Application Security: Electronic Commerce and E-Mail

Network Security Course
Iwan Syarif
Politeknik Elektronika Negeri Surabaya

Reference:
Panko, Corporate Computer and Network Security
Copyright 2005 Prentice-Hall
Figure 9-1: General Application Security Issues

- Executing Commands with the Privileges of a Compromised Application
  - If an attacker takes over an application, the attacker can execute commands with the privileges of that application
  - Many applications run with super user (root) privileges
Figure 9-1: General Application Security Issues

- Buffer Overflow Attacks
  - From Chapter 6: Vulnerabilities
  - Exploits
  - Fixes
    - Patches
    - Manual work-arounds, or
    - Version upgrades)
Figure 9-1: General Application Security Issues

- Buffer Overflow Attacks
  - Buffers are places where data is stored temporarily
  - If an attacker sends too much data, a buffer might overflow, overwriting an adjacent section of RAM
  - If that section is retrieved, various problems can occur
  - Read as data, read as program instructions, illegal values that cause a crash
Buffer Overflow Attacks

- Stacks are used to hold information temporarily on subprograms
- Stack overflows might allow an attacker to execute any command (Figure 9-2)
- An example: The IIS IPP Buffer Overflow Attack: Host variable is overflowed
Figure 9-2: Stack Entry and Buffer Overflow

1. Write Return Address

2. Add Data to Buffer

3. Direction of Data Writing

4. Overwrite Return Address

5. Start of Attack Code
Figure 9-1: General Application Security Issues

- Few Operating Systems But Many Applications
  - So application hardening is more total work than operating system hardening

- Application Security Actions
  - Understanding the server’s role and threat environment
  - If it runs only one or a few services, easy to disallow irrelevant things
Figure 9-1: General Application Security Issues

- Application Security Actions
  - Basics
    - Physical security (Chapter 2)
    - Harden the operating system (Chapter 6)
    - Backup (Chapter 10)
  - Install Application Patches
Figure 9-1: General Application Security Issues

- Application Security Actions
  - Minimize applications
    - Main applications
    - Subsidiary applications
    - Be guided by security baselines
  - Add application layer authentication
  - Implement cryptographic systems
Figure 9-1: General Application Security Issues

- Application Security Actions
  - Minimize the permissions of applications so that successful attackers will not own the machine
  - Hackers who take over an application obtain the permissions of that application
  - Many applications run as root, giving the hacker total control of the computer if compromised
  - Application take-over is the most common way to hack computers today
Figure 9-3: Webserver and E-Commerce Security

- Importance of Webservice and E-Commerce Security
  - Cost of disruptions
  - The cost of loss of reputation and market capitalization
Figure 9-3: Webserver and E-Commerce Security

- Importance of Webservice and E-Commerce Security
  - Customer fraud (including credit card fraud)
    - Loss of revenues when product is not paid for
    - Credit card company charge-back fees
    - Must use external firm to check credit card numbers
Figure 9-3: Webserver and E-Commerce Security

- Importance of Webservice and E-Commerce Security
  - Cost of privacy violations
  - Links to internal corporate servers
Figure 9-3: Webserver and E-Commerce Security

- Webservers Versus E-Commerce Servers
  - Webservice provides basic user interactions
    - Microsoft Internet Information Server (IIS)
    - Apache on UNIX
    - Other webserver programs
Figure 9-3: Webserver and E-Commerce Security

- Webservers Versus E-Commerce Servers
  - E-commerce servers add functionality:
    - Order entry,
    - shopping cart,
    - payment, etc.
  - Custom programs written for special purposes
<table>
<thead>
<tr>
<th>Webserver Software</th>
<th>Subsidiary E-Commerce Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component (PHP, etc.)</td>
<td>Custom Programs</td>
</tr>
</tbody>
</table>

**Figure 9-4: Webservice Versus E-Commerce Service**
Figure 9-3: Webserver and E-Commerce Security

- Some Webserver Attacks
  - Website defacement
  - Numerous IIS buffer overflow attacks, many of which take over the computer
Figure 9-3: Webserver and E-Commerce Security

