Return to Menu

MasterCard International

Information about this New Manual

New Manual

This *Electronic Commerce Security Architecture Best Practices*, dated April 2003, is an entirely new manual.

Contents

This manual contains architectures, methodologies, and best practices for establishing a secure electronic commerce environment.

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

Billing

MasterCard will not bill principal members for this document.

Questions?

If you have questions about this manual, please contact the Global Member Operations Support 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 *Electronic Commerce Security Architecture Best Practices* using the following e-mail address:

publications@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.

MasterCard International

Electronic Commerce Security Architecture Best Practices

April 2003

Media

This document is available:

- On MasterCard OnLine®
- On the MasterCard Site Data Protection Web site, https://sdp.mastercardintl.com

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63366-7263
USA

1-636-722-6100

www.mastercard.com

Using this Manual

Chapter 1 MasterCard Site Data Protection Program

Chapter 2 E-commerce Fundamentals

Using this Manual

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

Purpose

The *Electronic Commerce Security Architecture Best Practices* presents architectures, methodologies, and best practices for establishing a secure electronic commerce environment.

Audience

MasterCard provides this manual for acquiring members, merchants, and Member Service Providers that accept MasterCard for payment and store MasterCard account data on their electronic commerce infrastructures.

Overview

The following table provides an overview of this manual:

Chapter	Description
Table of Contents	A list of the manual's chapters and subsections. Each entry references a chapter and page number.
Using this Manual	A description of the manual's purpose and its contents.
1 Overview	An overview of the MasterCard program established to combat the security threats associated with online commerce.
2 E-commerce Fundamentals	Outlines the typical e-commerce transaction, and the various e-commerce modes of operation.
3 Security Architecture Components	Outlines the technical components, architectures, and configurations used in a typical electronic commerce environment.
Glossary	A dictionary of terms and acronyms used by MasterCard in relation to the Site Data Protection Program.

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 *Webster's New 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:

	St. Louis, Missouri USA Central Time	**Purchase, New York USA** Eastern Time	**UTC**
Standard time (last Sunday in October to the first Sunday in April [a])	9:00	10:00	15:00
Daylight saving time (first Sunday in April to last Sunday in October)	9:00	10:00	14:00

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

Revisions

MasterCard periodically will 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 date of the revision appears in the footer of each page.

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

The following documents and resources provide information related to the subjects discussed in this manual.

- *MasterCard Security Standard Applicable to Merchants and Member Service Providers*
- *MasterCard Security Standard Applicable to Vendors*
- *Electronic Commerce Requirements and Best Practices for Acquirers*

Support

Please address your questions to the Global Member Operations Support 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
Global Member Operations Support
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 Global Member Operations Support team addresses.

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

Atlanta	1-404-459-2400
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 Global Member Operations Support team at:

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

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

1 MasterCard Site Data Protection Program

This chapter provides an overview of electronic commerce transactions and the Site Data Protection Program developed by MasterCard to combat the security threats associated with electronic commerce.

Background

Electronic commerce is the business of buying and selling products, information, or services in an Internet based environment. Unlike traditional face-to-face transactions, e-commerce shoppers and merchants communicate through a public computer network.

E-commerce transactions are predominantly conducted via a credit or debit card. Typically, e-commerce merchants store cardholder information in databases to streamline the consumer checkout process. In doing so, Web merchants compile databases containing hundreds, thousands, or even millions of payment card accounts. For hackers, these databases represent a tremendous opportunity for theft and fraud.

MasterCard research indicates that Internet security concerns continue to play a major role in consumer reluctance to make online purchases. In fact, one study shows that three-quarters of those who do not shop online are concerned about unauthorized individuals gaining access to their personal information. Media reports about the hacking of top Web sites and the resulting theft of payment card information further fuels consumer concern. For online merchants, a hacker break-in can have potentially devastating consequences, including service disruptions, vandalism, extortion, and the loss of consumer confidence.

Hacker intrusions that result in an account data compromise present a particular source of financial risk for MasterCard and for members.

MasterCard Site Data Protection Program

To help combat the security threats associated with electronic commerce, MasterCard launched the MasterCard Site Data Protection (SDP) Service in February 2002. To encourage the adoption of security measures online, MasterCard has expanded the concept and developed the MasterCard Site Data Protection Program. This comprehensive, flexible program calls for members to adopt, implement, and maintain data security compliance programs for themselves and for their electronic commerce merchants and Member Service Providers (MSP) that participate or support MasterCard-branded electronic commerce.

A MasterCard member that wishes to benefit from participation in the SDP Program is fully responsible for ongoing compliance with the MasterCard Security Standard by itself and by all participants in the member's programs.

MASTERCARD MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THE SITE DATA PROTECTION PROGRAM OR THE CONTENTS OF THIS *ELECTRONIC COMMERCE SECURITY ARCHITECTURE BEST PRACTICES* MANUAL. MASTERCARD SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANT ABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE.

Member acknowledges and agrees that MasterCard shall not be liable to the member (or any third party, including customers of the member) for any:

- Loss, or
- Damages (including direct, special, punitive, exemplary, incidental, or consequential damages), or
- Costs (including attorney's fees) that,
  - arise from the member's (or the member's merchants or MSP) participation, use of, or failure to participate in or use the SDP Program (or any component thereof), or
  - otherwise arise from or related to the SDP Program.

The foregoing limitation of liability shall apply to any claim or cause of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if MasterCard has been notified of the possibility of such damages or claim.

MasterCard is deploying the MasterCard Site Data Protection Program through its acquirers worldwide and on a voluntary basis.

Through active participation, MasterCard acquirers can ensure that e-commerce merchants and MSPs adequately protect their environments against hacker intrusions. Additionally, acquirers that ensure that merchants and MSPs comply with the requirements detailed in the program may be afforded a partial or full waiver of assessments in cases of an account data compromise.

The MasterCard Site Data Protection Program consists of the following elements:

MasterCard Security Standard
• MasterCard Security Standard Applicable to Vendors
• MasterCard Security Standard Applicable to Merchants and Member Service Providers
• Electronic Commerce Security Architecture Best Practices
• Electronic Commerce Requirements and Best Practices for Acquirers

Components

- Electronic commerce self-assessment tool for merchants and Member Service Providers
- Security scanning tools

Solutions

- Existing MasterCard Site Data Protection Service, a solution offered by MasterCard through acquiring members
- Alternative Vendor Solutions that are compliant with the MasterCard Security Standard Applicable to Vendors

Rules

- Account Data Compromise Rules, including the associated waiver process through SDP Program compliance
- Merchant Registration Process through MasterCard Alerts for MasterCard Standard compliance

Security Vendor Certification

- Voluntary, fee-based service for the vendor community to gain MasterCard Standard compliant certification for marketing security services to acquirers, members, and Member Service Providers

MasterCard Security Standard

MasterCard has developed the following four documents that encompass the MasterCard Security Standard:

1. *MasterCard Security Standard Applicable to Vendors*: Presents requirements for third-party vendor solutions to be considered MasterCard compliant.
2. *MasterCard Security Standard Applicable to Merchants and Member Service Providers*: Provides e-commerce acquirers, merchants, and Member Service Providers with MasterCard requirements for participating in the MasterCard Site Data Protection Program and for demonstrating compliance.
3. *Electronic Commerce Security Architecture Best Practices*: Provides e-commerce merchants and Member Service Providers with best practices for developing and maintaining secure electronic commerce platforms.
4. *Electronic Commerce Requirements and Best Practices for Acquirers:* An electronic commerce resource for acquirers covering topics such as coding transactions, privacy, security, and more.

All of the above documents are available to members via the Member Publications product on MasterCard OnLine®.

Components

E-commerce merchants and MSPs that elect to participate in the MasterCard Site Data Protection Program must use two tools to determine their compliance with this Standard:

1. The Electronic Commerce Self-Assessment is a tool that asks merchants and MSPs a series of questions relating to information and network security. The assessment provides a self-grading mechanism, which allows immediate determination of compliance with the MasterCard Security Standard.
2. Security Scanning tools are vulnerability assessment tools which determine flaws in e-commerce merchant and MSP network infrastructures.

The detailed requirements for the security self-assessment and network scans are contained in chapters 2 and 3 of *MasterCard Security Standard Applicable to Merchants and Member Service Providers*.

Solutions

MasterCard members, e-commerce merchants, and MSPs can select the solution that best fits their needs. They can use either of the following:

1. The MasterCard Site Data Protection (SDP) Service, which is a service offered by MasterCard through the acquirer.
2. A third-party vendor or security consultant solution that is compliant with the *MasterCard Security Standard Applicable to Vendors*.

Note

MasterCard acquirers that choose to deploy third party solutions are responsible for ensuring that those solutions meet the requirements detailed in the *MasterCard Security Standard Applicable to Vendors* manual. MasterCard will offer an optional vendor certification program that will facilitate this evaluation.

