22, 2007]
- [13] Wi-Fi Alliance. (2003). "Enterprise Solutions for Wireless LAN Security." February 6, 2003. Available from: <http://www.wi-fi.org/> [Last accessed November 22, 2007].
- [14] Wi-Fi Alliance. (2005). "Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise." March 2005. Available from: <http://www.wi-fi.org/> [Last accessed November 22, 2007].
- [15] Wireless Application Protocol Forum. (2001). "Wireless Transport Layer Security." Version 06-Apr-2001