# Information about this New Manual

## New Manual


## Contents

This manual describes the risks associated with the use of wireless LANs, and provides some basic guidelines to mitigate the security risks introduced by the use of this technology.

Please refer to “Using this Manual” for a complete list of the contents of this manual.

## Billing

MasterCard will bill principal members for this document in printed format. Please refer to the *MasterCard Consolidated Billing System Manual* for billing-related information.

## Questions?

If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. Please refer to “Using this Manual” for more contact information.

## MasterCard is Listening...

Please take a moment to provide us with your feedback about the material and usefulness of the *Wireless LANs – Security Risks and Guidelines* using the following e-mail address:

`doc@mastercard.com`

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.
Wireless LANs – Security Risks and Guidelines

December 2004
Using this Manual

Purpose...................................................................................................................1
Audience.................................................................................................................1
Overview ................................................................................................................1
Excerpted Text .......................................................................................................2
Language Use .........................................................................................................2
Times Expressed.....................................................................................................2
Revisions.................................................................................................................3
Related Information...............................................................................................3
Support ...................................................................................................................5
  Member Relations Representative .................................................................5
  Regional Representative.................................................................................6
Terminology ...........................................................................................................6

Chapter 1 Introduction

Overview ................................................................................................................1-1

Comparison of Wireless Technologies...............................................................1-2
  802.11 – Wi-Fi for Computers and Laptops ......................................................1-3
  Bluetooth – Short-Range Data for Phones and PDAs ......................................1-4
  GPRS – Long-Range Data for Phones and PDAs.............................................1-5
Table of Contents

Chapter 2  Risks of Wi-Fi LANs

Introduction ......................................................................................................... 2-1
  Wi-Fi Security .................................................................................................. 2-1
Access Control .................................................................................................... 2-2
Data Confidentiality .......................................................................................... 2-3
Data Integrity ..................................................................................................... 2-4

Chapter 3  WLAN Guidelines

Basic WLAN Guidelines ...................................................................................... 3-1
  WLAN Implementation ................................................................................... 3-1
  WEP Encryption ............................................................................................ 3-1
  WLANs that use WPA .................................................................................... 3-2
  Related Documents ....................................................................................... 3-2
Conclusions ......................................................................................................... 3-3
Using this Manual

This chapter contains information that helps you understand and use this manual.

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Excerpted Text</td>
<td>2</td>
</tr>
<tr>
<td>Language Use</td>
<td>2</td>
</tr>
<tr>
<td>Times Expressed</td>
<td>2</td>
</tr>
<tr>
<td>Revisions</td>
<td>3</td>
</tr>
<tr>
<td>Related Information</td>
<td>3</td>
</tr>
<tr>
<td>Support</td>
<td>5</td>
</tr>
<tr>
<td>Member Relations Representative</td>
<td>5</td>
</tr>
<tr>
<td>Regional Representative</td>
<td>6</td>
</tr>
<tr>
<td>Terminology</td>
<td>6</td>
</tr>
</tbody>
</table>
Purpose

The purpose of this document is to raise the awareness among members regarding the risks associated with the use of wireless LAN technologies.

Additionally this document provides high-level guidelines for the secure use of wireless LAN technologies in order to mitigate the associated risks.

Audience

This manual is intended for acquiring and issuing members, and their respective agents, that have deployed, or that plan to deploy, wireless LAN technology.

Overview

The following table provides an overview of this manual:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>A list of the manual’s chapters and sections. Each entry references a chapter and page number.</td>
</tr>
<tr>
<td>Using this Manual</td>
<td>A description of the manual’s purpose and its contents.</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>Introduces the various wireless LAN technologies.</td>
</tr>
<tr>
<td>2 Risks of Wi-Fi LANs</td>
<td>Describes the risks associated with ‘Wi-Fi’ wireless LANs.</td>
</tr>
<tr>
<td>3 WLAN Guidelines</td>
<td>Offers basic guidelines to mitigate the security risks introduced by the use of WLAN technology.</td>
</tr>
</tbody>
</table>
Excerpted Text

At times, this document may include text excerpted from another document. A note before the repeated text always identifies the source document. In such cases, we included the repeated text solely for the reader’s convenience. The original text in the source document always takes legal precedence.

Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in *Merriam-Webster’s Collegiate Dictionary*. MasterCard is incorporated in the United States and publishes in the United States. Therefore, this publication uses U.S. English spelling and grammar rules.

An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

Times Expressed

MasterCard is a global company with locations in many time zones. The MasterCard operations and business centers are in the United States. The operations center is in St. Louis, Missouri, and the business center is in Purchase, New York.

For operational purposes, MasterCard refers to time frames in this manual as either “St. Louis time” or “New York time.” Coordinated Universal Time (UTC) is the basis for measuring time throughout the world. You can use the following table to convert any time used in this manual into the correct time in another zone:

<table>
<thead>
<tr>
<th></th>
<th>St. Louis, Missouri USA</th>
<th>Purchase, New York USA</th>
<th>UTC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Central Time</td>
<td>Eastern Time</td>
<td></td>
</tr>
<tr>
<td><strong>Standard time</strong></td>
<td>9:00</td>
<td>10:00</td>
<td>15:00</td>
</tr>
<tr>
<td>(last Sunday in October to the first Sunday in April a)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Daylight saving time</strong></td>
<td>9:00</td>
<td>10:00</td>
<td>14:00</td>
</tr>
<tr>
<td>(first Sunday in April to last Sunday in October)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a For Central European Time, last Sunday in October to last Sunday in March.
Revisions

MasterCard will periodically issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a “Summary of Changes” describing how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appears to the right of each revision marker.

Occasionally, we may publish revisions or additions to this document in an Operations Bulletin or other bulletin. Revisions announced in another publication, such as a bulletin, are effective as of the date indicated in that publication, regardless of when the changes are published in this manual.

Related Information

For further information on IEE 802.11 standards, and related security issues, please refer the following:


Using this Manual

Related Information

  URL: [http://www.airdefense.net/eNewsletters/May03/feature.htm](http://www.airdefense.net/eNewsletters/May03/feature.htm)

  URL: [http://documents.iss.net/whitepapers/wireless_LAN_security.pdf](http://documents.iss.net/whitepapers/wireless_LAN_security.pdf)


  URL: [http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html](http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html)

- **WPA Overview**, WiFi Alliance. URL: [http://www.wifi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf](http://www.wifi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf)

  URL: [http://www.extremetech.com/article2/0,3973,1073,00.asp](http://www.extremetech.com/article2/0,3973,1073,00.asp)


Support

Please address your questions to the Customer Operations Services team as follows:

Phone: 1-800-999-0363 or 1-636-722-6176
        1-636-722-6292 (Spanish Language support)

Fax: 1-636-722-7192

E-mail: Canada, Caribbean, and U.S. member_support@mastercard.com
        Asia/Pacific apms@mastercard.com
        Europe css@mastercard.com
        South Asia/Middle East/Africa emeaap@mastercard.com
        Latin America (Spanish Language support) lagroup@mastercard.com

Address: MasterCard International Incorporated
         Customer Operations Services
         2200 MasterCard Boulevard
         O'Fallon MO 63366-7263
         USA

Telex: 434800 answerback: 434800 ITAC UI

Member Relations Representative

Member Relations representatives assist U.S. members with marketing inquiries. They interpret member requests and requirements, analyze them, and if approved, monitor their progress through the various MasterCard departments. This does not cover support for day-to-day operational problems, which the Customer Operations Services team addresses.

To find out who your U.S. Member Relations representative is, contact your local Member Relations office:

Atlanta 1-678-459-9000
Chicago 1-847-375-4000
Purchase 1-914-249-2000
San Francisco 1-925-866-7700
Regional Representative

The regional representatives work out of the regional offices. Their role is to serve as intermediaries between the members and other departments in MasterCard. Members can inquire and receive responses in their own language and during their office’s hours of operation.