Rules

A MasterCard acquirer is subject to an assessment in cases of account data compromise. MasterCard rules require members to ensure that all e-commerce merchants and MSPs keep all systems and media containing MasterCard account, cardholder, or transaction information (whether physical or electronic) in a secure manner to prevent access by, or disclosure to any unauthorized party. Additionally, all sensitive cardholder information that the merchant or MSP no longer considers necessary to retain must be destroyed in a manner that will render the data unreadable.

If an intrusion occurs, whether in the acquirer's merchant systems or MSP systems, the acquirer must provide MasterCard with complete information about the compromise and engage a data security firm in compliance with the *MasterCard Security Standard Applicable to Vendors* manual to assess the vulnerabilities of the merchant or MSP systems. MasterCard may impose assessments, including an incident assessment, administration fees, and issuer card-recovery fees on the acquirer.

Members should consult the *Security Rules and Procedures* manual, chapter 7, and *Bylaws and Rules*, chapter 9, for more information.

An acquirer can request a waiver from assessments based on a MasterCard review of the security situation at the time of the compromise. Eligibility criteria include, but are not limited to:

- The compromised party has used a solution that meets the MasterCard Security Standard.
- The compromised merchant or MSP is found to be "SDP compliant" at the time of the account data compromise. Additionally, the compromised party must produce self-assessment reports with a Green or Yellow rating, and scan reports with no level three, four, or five vulnerabilities, to demonstrate compliance with the *MasterCard Security Standard Applicable to Merchants and Member Service Providers*.
- The acquirer has registered the compromised merchant and/or associated MSP as being compliant with the *MasterCard Security Standard Applicable to Merchants and Member Service Providers*. Acquirers can register merchants and associated MSPs through the MasterCard Merchant Registration Program (available through the MasterCard Alerts Product). Details regarding merchant registration procedures and pricing can be found in the *Security Rules and Procedures* manual.

MasterCard will examine all circumstances to determine if a waiver or partial waiver of assessment is appropriate. Any such determination is made in MasterCard's sole discretion and is final and not subject to appeal.

Security Vendor Certification

To be eligible for any waiver of an assessment resulting from an account data compromise, MasterCard acquirers must ensure that their electronic commerce merchants and MSPs use the services of a security vendor that complies with the *MasterCard Security Standard Applicable to Vendors*. Using the *MasterCard Security Standard Applicable to Vendors*, members can self-evaluate vendors for compliance.

Security vendors that wish to be certified by MasterCard should visit the MasterCard SDP Program Web site at https://sdp.mastercardintl.com for certification procedures.

Additionally, MasterCard will deploy a voluntary, fee-based security vendor certification service in 2003. A list of certified security vendors will be available on the MasterCard SDP Web site.

Meeting Compliance Requirements

An acquirer must ensure that any of its merchants, or MSPs that are afforded access to, or store account data, or both, is in compliance with the MasterCard Security Standard. Specifically, an acquirer must ensure its e-commerce merchants and MSPs meet the following conditions in order to qualify as SDP compliant:

- All e-commerce merchants and MSPs must complete an annual self-assessment, which is included in the *MasterCard Security Standard Applicable to Merchants and Member Service Providers* manual, and posted in a PDF file format on the MasterCard Site Data Protection Web site at https://sdp.mastercardintl.com. Using the self-assessment grading system, e-commerce merchants and MSPs can immediately determine if their security measures are acceptable (Green and Yellow) or unacceptable (Red).
- A merchant having an average monthly e-commerce gross dollar volume (eDGV) in excess of USD 50,000 or with greater than 1,000 transactions per month is defined as a large merchant. Large merchants and all e-commerce MSPs must scan their Web infrastructure quarterly.
- An e-commerce merchant having less than USD 50,000 eGDV or less than 1,000 transactions per month must scan its Web infrastructure annually.

Note **Acquirers should determine merchant monthly eDGV and transaction volumes based on an average of the previous 12 months.**

- The scan reports must indicate that no level 3, 4, or 5 vulnerabilities exist. If these risks do exist, corrective measures must be taken to bring security into compliance as outlined in this document. After taking corrective measures, users must retake the survey and produce a clean scan report to demonstrate compliance.
- To ensure compliance, acquirers should request and review completed merchant and MSP reports (self-assessment and scan reports).
- Once the acquirer determines compliance, the merchant or MSP must be registered through the MasterCard Alerts product on MasterCard Online®.

Acquirers should also strongly suggest that Web site infrastructure designs be in accordance with the *Electronic Commerce Security Architecture Best Practices* manual.

2 E-commerce Fundamentals

This chapter outlines the typical e-commerce transaction, and the various e-commerce modes of operation.

Overview

This chapter outlines the typical e-commerce transaction, and the various e-commerce modes of operation. Relevant security issues and best practices are also discussed.

E-commerce Transaction

To understand the various architectures of the e-commerce components it is important to understand the typical flow of an e-commerce transaction.

The shopping experience of the cardholder consists of several sequential steps:

1. **Shopping**—the cardholder browses the catalog of the e-commerce merchant, selects one or more products, and adds these products to the shopping basket or cart.
2. **Checkout**—the cardholder proceeds to checkout and provides identification, including name, billing address, and shipping address. If the cardholder is already a customer of the merchant, he or she may log into the site with a username and password. Once logged in, the cardholder's information is already present on the merchant Web site. The cardholder confirms this information.
3. **Online Payment**—the cardholder pays for the order by entering card details. This process is known as "online payment."

Online Payment Configurations

There are three methods for implementing the process defined as "online payment." The e-commerce merchant may:

1. Own the payment software.
2. Use a server point of sale (POS) operated by an acquirer.
3. Use a POS operated by a Payment Service Provider (PSP).

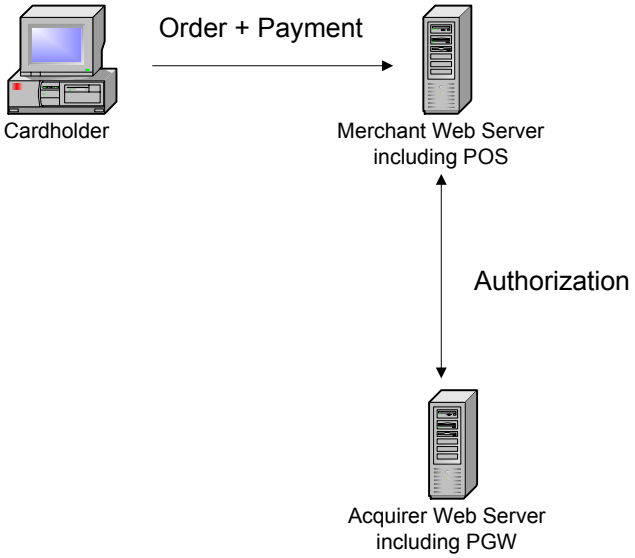
Note **Anyone other than the merchant and the acquirer with access to the electronic commerce transaction information is called a service provider.**

Merchant Owns Payment Software

The merchant may purchase a payment-processing component and install this software on the server. The software is known as a point of sale (POS) or payment module. This module communicates with a payment gateway (PGW) typically installed at an acquirer or other third party.

In this scenario, the cardholder transacts only with the merchant Web site. The merchant's POS sends the payment details to a payment gateway and obtains an authorization.

Figure 2.1—Merchant owns payment software



Security Issue

The e-commerce merchant Web site stores confidential payment information.

Best Practice

- The cardholder details should be stored encrypted.
- The merchant should use Secure Socket Layer (SSL) or another industry standard for data encryption.

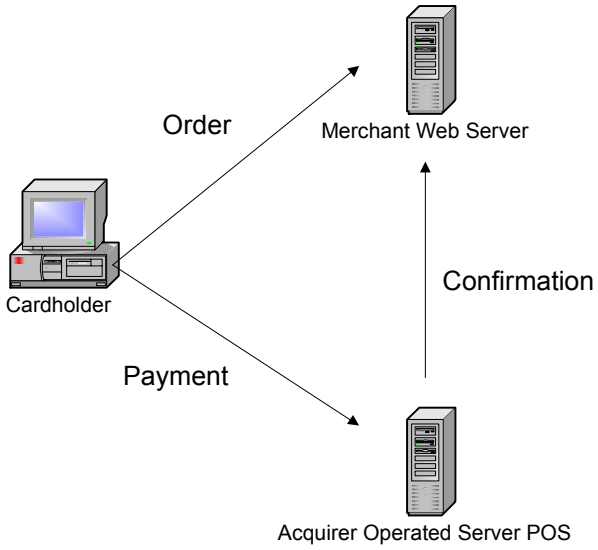
Merchant Uses Acquirer Operated Server POS

Merchants may redirect cardholders to an acquirer Web site for payment. The server POS operated by the acquirer handles the complete payment process and directs the customer back to the merchant Web site after the payment process is complete.

Typically, the merchant is not provided with payment details; the merchant's Web server holds only information related to the order. (In some cases, for example in the airline industry, the merchant can have access to the credit card information.)

The merchant can access the Web site of the acquirer and see an overview of all payments. The merchant can use an online interface on the acquirer's Web site to capture, cancel, or refund payments.

Figure 2.2—Merchant using an acquirer operated server POS



The disadvantage of this mode of operation is the inconvenience to the merchant if the merchant wants to accept multiple brands or different payment instruments. If a single acquirer does not offer this service, the merchant must integrate multiple interfaces to acquirers that accept each brand or payment instrument.

The advantage of this mode of operation is that the merchant does not have to concentrate on the technical aspects of integrating a payment processing software.

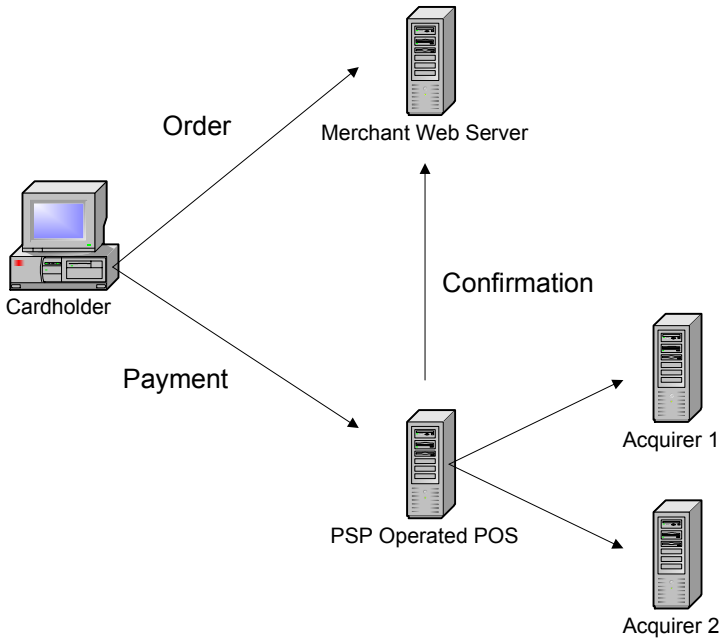
Security Issue

In most cases, the confidential payment information is solely located on the acquirer's server. This should be a secure environment, because it will contain a high concentration of data for multiple merchants. Using an acquirer operated server POS reduces the merchant's risk because only the order information is stored at the merchant site. If the merchant stores payment information at its site, the merchant environment also must be properly protected.

Payment Service Provider (PSP)

The merchant may use a server POS operated by a service provider, also called a Payment Service Provider (PSP). A PSP is a third party operating a POS on behalf of the merchant; a PSP must be registered with MasterCard as a Member Service Provider (MSP). The process is similar to a merchant using an acquirer operated POS, except in this case, the cardholder is completing a payment transaction on the Web site of the PSP, and the PSP is transacting with the acquirer(s).

Figure 2.3—Merchant using a payment service provider (PSP)



The merchant can access the Web site of the PSP and see an overview of all payments. If a capture, cancel, or refund is necessary, the merchant can do this on the Web site of the PSP.

The advantages of this mode of operation to the merchant are:

- The merchant does not have the technical skills and prefers not to be responsible for technical aspects of a payment processing software integration.
- This approach offers the merchant the possibility to accept many different payment methods in a single integration effort.

Security Issue

The confidential payment information is located at the PSP. This should be a secure environment, because it will contain a high concentration of data for multiple merchants. This reduces the merchant's risk because only the order information is stored at the merchant site. If the merchant stores payment information at its site, then the merchant environment also needs to be properly protected.

If the Merchant Does Not Own Payment Software

When the e-commerce merchant does not own payment software, further action is necessary after the e-commerce transaction is complete. These actions could include:

- "order treatment"
- "capture" or "refund"

Order Treatment

Order treatment means that the merchant needs a solution to see that there is a new order. Depending on the location of the e-commerce components, the merchant may access this information remotely or locally on the server.

If accessing the information remotely, proper precautions are necessary to guarantee the confidentiality of the information during transmission. The information must be protected against eavesdropping during transit on the network. Secure Socket Layer (SSL) communication and Virtual Private Network (VPN) are two communication methods that provide a high level of protection during transmission with a remote server.

Payments Capture and Refund

After order delivery to the customer, the merchant needs the ability to activate the capture of the payment. In the same manner, if the goods are returned the payment may need to be refunded.

This process is necessary to bill the customer's credit card with a previously obtained authorization or to reverse a previously billed amount.

Depending on the scenario of the payment flow, the merchant will have to connect to their POS, the site of the acquirer, or the site of the PSP. High volume merchants could use an automated task activated from the backend. In all cases, this payment related communication must be properly secured.

Security Issue

Encrypt the communication to protect all information from eavesdropping.

Best Practice

Merchants should never display the complete card number on screen. Merchants may display only the last four digits of the account number. All preceding digits must be replaced with fill-characters such as such as "X," "*," or "#." Fill-characters must not include blank spaces or numeric characters.

Typical E-commerce Modes of Operation

Not all merchants have their own dedicated equipment and connections. Consequently, there are three modes of operations:

1. Dedicated
2. Co-Location
3. Hosting

Dedicated

Dedicated configurations are those where the merchant has all equipment and software in-house. The merchant owns control over all equipment including network components and has decision-making authority.

Co-location

Co-located configurations are those where the merchant owns the server and the installed software, but the server is located in a data center of an Internet Service Provider (ISP). The ISP, not the merchant, owns the network equipment such as, routers, firewalls, and Intrusion Detection System (IDS). The network components (including bandwidth) are shared among many customers of the ISP.

Security Issue

People not working for the merchant organization can access the server.

Hosting

Hosting is a merchant Web site operated by a third party. Because hosting providers share their resources with multiple customers, a variety of customer Web sites are located on the same server. This type of server is called a "multi-homed" Web server. In this situation, the merchant does not own or control the server and network components.

Security Issues

- People not working for the merchant organization can access the server.
- Security management including firewall maintenance, IDS, vulnerability assessment, and security patches are out of the merchant's control.
- Another Web site on the same server could contain a weakness that compromises the security on all other Web sites.

3 Security Architecture Components

This chapter discusses the technical components, architectures, and configurations used in a typical electronic commerce environment.

Overview

This chapter outlines the technical components, architectures, and configurations used in a typical electronic commerce environment. Additionally, the chapter addresses relevant security issues and best practices.

Technical Component Groups

E-commerce environments are comprised of two distinct component groups. The first group contains the router, firewall, and intrusion detection system, referred to collectively as network components.

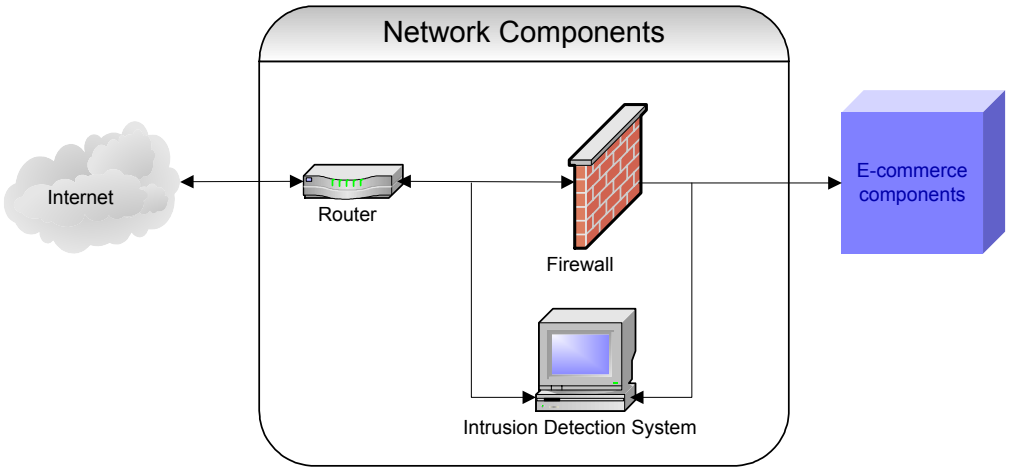
The second group contains the operating system (OS), Web server, application server, database server, e-commerce application, mail server, Domain Name Server (DNS), and additional applications, referred to collectively as e-commerce components.

Not all components are present in every e-commerce environment and many component combinations are possible. Some e-commerce environments might have a limited number of the discussed components, but the possible combinations are endless.

Network Components

Three important network components include the router, the firewall, and the intrusion detection system (IDS).

Figure 3.1—Network components



Router

The router is a device that connects the merchant's network to the Internet. The router is responsible for routing packets to and from the external Internet. The router comes with firmware and a configuration. It is important to protect this device and its configuration from unauthorized modification.

The router configuration can include a filter or an access list. The filter prevents certain types of packets or protocols from entering or leaving the internal network, and the access list blocks traffic to or from certain hosts.