To find out the location of the regional office serving your area, call the Customer Operations Services team at:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish Language support)

Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>A family of IEEE standards for wireless LANs first introduced in 1997.</td>
</tr>
<tr>
<td>802.11i</td>
<td>An IEEE standard which provides robust security for wireless LANs; it supports dynamic negotiation of authentication and encryption algorithms.</td>
</tr>
<tr>
<td>802.1X</td>
<td>An IEEE security protocol for robust authentication for wireless LANs that adhere to the 802.11 standard. It relies on the Extensible Authentication Protocol (EAP, an extension to the PPP protocol that enables a variety of authentication protocols to be used) to pass messages to any of a variety of authentication servers such as Kerberos or RADIUS.</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers, see <a href="http://www.ieee.org">www.ieee.org</a></td>
</tr>
</tbody>
</table>
| MAC   | 1. Medium Access Control – a unique serial number assigned to network devices.  
2. Message Authentication Code – a number computed from the contents of a message, used to authenticate the message. |
| NIST  | National Institute of Standards & Technology is the standards-defining agency of the U.S. Government, formerly the National Bureau of Standards. See www.nist.gov |
| SSID  | Service Set Identifier. The name assigned to a wireless Wi-Fi network. All wireless devices must use this case-sensitive name (a text string up to 32 bytes long) in order to communicate. |
### Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Virtual Private Network, a private network that is configured within a public network (e.g., the Internet) in order to take advantage of the economies of scale and management facilities of large networks.</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy – an 802.11 security protocol for wireless networks.</td>
</tr>
<tr>
<td>WLAN</td>
<td>A wireless network uses radio waves, microwaves, or both to communicate and transmit data between and among computers and devices equipped with wireless capability. Wired networks, on the other hand, use physical cable connections. Wireless LAN refers to the 802.11 family of specifications developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). These standards specify an over-the-air interface between a wireless client and a base station, or between two wireless clients. It includes standards such as 802.11b (more popularly known as Wi-Fi) as well as 802.11a and 802.11g which specify the behavior of wireless networks operating at varying frequencies.</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access – a specification of security enhancements to the IEEE 802.11b specifications derived from the IEEE 802.11i draft. It was designed to address security vulnerabilities found in the Wired Equivalent Privacy protocol (WEP) and will be forward compatible with the 802.11i standard when it is finalized.</td>
</tr>
</tbody>
</table>
Introduction

This chapter provides a general overview of this document, and introduces the various wireless LAN technologies.

Overview .............................................................................................................1-1

Comparison of Wireless Technologies ...............................................................1-2
  802.11 – Wi-Fi for Computers and Laptops .....................................................1-3
  Bluetooth – Short-Range Data for Phones and PDAs..................................1-4
  GPRS – Long-Range Data for Phones and PDAs ...........................................1-5
Overview

In an effort to be more flexible about working arrangements and to save money on infrastructural wiring, many organizations are deploying – or are considering deploying – wireless local area networks (WLANs). WLANs allow employees to work in a variety of workspaces and can enable networking in areas that wires cannot easily serve. The technology is new, inexpensive, and relatively easy to set up. When implemented with commodity hardware, WLANs are, however, very difficult to secure. Members and member service providers (MSPs) are likely to consider wireless technology because it fosters easy and convenient computing. Individual merchants are also likely to consider deploying wireless technology for the same reasons.

WLANs extend an organization’s LAN into areas that attackers can easily reach, without even being inside the building or visible to corporate security staff. WLANs allow data to leave the organization in an uncontrolled manner, bypassing network security controls and auditing, thus creating significant new risks for the organizations that deploy them.

The network protections offered by today’s WLAN equipment are typically very weak, and are easily circumvented or compromised. Data available to any node on a wireless network is also threatened by attackers and is very difficult to keep secure. Inexpensive commodity hardware exists that can intercept the signals up to one mile (1600m) away, map the available network, and analyze security measures. Free software tools allow relatively unskilled attackers to gather data and attempt to break cryptographic protections on most WLANs.

Warning For the above reasons, it is critical that WLANs are not used to transmit sensitive information, such as cardholder account information. When data is transmitted over a WLAN, it should be secured using the best practices available.

Various wireless LAN technologies exist today. Those that are based upon the IEEE 802.11 standards (so-called ‘Wi-Fi’ networks) are the most important to understand because of their relatively long range, ease of use, and inexpensive prices. They are the most likely to be established by both unauthorized employees and inexperienced corporate IT staff alike. They offer a broader set of risks to broader classes of potential attackers than the other kinds of wireless networks.

This document therefore focuses on the dangers of 802.11 WLANs, aims to raise awareness of the security risks associated with WLANs, and provides basic guidance on how to mitigate those risks.
Comparison of Wireless Technologies

There are other kinds of wireless devices apart from the standard 802.11-based general-purpose WLAN, popular with personal computers. All of them create similar risks. This section describes the three principal wireless technologies in use today, each of which is capable of accessing the Internet, without the use of wires or cables:

- IEEE 802.11
- Bluetooth
- GPRS

Companies are most likely to consciously deploy 802.11 networks and thus 802.11 WLANs require the most immediate guidance. However, one cannot overlook the other types of wireless data interchange, as they too allow data to flow in and out of the corporate network.

All three wireless technologies create unique risks to an organization’s network infrastructure. Bluetooth and GPRS technologies are primarily a concern for insider-based attacks. They allow insiders to create unregulated tunnels to the outside. There is still, however, the possibility that a mobile phone or PDA could be compromised in some way while outside the corporate LAN and then it could launch an attack after being brought into the corporate environment. Such an attack is still very uncommon with today’s technology, but it is becoming increasingly possible with every passing month.

Refer to “Related Information” for additional information about WLAN risks.
802.11 – Wi-Fi for Computers and Laptops

Most people initially think of ‘Wi-Fi’ when they think ‘wireless.’ Wi-Fi is an industry interoperability standard for wireless networking devices, and is based on the IEEE standards 802.11b or 802.11g.

The adoption of Wi-Fi networking has exploded in recent years. The installed base has jumped from thousands of nodes in 1999, to millions of nodes in 2004. You can purchase a wireless adapter, for your desktop or laptop computer, for as little as USD 50 at any major office supply or computer store. Access points that allow a number of wireless nodes to join the wired network are equally inexpensive. This is significant to any networking infrastructure because it means that employees can easily afford to set up their own base station and connect the corporate LAN to a wireless LAN, without the knowledge or approval of their organization’s IT staff.

Wi-Fi networks create arguably the most significant risks. They are more likely to be established by an organization’s IT staff to provide intentional (and unintentional) access to sensitive data. Wi-Fi access points create infrastructure that is equally usable by both legitimate and illegitimate users alike. Unlike Bluetooth, the Wi-Fi signal extends well beyond the walls of the office building.

The cryptographic protection provided by the first generations of Wi-Fi equipment is weak at best. Furthermore, attack tools that automate the discovery and compromising of Wi-Fi networks are free, readily available, and mature.

This type of WLAN is described in more detail in the remaining chapters.
Bluetooth – Short-Range Data for Phones and PDAs

Bluetooth personal area networking appears in laptop computers, desktop computers, as well as PDAs and mobile phones. It provides the ability for devices to interconnect over relatively short distances, and exchange data.

Bluetooth technology is somewhat similar to 802.11 in its use of the same frequency spectrum. However, its security architecture and use of cryptography is much more robust, making it a more secure method of transmitting data over the air. It is often overlooked when considering wireless security because it is not well known, nor is it as commonly included on personal computers as 802.11. Bluetooth is found, however, on devices such as mobile phones and PDAs. Corporate IT staff have little or no direct control over such devices, since they are often purchased and maintained by individual employees. You can use Bluetooth to link a mobile phone to a laptop, while the cellular technology in the phone allows it to act as a conduit to the Internet. Suddenly, an innocuous mobile phone is an invisible tunnel to the Internet from the local LAN. It silently bypasses all networking infrastructure security controls and policies.