Security Issues

- A router has a unique Internet Protocol (IP) address. In most cases, a router can be configured through a Telnet session. A Telnet session is an interactive logon that gives the administrator a command prompt to configure the device. In advanced cases, configuration can be accomplished using a Web browser.
- A password protects access to the router. A vendor default password is a password installed in the factory. Failure to modify the default allows anyone with knowledge of the vendor default password to access and modify the router configuration.
- Password guessing techniques can be used to obtain unauthorized access.
- If obsolete firmware is used, there may be vulnerabilities in the device. The most common are vulnerabilities that allow a denial of service (DoS) attack. This type of attack allows anyone connected to the Internet to send a malicious, formatted packet to the device, making it hang or crash. Consequently, the merchant is disconnected from the Internet resulting in loss of revenue and image.
- Simple Network Management Protocol (SNMP) is a protocol that allows remote configuration and monitoring of a router. Security is based on a secret community string; an SNMP community string is the password needed to access an SNMP agent. In the factory, the device configuration includes a default community string. Failure to change the default community string allows anybody with a connection to the router to change the settings. There are two types of community strings: read-only and read-write. Many devices use "public" as the default read-only community string, and "private" as the default read-write community string.

Best Practices

- Telnet is not a secure protocol, and should not be used over the Internet. Use secure shell (SSH) instead.
- Change the vendor default password before placing the router in a production environment.
- Change the default community string if the router is using SNMP.
- SNMP is not a secure protocol and should not be used over the Internet.
- Passwords must be, at a minimum, six characters long and consist of a mix of alphanumeric values.
- Change passwords at least every 30 days.
- Physically protect and store the router in a secure room.
- Use configuration hardening by disabling all unnecessary services in the router configuration.
- If there is a new firmware release, install it in the router.
- Scan routers regularly for vulnerabilities.

Firewall

A firewall is the component that acts as a first line of defense against intrusion of the internal network from the outside world. The firewall accepts or rejects packets coming from the Internet or going towards the Internet based on rules. The firewall must be protected from intrusion and alteration.

Another function of a firewall is network address translation (NAT). This means that the firewall can translate the addresses of network packets and hide the real internal network address (used by internal machines) from the external network. The goal of NAT is to make it more difficult for unauthorized users to determine the internal network topology.

A firewall comes in many types and many forms. Some firewalls are dedicated hardware boxes. Other firewalls are software installed on a server with two or more network cards. Firewall-1® from Checkpoint is a well-known software-based firewall. Cisco Pix is an example of a hardware firewall.

Security Issues

- Malicious users routinely develop new vulnerabilities and exploits that can penetrate or avoid a firewall.
- Installation of a firewall does not guarantee complete security. A malicious exploit can pass through the firewall as Hyper Text Transfer Protocol (HTTP) traffic.
- A common problem with firewalls is incorrect or inadequate configuration of the rules.

Best Practices

- Keep firewalls up to date, and install available patches regularly.
- Scan firewalls regularly.
- Log any attempts to violate the firewall rules.
- Review firewall logs regularly.
- Allow necessary traffic only. Consider using an application shield device that denies all traffic not specifically recognizable by the Web server. An example is Ubizen's DMZ/Shield. Another example is the ISS Realsecure® product, which verifies whether a DNS request (UDP port 53) is real or malicious data disguised as a DNS request.
- Use NAT to hide the internal network architecture.
- Think in multiple layers of security and do not blindly rely on the firewall to block some traffic and protect all servers. With multiple layers of security, the system can remain secure, even in the event of a firewall compromise.
- Physically protect and store the firewall in a secure room.
- Establish a formal procedure to manage changes to the firewall rules.

Intrusion Detection System (IDS)

The IDS typically screens all network packets, and is a system used as a second line of defense against intrusion of the internal network from the outside world. IDS uses a network card in "sniffing" mode also called the sensor.

IF...	THEN...
the sensor is located in front of the firewall	All attempts to penetrate or exploit arriving at the firewall can be detected
the sensor is located behind the firewall	All successful penetrations, and exploits that passed the firewall can be detected

The IDS is configured with rules. The rules define what attacks to detect, and what action to take upon detection.

The IDS can be linked dynamically to block the firewall when it detects an intrusion attempt. Consequently, unwanted results could occur when doing a penetration test and testing for vulnerabilities. When the IDS detects an attempt, it adds a rule to the firewall and blocks all future traffic from the source IP address. This could make further testing impossible.

Examples of network based intrusion detection systems are ISS RealSecure® and Snort.

Host-based IDS

It is also possible to have a host-based IDS. A host-based IDS is software installed locally on the server to be monitored and looks for intrusion on the server itself. Typically, the software looks for file system access, file changes, and other possible anomalies that are an indication of intrusion.

An example of a host based intrusion detection system is Tripwire.

Security Issue

Special techniques known as evasion techniques can mislead an IDS. For example, one evasion technique fragments all TCP/IP packets so the signature is not recognized because the data is fragmented over multiple packets. Another evasion technique encodes data in the Unicode format.

Best Practices

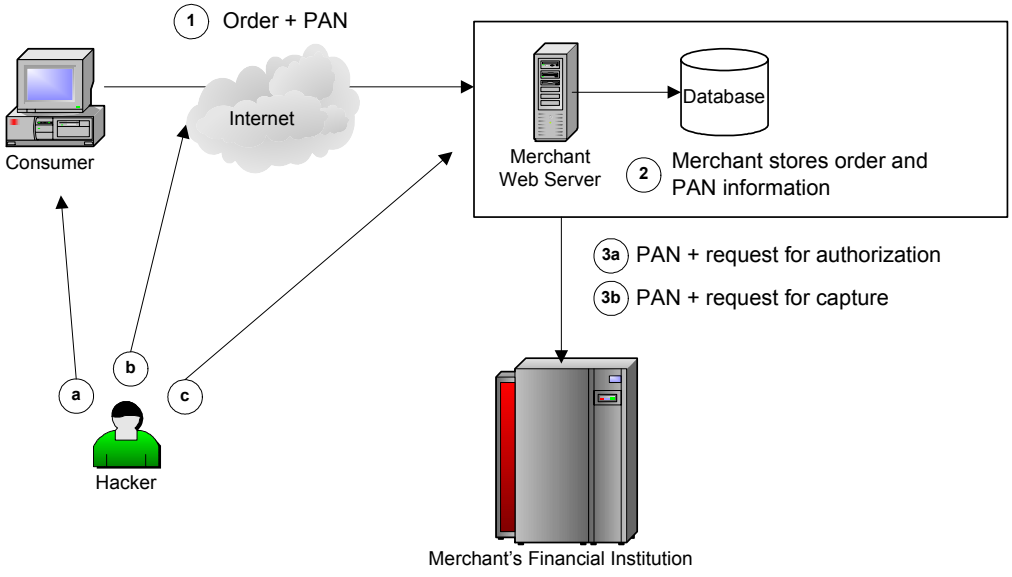
- Review log files regularly.
- Update IDS rules regularly to include the latest attacks.
- Use a stream pre-processor reassembling all the packets to help counter some evasion techniques based on fragmentation.
- Use a Unicode pre-processor to help counter some evasion techniques based on Unicode encoding.
- Physically protect and store the IDS in a secure room.

E-commerce Components

E-commerce components can be found on a single server or they can span multiple servers depending on the size of the merchant's e-commerce environment.

Figure 3.2 illustrates the use of payment cards in an e-commerce environment, and shows the various methods hackers use to steal those payment card account numbers.

Figure 3.2—Typical hacking methods



E-commerce transactions can be broken up in several steps:

1. The consumer places an order and transmits the payment card account number to the merchant.
2. The merchant stores the order and the account holder information in a database for future reference.

3a. The merchant transmits the amount of the purchase and the account holder information to a financial institution in order to obtain an authorization, indicating the reservation of funds that allows settling the transaction later.

3b. Finally, after the delivery of goods to the consumer, the merchant asks the financial institution to settle the transaction and credit the merchant account. This action is known as capture.

The hacker can steal account holder information several ways:

a. The hacker can impersonate the merchant or make a bogus Web site. The consumer does not notice this and sends the order and credit information directly to the hacker. Another scenario exists where the hacker installs a key-logger on the device of the consumer, logging all information typed on the keyboard, including account holder information including the payment card number.

b. The hacker observes the communication between the cardholder and the merchant. Transmitting credit card information on the network without encryption, allows the hacker to read this information.

c. The hacker can penetrate the merchant's e-commerce environment and steal information in the database.

The merchant's Web server may have many different software components. Together, these components form an e-commerce application that is serving customer requests over the network. Typically, components are found in layers. Components also may be implemented on more than one physical machine. A separate database server is a common practice.

The following components can be found in an e-commerce environment:

- operating system (OS)
- database server
- Web server
- scripts, servlets, Common Gateway Interface (CGI)
- application server
- application beans
- DNS server
- mail server
- other applications

Operating System

The OS is the lowest layer of software found in an e-commerce environment.

If the e-commerce components span multiple physical machines, it is possible that the Web server runs on one OS and the database server runs on another OS. Spreading the e-commerce components over more than one machine enhances the risks in securing inter-machine communications. This issue is discussed later in this chapter.

Merchants may choose to span e-commerce components over multiple physical machines for several reasons:

- One reason could be added security. For example, the database server is in a separate subnet, making it inaccessible from the Internet.
- Another motivation can be for performance reasons. An OS can be optimized for best performance as a network server, serving multiple concurrent requests for Web pages. An OS also can be adjusted for best performance as a database server for which throughput to the disk system is most critical. This could be a conflict if all software is residing on a single box, hence the choice of using two servers to resolve this conflict.

Examples of Operating Systems are: Microsoft Windows, OS400 and various UNIX styles: IBM AIX, Sun Solaris, HP-UX and, Linux.

Security Issues

- New vulnerabilities and exploits are regularly discovered making the OS vulnerable to attacks.
- A standard OS installation is usually not secure.

Best Practices

- Harden an OS before it is used in production. Disable all unnecessary services in the configuration of the server.

Definition **Hardening is the process of extra actions following a default installation, including the removal of unnecessary services, the renaming of built-in accounts, changing passwords, removing powerful tools, and the tightening of overall security.**

- Keep the OS up-to-date and patched regularly. Frequent scanning ensures that the OS has the latest patches available.
- Passwords must be, at a minimum, six characters long and consist of a mix of alphanumeric values.

- Change passwords at least every 30 days.

Database

The database is the component responsible for storing and retrieving data. For Web merchants, databases usually contain sensitive cardholder data, including payment card account numbers.

The database could be simple, like a flat file, or the database could be a complex relational database using a separate relational database product. The database can be installed on the same machine, or the database could be located on a separate machine.

When a relational database management system (RDBMS) is used, the application will use an interface to communicate to the RDBMS. Examples of such interfaces are Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), and in some cases, native mode. ODBC and JDBC try to make some level of abstraction of the underlying database management system allowing the use of application software with different database products.

Examples of Databases include Microsoft SQL Server, Oracle, and Sybase.

Security Issues

- The content of a database could be accessed outside of an application, bypassing logical controls in the application.
- The content of a database could be accessed over the Internet if the database server port is open.
- New vulnerabilities are regularly discovered and may introduce weaknesses to the database.

Best Practices

- Encrypt sensitive cardholder information such as account numbers.

  Because computer power continually improves, the merchant should use state of the art cryptographic algorithms to make sure the work factor is long enough. The work factor is the time needed to try all combinations for a key during a brute force attack.

  While Data Encryption Standard (DES) and Triple DES are widely used algorithms, the National Institute of Standards and Technology (NIST) chose a new algorithm as the Advanced Encryption Standard (AES). The new algorithm addresses the increasing capacity of computers and makes the work factor long enough to keep the encrypted information confidential. AES is also known as Rijndael, a concatenation of the names of the researchers who developed the algorithm.

- Ensure encryption keys cannot be stolen. A tamper proof hardware device is a good practice for secure storage of keys.
- Back up database content regularly, encrypt backup files, and protect access to backup media.
- Do not give remote access to the database unless the communication is encrypted and the access is necessary.
- Keep RDBMS up-to-date, and patch regularly.
- Give database access to programs and users only where there is a need. Do not grant write-access if not necessary.

Web Server

The Web server application is a program that accepts HTTP/HTTPS requests from the customer's browser over the Internet and delivers the corresponding content back to the customer's browser.

Examples of well-known Web servers include Microsoft IIS (Internet Information Server), Apache, and Netscape.

Security Issues

- A poorly configured Web server can be used to access data on the server that should not be downloadable.
- Write and execute rights should be assigned very carefully. They could be used to execute commands on the Web server and to change the server configuration.
- A Web server can be vulnerable to a DoS attack, buffer overflow and other vulnerabilities.

Best Practices

- Do not store cardholder data on a Web server.
- Harden Web servers to tighten the security and remove exploitable tools.
- Keep Web servers up-to-date, also patch, and scan regularly.
- Disable directory browsing on a Web server.
- Do not return extensive error codes to the browser. Turn off debug information because it may provide useful clues to a hacker.

CGI, Scripts, Servlets

A request to a Web server can be static as in a request for an HTML page or an image. However, most of the e-commerce Web sites today require dynamic content.

The process that allows cardholders to enter card data on a Web page involves dynamic data transfer. In this process, the merchant accepts data and passes the data from the Web server to the backend systems for authorization and order processing. This dynamic link between the public-facing merchant Web-server and the merchant's backend systems create a particular area of vulnerability.

Dynamic Web sites can be built using CGI, scripts, and servlets. They are three possible technologies and they provide a mechanism to extend a Web server with new functionality. The request sent by the browser to the Web server is then forwarded to the CGI, script, or servlet. The request typically includes some parameters. The CGI, script, or servlet returns the result to the Web server and the Web server returns the output to the customer's browser.

The CGI is an external process to the Web server. Script and servlet are new methods developed for performance reasons over CGI. Often, these processes load only once and are then cached by the Web server, making them faster than a CGI.

Some examples of script languages are PERL and PHP4. An example of a servlet engine is Tomcat.

Security Issue

- CGI, scripts, or servlets can introduce a variety of exploits. Buffer overflow attacks are the most common. A buffer overflow happens when the CGI, script, or servlet does not safely control the parameters passed to it, resulting in overwriting some part in memory. When the extra data is carefully crafted, the hacker can run arbitrary code on the remote target.
- Give special attention to CGI, scripts, or servlets that allows a command to run in a shell.
- SQL injection can be used to access the database beyond the scope of the e-commerce application.

Best Practices

- Use industry standard programming methods when writing CGI, scripts or servlets.
- Never rely on client side input control when developing CGI, scripts, or servlets.

Application Server

Using an application server enhances security, portability, and scalability.

Improve security by configuring the application server to split the e-commerce components on several machines, making the backend inaccessible from the Internet.

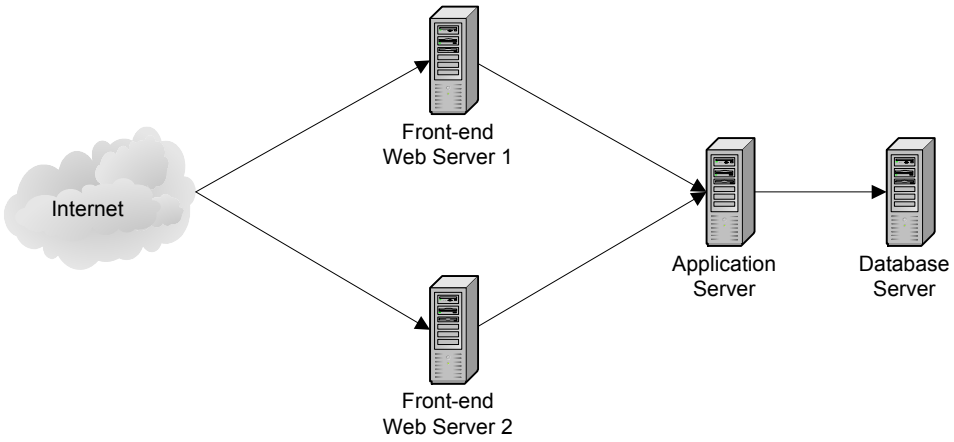
Portability means that applications written in an application server environment can be used with minor or no changes on various platforms for which the application server is available.

Scalability means that for performance reasons an application server can run on multiple servers working together as a cluster. The application server layer will take care of the scheduling and communication between the servers to make them work together as one logical unit. That is, one application server can work on behalf of multiple Web servers or other e-commerce components.

Well-known application servers include Weblogic, JBoss, and Netscape application server.

Figure 3.3 shows the use of an application server to link several Web servers.

Figure 3.3—Application Server



Security Issues

- A standard installation could be insecure.
- New vulnerabilities are found regularly and published on the Internet. These vulnerabilities can be used to build exploits that compromise the server.

Best Practices

- Remove demonstration applications after installing an application server. Demonstration applications are shipped with the product to demonstrate advanced usage of the product. If not removed, these example applications can provide back doors that enable system penetration.
- Harden an application server after installation. Rename built-in accounts, and change the password.
- Keep the application server up-to-date, and patch and scan regularly.

Application Beans

A bean is an object with a published interface. A bean can provide services to servlets, or it can be invoked from a standalone Java application.