Unlike 802.11 devices, which can easily be discovered through various ‘sniffing’ techniques, Bluetooth devices that are not explicitly ‘discoverable’ are very difficult to detect.

Small devices, such as PDAs and mobile phones, are increasingly using general-purpose operating systems such as Symbian, Windows CE, and PalmOS. Like other complex operating systems, these embedded systems have had exploitable vulnerabilities. Because they are also Internet capable, embedded wireless devices that run general-purpose operating systems create the same kinds of risks as common laptop PCs. The low incidence of exploitation on these devices can be attributed to the scarcity of hackers creating exploits, not a lack of exploitable conditions. It is only a matter of time before significant, viral attacks are created against mobile embedded devices.

Bluetooth technology also allows devices to talk directly to each other, without any infrastructural support. They can automatically discover each other and communicate simply by being within about 30 feet (10m) of each other. Security settings in Bluetooth can be very strong, but often are weak by default. It is very easy for one device to send malicious data to another. It is often true that devices will share all their data readily with other devices without any authentication. Simply standing near a person’s Bluetooth-enabled phone may be all that is required to download all their contact information, e-mail and any other data stored on that phone.
GPRS – Long-Range Data for Phones and PDAs

GPRS is a standard that leverages existing mobile phone technology infrastructure to provide digital data service to portable devices, including PDAs and mobile phones. Connections to a laptop or desktop computer from those PDAs and mobile phones, using something simple like a Universal Serial Bus (USB) cable can leverage that GPRS technology to provide an alternate path to the Internet. Again, this wireless technology permeates virtually all office buildings and completely bypasses any existing network security infrastructure and controls.

Unlike Bluetooth, GPRS does not provide direct device-to-device connectivity. In that regard, it is safer. It still, however, provides an alternate path to the Internet that is unregulated and beyond the control of an organization’s IT staff.
Risks of Wi-Fi LANs

This chapter describes the risks associated with the use of ‘Wi-Fi’ wireless LANs.

Introduction ................................................................. 2-1
Wi-Fi Security ............................................................. 2-1
Access Control ............................................................ 2-2
Data Confidentiality ..................................................... 2-3
Data Integrity ............................................................. 2-4
Introduction

This chapter focuses on the primary weaknesses and resulting risks associated with IEEE 802.11 wireless (Wi-Fi) LANs. These risks can be separated into three categories:

- Access control
- Data confidentiality
- Data integrity

The other wireless technologies are significant, and should also be considered. However, Wi-Fi LANs present the most urgent risks to address for those organizations that currently have little or no guidance on wireless technologies.

Wi-Fi Security

Originally, all Wi-Fi equipment was shipped with a technology called wired equivalent privacy (WEP) as its only security mechanism. It was never intended to be unbreakable, or even as secure as a protocol like ‘Secure Socket Layer’ (SSL). In 2000 and 2001 however, several attacks were published that completely defeated WEP protections. Today, tools exist that automate attacks on WEP protections and compromise networks in real-time.

The common hardware most likely to be deployed often uses WEP by default, and fails miserably in all areas of security. WEP must be considered to be as untrustworthy as the Internet itself, no matter how many security features are enabled.

A new security protocol called Wi-Fi Protected Access (WPA) was standardized in 2003 as a stopgap security measure. It improves on WEP in a variety of vital areas, making it far more resilient to attack. WPA is a temporary industry standard until significantly stronger protections, such as those described in IEEE 802.1x, can be ratified and commercialized. This chapter addresses the dangers of WLANs using either WEP or WPA protection.