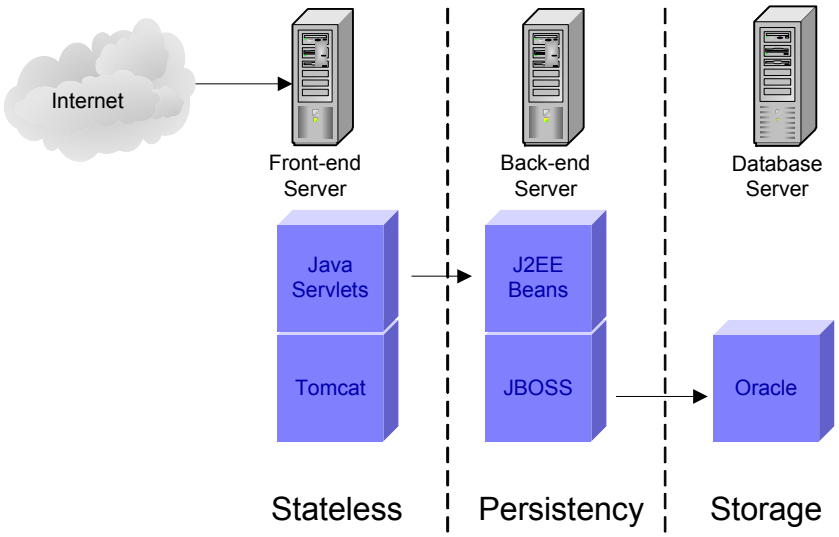
Application components running in the application server are often custom developed and are by far the most difficult to audit. They also can introduce weaknesses into the system and should be developed with care.

When using the Java Enterprise architecture (J2EE), the application will typically be composed of different components. The presentation layer (front-end) will be using Java servlets. The business logic (back-end) will be using Java enterprise beans.

A servlet is comparable to a CGI script and uses the incoming parameters to do some server side processing and in most cases returns some HTML output back to the Web browser.

The following diagram shows a possible architecture with a Tomcat servlet engine and a JBoss J2EE application server.

Figure 3.4—Typical J2EE Architecture



The servlets in the stateless front-end will make a call to the beans in the persistency layer using remote invocation interface (RMI).

DNS Server

The role of a DNS server is to resolve a domain name into an IP address. When typing a URL in a Web browser, the Web browser will ask a DNS server to resolve the domain name into an IP address, such as 192.168.10.1.

DNS is a distributed protocol and is based on many DNS servers working together to serve requests to resolve a domain name. Each server has a local cache to avoid a remote query for every single request. This creates a potential vulnerability where malicious people "poison" the cache and divert the traffic to a bogus server. Often the merchant does not own a DNS, but uses a DNS server of a service provider.

Security Issue

- A DNS server compromise could send consumers to a replacing Web server under the control of a hacker.
- DNS servers often have vulnerabilities and they are used as the entry point into the network of the organization. Once a DNS server compromise occurs, the next step is to compromise another server using the DNS as a stepping-stone.

Best Practices

- Harden DNS servers.
- Scan and patch DNS servers regularly.
- Physically store and protect the DNS servers in a secure room.
- Limit zone transfers to trusted servers.
- Separate an internal DNS server from an external DNS server.

Mail Server

The merchant uses a mail server to receive and send e-mail messages. Often the merchant communicates to the consumer using e-mail. E-commerce applications also send automated e-mail messages to consumers.

Security Issue

- Mail servers often contain weaknesses that can be used to penetrate the network.
- The mail server could be used to send unauthorized messages to the consumers asking for their credit card number or other information on behalf of the merchant.
- E-mail messages are not secure when sent unencrypted.

Best Practices

- Harden mail servers.
- Scan and patch mail servers regularly.
- Do not exchange unencrypted cardholder details over e-mail.

Other Applications

In some cases, merchant systems contain other applications.

Common examples of other third party applications are standard applications used for remote maintenance. This could introduce a potential vulnerability because these applications provide ways to compromise the system.

Well-known examples are PCAnywhere, and VNC.

Other applications commonly found on a merchant server are backup software, monitoring software, payment modules, intrusion detection modules, and anti-virus software.

Security Issue

Remote management programs could be exploited allowing unauthorized users to access systems remotely.

Best Practices

Install third party applications only on a need-to-have basis.

Typical E-commerce Architectures and Configurations

The following section addresses the most common architectures for merchant e-commerce environments.

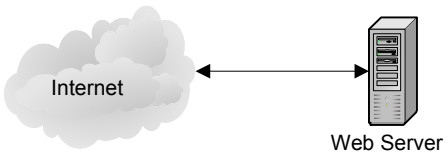
Note **In this section, the diagrams are logical schemes showing the flow of information and not actual network diagrams.**

Security issues and best practices previously covered during the discussion of individual components will not be repeated but remain applicable.

Single Box

The simplest architecture is a single box containing all the software required for the e-commerce environment. The following diagram shows this type of architecture.

Figure 3.5—Single box configuration



The following table explains the single box configuration possibilities:

Components	Comments
Operating system	The OS can be one of many possibilities. UNIX is a common example for this single box solution.
Web server	The Web server can be one of the many existing Web servers. Examples include IIS, Apache, and Netscape.
Database	The database is not necessarily present. If a database is installed in this scenario, it resides on the same machine. Sensitive cardholder information should never be stored on a Web server in this configuration.
Application server	Use of an application server is an option in this configuration.
Other applications	The server can contain other applications such as remote management, backup, or other specific tasks.
Firewall	Not all merchants install a firewall in this scenario, although it is possible to install one on the server. There are still servers connected to the Internet without firewall protection.

Security Issues

- The single box is a vulnerable architecture because installing all components on one server does not provide a secure second line of defense for server penetration.
- The database is installed on a machine directly accessible from the Internet. In case of a penetration, the hacker can steal the content of the database, including sensitive cardholder information.

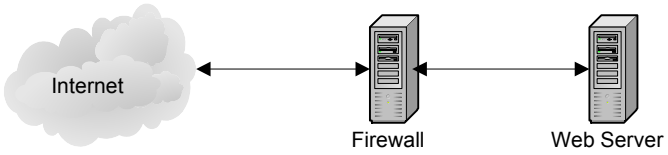
Best Practices

- This configuration is not recommended.
- In the event that this configuration is used, install layers for security, so that if one layer is broken, the system has other security layers in place. This makes penetration more difficult.

Single Box behind a Firewall

Internet merchants often install a firewall between the box and the Internet to make the single box architecture more secure. The following diagram illustrates this type of architecture.

Figure 3.6—Single box behind a firewall



The following table explains the possibilities of a single box behind a firewall configuration:

Components	Comments
Operating system	There can be many OS possibilities.
Web server	The Web server can be one of the many existing Web servers.
Database	The database is not necessarily present. If a database is installed in this scenario, it resides on the same machine.
Application server	Use of an application server is an option in this configuration.
Other applications	The server can contain other applications, such as remote management, backup, or other specific tasks.
Firewall	The firewall is installed on a dedicated machine. Even with a firewall in place, the Web server also should be secured. Install layers of security. Each additional layer is an extra defense.

Security Issues

A firewall installation does not guarantee complete security. It is possible to construct a malicious exploit that passes the firewall as HTTP traffic. A firewall does not offer complete protection.

Best Practice

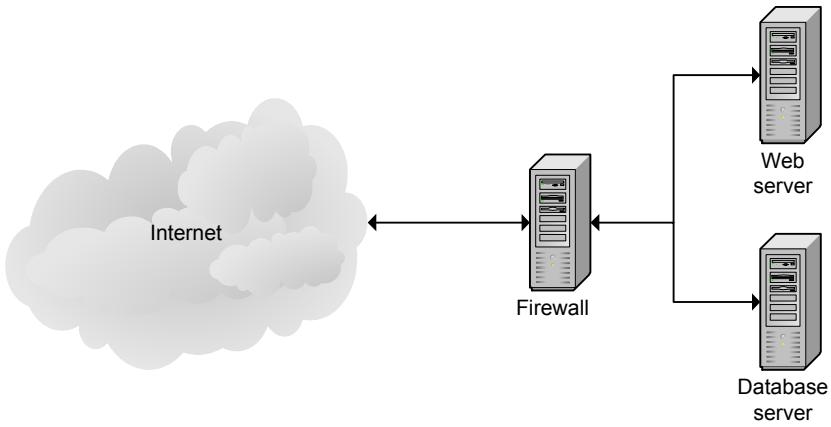
An IDS can help to detect malicious traffic passing the firewall.

Web Server and Separate Database Server behind a Firewall

Installing a database on a separate machine improves performance and adds an additional layer of security. There are two options to separate the database.

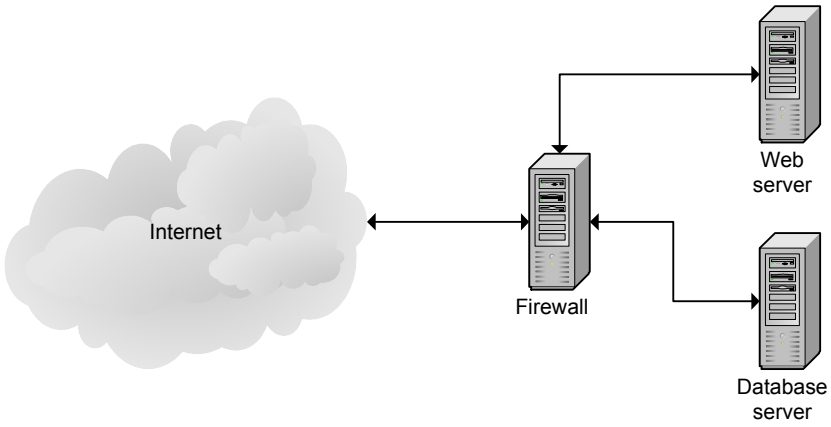
The first option is to install the Web server on the same network segment of the database server behind the firewall. If the firewall has NAT installed, the database typically has an IP address that is not routable and only known in the internal network of the merchant.

Figure 3.7—Web server and separate database server behind a firewall



The second option is to install the database server on a separate network segment if the firewall has more than two network cards. In this scenario, if a hacker were to compromise the Web server the hacker still would have to get through the firewall to access the database server.

Figure 3.8—Web server and separate database behind a firewall on a separate network segment



The following table explains the possibilities of a Web server and separate database behind a firewall on a separate network segment:

Components	Comments
Operating system	The OS can be many possibilities. It is possible that the Web server is using a different OS from the database server.
Web server	The Web server can be one of the many existing Web servers.
Database	The database is installed on a separate machine. The Web server will communicate with the database server through ODBC, JDBC or a native protocol.
Application server	Use of an application server is an option in this configuration.
Other applications	The server can contain other applications, such as remote management, backup, or other specific tasks.
Firewall	The firewall is installed on a dedicated machine. Depending on the situation, the firewall has two or more separated network segments.

Security Issues

- A firewall does not guarantee complete security. It is possible to construct a malicious exploit that passes the firewall as HTTP traffic.
- The communication between the application on the Web server and the database could be subject to eavesdropping so should be encrypted.
- Even if the firewall is protecting the database, SQL injection could access the database beyond the scope of the application.

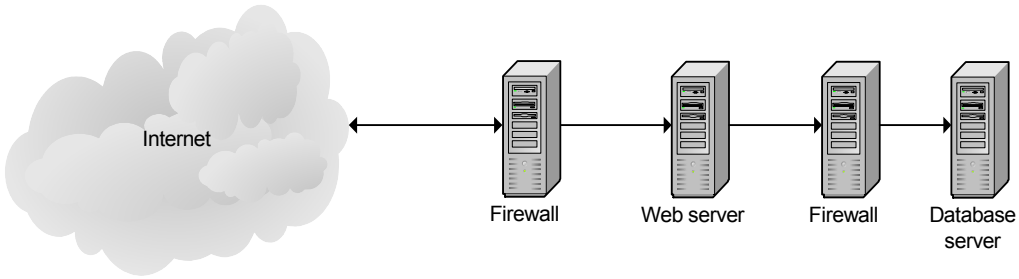
Best Practices

- Encrypt the communication between the application and the RDBMS. Special ODBC drivers exist and provide this service transparently for the application.
- An IDS can help to detect malicious traffic passing the firewall.
- The e-commerce application should never rely on client side input controls.

Multiple Firewall Configuration

In a multiple firewall configuration, an extra firewall increases the security. The extra firewall acts as an extra security layer. This means that if a compromise occurs on one layer, the other layer continues to protect.

Figure 3.9—Multiple firewall configuration



The following table explains the possibilities of a multiple firewall configuration:

Components	Comments
Operating system	The OS can be many possibilities. It is possible that the Web server is using a different OS from the database server.
Web server	The Web server can be one of the many existing Web servers.
Database	The database is installed on a separate machine. The Web server communicates with the database server through ODBC, JDBC or a native protocol. The communication to the database is protected with a firewall. This allows the firewall to control the traffic directed towards the database.
Application server	Use of an application server is an option in this configuration.
Other Applications	The server can contain other applications such as remote management, backup, or other specific tasks.
Firewall	The firewalls are installed on dedicated machines. Depending on the situation, two different brands of firewalls can be used. If an exploit is published for one brand, the other is not necessary exploitable.

Security Issues

- A firewall does not guarantee complete security. It is possible to construct a malicious exploit that passes the firewall as HTTP traffic.
- The communication between the application on the Web server and the backend could be subject to eavesdropping; therefore, the communication should be encrypted.

Best Practices

- The communication between the application and the RDBMS can be encrypted. Special ODBC drivers exist and provide this service transparently for the application.
- An IDS can help to detect malicious traffic passing the firewalls.

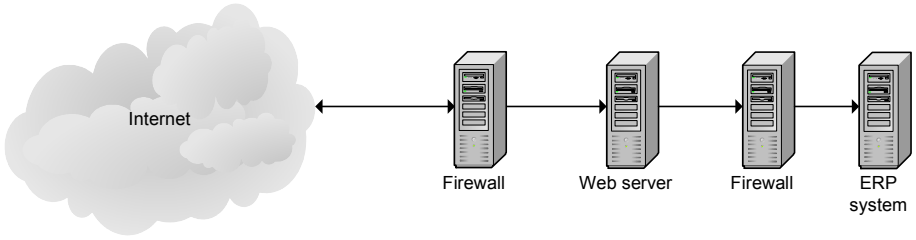
Multiple Firewall Configuration with Back-end

Today integration is increasingly an issue with large e-commerce merchants and Member Service Providers (MSP) relying on e-commerce as a channel for their revenue. For large e-commerce merchants and MSPs, it is not possible to re-enter all data from the e-commerce components into their legacy system. Therefore, the e-commerce components will be tightly integrated to the backend systems.

Many different scenarios are possible for integrating an e-commerce environment into an existing backend. The most important requirement is to have proper separation and good security practices in place.

The following diagram illustrates an example of integration with a backend. A good example is an Enterprise Resource Planning (ERP) environment linked to an e-commerce front-end.

Figure 3.10—Multiple firewall configuration with backend



The following table explains the possibilities of a configuration for multiple firewalls with a back-end configuration:

Components	Comments
Operating system	The OS can be many possibilities.
Web server	The Web server can be one of the many existing Web servers.
Enterprise Resource Planning (ERP) system	ERP systems typically include inventory, accounts payable, and other processes of the company. In large implementations the e-commerce environment will be integrated and interact with these environments. Examples of an ERP application include SAP and Navision.
Application server	In this configuration, the use of an application server is an option. If an application server were used, the fourth server located behind the second firewall would be the preferred location.
Other applications	The server can contain other applications, such as remote management, backup, or other specific tasks.
Firewall	The firewalls are installed on dedicated machines. Depending on the situation, two different brands of firewalls can be used. If an exploit is published for one brand, the other is not necessary exploitable.

Security Issues

- A firewall does not guarantee complete security. It is possible to construct a malicious exploit that passes the firewall as HTTP traffic.
- The communication between the application on the Web server and the backend could be subject to eavesdropping; therefore, the communication should be encrypted.

Best Practices

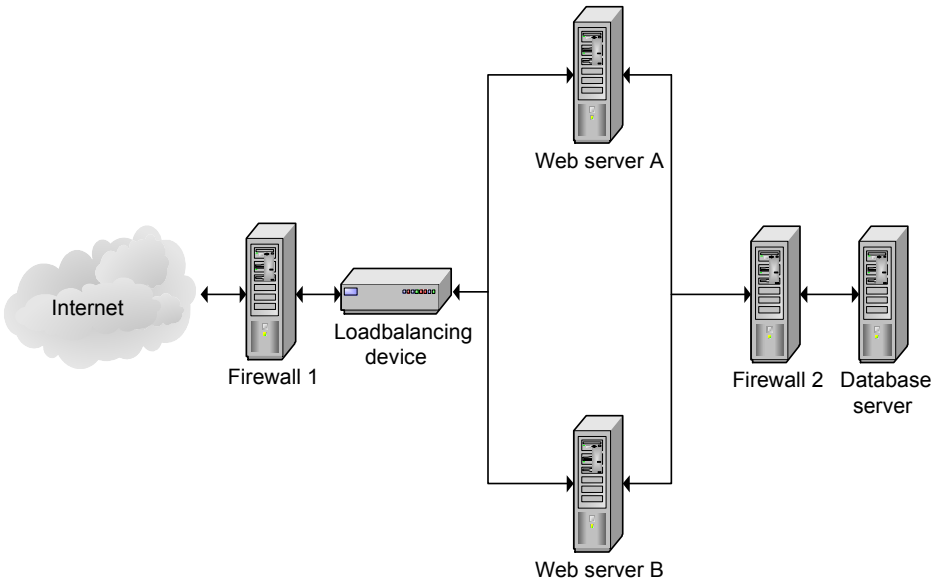
- An IDS can help to detect malicious traffic passing the firewalls.
- Using encryption could protect the communication between the e-commerce front end and the back end.