Very recent equipment using WPA is more secure, since the cryptographic protections are more robust. They can be deployed securely, but great care is still required. Finding WPA-enabled equipment in the marketplace is not impossible, but requires careful scrutiny of specifications. Furthermore, upgrading to an all-WPA environment can create a burden on IT staff when upgrading existing WEP-based equipment.
Access Control

Virtually all WEP techniques for restricting access can be circumvented. Most rely on the hardware address of the devices in the network and attackers can counterfeit such addresses at will. Unauthorized devices simply masquerade as authorized ones. Some networks use the ability to encrypt data (i.e., the ability to correctly perform WEP cryptography) as an indicator that the device is authorized to operate on the wireless network. Since WEP cryptography is easy to break, this is not a sufficient authorization indicator.

WPA uses a different access control mechanism. It leverages RADIUS, a protocol originally designed for authenticating modem-based Internet access, to authenticate systems more rigorously when they try to connect to the network. Unlike WEP-based access points, wireless access points in a WPA-authenticated network are very restrictive until a system is authenticated. Before a wireless client is authenticated, it is only allowed to communicate with the authentication server. It will be unable to communicate with any other part of the network until it is authenticated. This helps prevent an unauthenticated station from attacking the internal infrastructure. However, unauthenticated stations can still attack authenticated stations or try to impersonate authenticated stations. In WPA networks, such impersonations are harder to perform successfully. While WPA is an improvement over WEP, vulnerabilities are still being discovered, as demonstrated in a recently publicized ‘pass phrase’ flaw in WPA.
Data Confidentiality

Wireless networks must place greater importance on data confidentiality than traditional wired networks. Attacking a wired network requires physical access to the network itself. Physically protecting the corporate LAN infrastructure is relatively straightforward, and is well understood by existing IT staff. The signals from wireless access points however, can be picked up well outside the walls of the building. They can be received in the parking lot, in an adjacent building, or perhaps from a rooftop several blocks away.

Furthermore, the data that is transmitted can be stored by an adversary and analyzed later. Essentially, an attacker can sit unnoticed up to a mile (1600m) away from the company, silently receiving network transmissions. An attacker can store received data and attempt to crack that data at their leisure. If successful in compromising the network’s encryption once, an attacker may be able to decrypt subsequent data transmissions in real time.

WEP is trivial to break, and busy WEP-based Wi-Fi networks can be broken in a matter of hours using readily available, commodity PC hardware. For this reason, wireless networks that rely on WEP for data confidentiality must never transmit sensitive information. WEP-protected networks should use encryption at higher protocol levels, such as SSL and HTTPS. There have been documented attacks against SSL and HTTPS protocols, including ‘man-in-the-middle’ attacks. Thus, using these encryption protocols over WEP does not eliminate the risk of using wireless. It merely reduces the risk.

By contrast, WPA encryption is far more difficult to break. It is more resilient to brute-force attacks against the WPA encryption key. Even though it is not unbreakable, the designers of WPA added ‘countermeasures’ to help detect brute-force attacks on the wireless network, and delay them.

Wireless networks using WPA are better off than those using WEP. Despite the substantially improved security of WPA, encryption should be used at higher layers in the protocol stack in order to offer appropriate protection to sensitive information. Even with WPA, the amount of sensitive information allowed to traverse the wireless LAN should be as limited as possible.

Equipment supporting a robust WPA infrastructure is only now becoming available on the market. It is highly likely that any organization deploying wireless technology will be using all WEP or a mixture of WEP and WPA. Those that have a significant existing infrastructure probably use all WEP-based protections.
Data Integrity

Given how easy it is to break WEP protections, there is an additional risk that data can be intercepted and modified in real time. So-called ‘man-in-the-middle’ attacks are the classic attack involving data interception with the opportunity to modify data as it passes by. There are a number of possible ‘man-in-the-middle’ attacks that are unique to WLANs.