Complex Load Balanced Architecture

The following diagram shows that a merchant environment can be complex; if necessary, some components can be redundant for both performance and availability reasons. A load-balanced architecture automatically directs visitors to the machine that is least occupied.

In the example below, the Web servers are redundant. A load-balancing device is a component in front of the Web server that divides the load over the two servers. If one Web server fails, then the load-balancing device automatically directs traffic to the other Web server to avoid service interruption.

Figure 3.11—Complex load balanced architecture



The following table explains the possibilities of a complex load balanced architecture:

Components	Comments
Operating system	The OS can be many possibilities.
Web server	The Web server can be one of the many existing Web servers.
Database server	The database is installed on a separate machine. The Web server will communicate with the database server through ODBC, JDBC or a native protocol. The communication to the database is protected with a firewall. This allows controlling the traffic towards the database.
Application server	In this configuration, the use of an application server is an option.
Other applications	The server can contain other applications, such as remote management, backup, or other specific tasks.
Firewall	The firewalls are installed on dedicated machines. Depending on the situation, two different firewalls can be used. If an exploit is published for one brand, the other is not necessary exploitable.

Security Issues

- A firewall does not guarantee complete security. It is possible to construct a malicious exploit that passes the firewall as HTTP traffic.
- The communication between the application on the Web server and the backend could be subject to eavesdropping; therefore, the communication should be encrypted.

Best Practices

- The communication between the application and the RDBMS can be encrypted. Special ODBC drivers exist that do this transparently for the application.
- An IDS can help to detect malicious traffic passing the firewalls.

Glossary

This chapter defines various terms, concepts, acronyms, and abbreviations used in this document. These definitions appear for convenience only and are not to be used or otherwise relied on for any legal or technical purpose. MasterCard specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as MasterCard deems fit.

Advanced Encryption Standard (AES)

An encryption algorithm for securing sensitive data.

AES

See Advanced Encryption Standard.

authentication

For purposes of SDP, ensuring that the message is genuine, that it has arrived exactly as it was sent, and that it comes from a stated source.

backup

The hardware and software resources available to recover after a degradation or failure of one or more system components.

cardholder

The customer to whom a card has been issued or the individual authorized to use the card.

CGI

See Common Gateway Interface.

Common Gateway Interface (CGI)

The common gateway interface (CGI) is a standard way for a Web server to pass a Web user's request to an application program and to receive data back to forward to the user.

Cryptography

The methods and practice of transforming confidential information to make it unintelligible to parties not authorized to know it.

Data Encryption Standard (DES)

A cryptographic algorithm adopted by the National Bureau of Standards for data security. Encryption scrambles PINs (personal identification numbers) and transaction data for safe transmission.

Ddos

See Distributed denial of service.

Denial of Service (DOS)

A denial of service (DoS) attack is an incident in which a user or organization is deprived of an expected resource. Typically, the loss of service is a particular network service, such as e-mail, or the temporary loss of all network connectivity and services.

DES

See Data Encryption Standard.

Distributed denial of service (DdoS)

On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

DoS

See Denial of Service.

eavesdropping

A third-party attack where information remains intact, but its privacy is compromised.

electronic commerce

The exchange of goods or services for payment between a cardholder and merchant that involves electronic communication.

electronic commerce merchant

A merchant that sells products and services online and accepts MasterCard payment products.

encryption

The technique of modifying a known bit stream so that it appears to be random to an unauthorized observer. It often is done automatically before data is transmitted.

Enterprise Resource Planning (ERP)

Enterprise resource planning is the set of activities supported by application software that helps a company manage many facets of its business.

ERP

See Enterprise Resource Planning.

face-to-face transaction

A transaction where the card, the cardholder, and the merchant representative are all present at the time of the transaction.

host

An intelligent processor or device that is connected to a network and satisfies the needs of remote users.

HTTP

See Hypertext Transfer Protocol.

Hypertext Transfer Protocol

The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

ICMP

See Internet Control Message Protocol.

Internet

The largest collection of networks in the world, interconnected to allow them to function as a single virtual network.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet.

LAN

See local area network.

large e-commerce merchant

MasterCard defines a large e-commerce merchant as a merchant with an average monthly MasterCard eGDV greater than USD 50,000 or with greater than 1,000 e-commerce transactions per month.

local area network (LAN)

A link-up of workstations and peripheral equipment in an office, building, or locality so users may communicate and share equipment and information.

log

A record of everything pertinent to a system function. A collection of messages that provides a history of message traffic.

merchant

A retailer, or any other person, firm, or corporation that (pursuant to a merchant agreement) agrees to accept MasterCard-branded cards, when properly presented.

NAT

See Network Address Translation.

Network Address Translation (NAT)

Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network.

Operating System (OS)

Master control program that runs the computer. The operating system is the first program copied into the computer's memory, from a disk or tape, after the computer is first turned on.

OS

See Operating System.

packet

A sequence of data, with associated control information, that is switched and transmitted as a whole; refers mainly to the field structure and format defined within the CCITT X.25 recommendation.

PAN

See Primary Account Number.

Payment Service Provider

A member or merchant registered with MasterCard to facilitate funds transfers between two parties using the MasterCard infrastructure. A Payment Service Provider accepts funds from the payer (sender) initiating the transfer, and subsequently delivers the funds using the MasterCard Payment Transaction or other funds transfer methods. The Payment Service Provider does not sell goods and services; however, a Payment Service Provider may facilitate payment for goods and services by acting as an intermediary between a buyer and a seller.

personal identification number

A four- to 12-character secret alphanumeric code that enables an issuer to authenticate the cardholder for the purpose of approving an ATM or terminal transaction occurring at a point-of-interaction device.

For MasterCard OnLine, PIN is a four-digit code that allows a user to access MasterCard OnLine, in conjunction with a SecurID device.

PIN

See personal identification number.

Point of Sale

The location where a transaction occurs.

POS

See Point of Sale.

Primary Account Number

The number that is embossed, encoded, or both, on a MasterCard card that identifies the issuer and the particular cardholder account. The PAN consists of a major industry identifier, issuer identifier, individual account identifier, and check digit.

PSP

See Payment Service Provider.

RDBMS

See Relational Database Management System.

Relational Database Management System (RDBMS)

A method in data processing whereby data are presented to programs in the form of unique rows of data without regard to how the data is physically stored. A software system that integrates more than one applications program so that interfaces are not necessary and each is accessible instantly.

replay-attack

The process of sending a previously sent message as a method of perpetrating fraud.

Scanning tools

Automated tools that check the merchant or Member Service Provider e-commerce environment for vulnerabilities.

SDP-compliant vendor

Security vendors that are in compliance with the MasterCard Site Data Protection Security Standards as presented in this document.

Secure Shell (SSH)

is a Unix-based command interface and protocol for securely getting access to a remote computer.

Secure Socket Layer (SSL)

Secure Socket Layer (SSL) developed by Netscape Communications Company, is a standard that encrypts data between a Web browser and a Web server. SSL does not specify what data is sent or encrypted. In an SSL session, all data sent is encrypted.

Simple Network Management Protocol

SNMP is the protocol governing network management and the monitoring of network devices and their functions.

small e-commerce merchant

MasterCard defines a small e-commerce merchant as a merchant with an average monthly MasterCard e-commerce gross dollar volume (eGDV) less than USD 50,000 or with less than 1,000 e-commerce transactions per month.

smart card

A credit or debit card containing a computer chip with memory and interactive capabilities used to identify and store additional data about the cardholder, cardholder account, or both. Also called an integrated circuit card or a chip card.

sniffer

A sniffer is a program that can be used to maliciously capture data being transmitted on a network.

SNMP

See Simple Network Management Protocol.

spoof

On the Internet, spoofing is the action of deceiving for the purpose of gaining access to someone else's resources, for example, to fake an Internet address.

SSH

See Secure Shell.

SSL

See Secure Socket Layer.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

Transmission Control Protocol/Internet Protocol

A standardized set of communication protocols that support peer-to-peer connectivity for both local and wide-area networks.

virtual private network

A service that enables large organizations to use a telecommunications carrier's network as if it were their own private line connections. MasterCard uses VPN services for the Banknet telecommunications network.

VPN

See virtual private network.

World Wide Web (WWW)

A service on the Internet consisting of servers that send documents to World Wide Web browsers residing on user's systems. Web documents typically contain hypertext links to other documents.

World Wide Web browser

Desktop software residing on the user's system that enables users of the Internet to access information resources. World Wide Web browsers request and display HTML (Hypertext Markup Language) documents from World Wide Web servers. Users can install other add-on or plug-in software programs that process data that is in formats other than HTML. Also referred to as Web browser or browser.

World Wide Web server

A server that stores and presents documents in formats such as HTML (Hypertext Markup Language.) A World Wide Web server can run additional external programs that prepare HTML pages dynamically.

WWW

See World Wide Web.