It is simple for an attacker to learn the identifier for the WLAN (its ‘Service Set Identifier’, or SSID) and then set up an access point advertising the same SSID. Devices may associate with this rogue access point, which can selectively relay some or all packets on to the real network. Having interposed itself between the legitimate stations and the legitimate network, the rogue access point can choose to selectively modify, or suppress, messages that it is relaying.

Assuming that robust WPA-enabled equipment can be found, and infrastructure can be installed to support it, data integrity is significantly improved by using WPA. The cryptography that is used in WEP is still used by WPA, but a variety of modifications makes it more robust. For example, message integrity features in WEP could be forged or circumvented. WPA message integrity methods are more rigorously protected by cryptography.
WLAN Guidelines

This chapter offers basic guidelines to mitigate the security risks introduced by the use of WLAN technology.

Basic WLAN Guidelines ......................................................................................3-1
WLAN Implementation ....................................................................................3-1
WEP Encryption ............................................................................................3-1
WLANs that use WPA....................................................................................3-2
Related Documents .......................................................................................3-2
Conclusions .........................................................................................................3-3
Basic WLAN Guidelines

This chapter offers basic guidelines to mitigate the security risks introduced by the use of Wi-Fi technology. These guidelines apply equally to:

- Issuers
- Acquirers
- Merchants
- Third Party Processors (TPPs)
- Data Storage Entities (DSEs)

WLAN Implementation

Generally, WLANs should be avoided unless there is an identified business need to deploy this technology.

If deployed, WLANs should be significantly segregated from production networks and corporate networks.

Only those WLANs that are installed following the most up-to-date security practices should be allowed any sort of access to corporate resources.

WEP Encryption

Wireless networks that do not use any encryption, or are only able to use 40-bit WEP (often mistakenly labeled 64-bit) should not be used. Such protections can be compromised in real-time by unskilled attackers using inexpensive hardware and open source attack tools.

Networks able to operate with 104-bit WEP (mistakenly labeled 128-bit) should be treated with the same caution and mistrust as unknown connections from the Internet.

In addition to the use of 104-bit WEP, networks should have MAC address-based access controls and should have clearly defined administrator policies and procedures. The procedures should include regular rotation of the WEP keys and should disable broadcasting of the network SSID.

WLANs that use 104-bit WEP should be outside of the corporate firewall and require the same kinds of authentication that is required when users work off site. Any access that is prohibited to off-site users should also be prohibited to such wireless users, even though they may be physically located on site.
The same unskilled attackers, using the same inexpensive hardware and open source software, can attack these networks. It will take them more than twice as long to crack the cryptography, but this should not be considered a significant barrier.

**WLANs that use WPA**

Those networks able to implement WPA completely – and without any WEP compatibility – are candidates for greater trust. Higher-level protocol protections (such as SSL, HTTPS, or VPN) should be used for wireless nodes that access any trusted resources.

All wireless traffic should be funneled to one wired VPN or network segment to provide a single entry and exit point to/from the corporate network. Procedures for the monitoring and logging of wireless traffic, and unexpected network events, must be defined and implemented; this is considered essential to detect potential attacks.

**Related Documents**

In order to address payment industry requirements, MasterCard has changed the relevant security rules and data protection standards to incorporate the above mentioned basic WLAN security guidelines. These rules and standards will apply to issuers, acquirers, merchants, third party processors (TPPs) and data storage entities (DSEs) that use wireless LAN technology connected to networks or servers that process or store MasterCard transaction data, account data, or both.
Conclusions

Issuers, acquirers, MSPs, merchants, TPPs, DSEs are likely to be using, or exploring the use of, WLAN technology. Unfortunately, all current WLAN protocols and wireless devices are vulnerable to attacks that could put sensitive information at risk, including cardholder information.

Wireless technologies are new enough that they can easily be improperly deployed. Furthermore, most commodity products ship with insufficient security features, or with their security features disabled.

Risk mitigation strategies should be put in place to address the risks and threats identified in this document.

MasterCard has updated the relevant security rules and data protection standards to ensure adequate coverage of the risks associated with the use of wireless LANs.