Some Webserver Attacks

- IIS directory traversal attacks
  - Normally, paths start at the WWW root directory
  - Adding ../ might take the attacker up a level, out of the WWW root box
  - If traverse to command prompt directory in Windows 2000 or NT, can execute any command with system privileges
Figure 9-3: Webserver and E-Commerce Security

- Some Webserver Attacks
  - IIS directory traversal attacks
    - Companies filter out / and \n  - Attackers respond with hexadecimal and UNICODE representations for / and \n
Figure 9-3: Webserver and E-Commerce Security

- Some Webserver Attacks
  - Apache has problems, too
Figure 9-3: Webserver and E-Commerce Security

- Patching the Webserver and E-Commerce Software and Its Components
  - Patching the webserver software is not enough
  - Also must patch e-commerce software
  - E-commerce software might use third-party component software that must be patched
Figure 9-3: Webserver and E-Commerce Security

- Controlling Dynamic Webpage Development
  - Static versus dynamic webpages
  - For static webpages:
    - GET /path/filename.extension HTTP / version
  - CGI to pass parameters to a program
    - GET /path/programname.exe?variable1="value"&variable2="value"…
    - Inefficient. Starts new copy of program with each request
Figure 9-3: Webserver and E-Commerce Security

- Controlling Dynamic Webpage Development
  - ASP is Microsoft’s server-side scripting language
  - ISAPI from Microsoft starts a .dll component
    - Component continues to run; no need to start a new copy with each request
Figure 9-3: Webserver and E-Commerce Security

- Controlling Dynamic Webpage Development
  - Controlling software development
    - Programmer training in safe programming methods
  - Auditing for security weaknesses
Controlling Dynamic Webpage Development

- Deployment

- Development servers: Developers must have wide privileges

- Staging servers: Only testers and systems administrators should have privileges

- Production servers: Only systems administrators should have privileges
Figure 9-3: Webserver and E-Commerce Security

- User Authentication
  - None: No burden on customer (e.g., traditional SSL/TLS)
  - Username and password provide some protection but may be given out without checking customer quality
  - IPsec and digital certificates: Expensive and difficult for customers
  - TLS with client digital certificates: Less expensive than IPsec but difficult for customers
Figure 9-3: Webserver and E-Commerce Security

- Browser Attacks
  - Take over a client via the browser
    - Interesting information on the client
    - Can use browser to attack clients
Figure 9-3: Webserver and E-Commerce Security

- Browser Attacks
  - Client-side scripting
    - Java applets: Small Java programs
    - Scripting languages (not full programming languages)
      - JavaScript and VBScript
    - Active-X from Microsoft; highly dangerous because it can do almost everything
Figure 9-3: Webserver and E-Commerce Security

- **Browser Attacks**
  - Malicious links
  - User must click on them to execute (but not always)
  - Common extensions are hidden by default in windows
    - attack.txt.exe seems to be attack.txt
Browser Attacks
  - Common Attacks
    - File reading and executing a command
    - Redirection to unwanted webpage
    - Scripts might change the registry, home page
    - Might Trojanize the program called when user mistypes a URL
    - Pop-up windows behind main window so source is hard to find
Figure 9-3: Webserver and E-Commerce Security

- **Browser Attacks**
  - Common Attacks

- Cookies and web bugs
  - Cookies are placed on user computer; can be retrieved by website
  - Can be used to track users at a website
  - Web bugs—links that are nearly invisible—can do the same
Browser Attacks

- Common Attacks

  - Choose domain names that are common misspellings of popular domain names
    - Microsoft.com, www.whitehouse.com (a porn site)

  - Opening two windows; transfer information from client window to webserver window
Figure 9-3: Webserver and E-Commerce Security

- Browser Attacks
  - Enhancing Browser Security
    - Patches and updates
    - Set strong security options (Figure 9-5) for Microsoft Internet Explorer 6.0
    - Remotely managing browsers on employee client PCs
Figure 9-5: Internet Options Dialog Box in Internet Explorer 6.0
Figure 9-6: E-Mail Security

- E-Mail Technology
  - E-Mail Clients and Mail Servers (Figure 9-7)
    - Mail server software: Sendmail on UNIX, Microsoft Exchange, and Lotus/IBM
    - Exchange, Notes dominate on Windows servers
    - On Windows clients, Microsoft Outlook Express is safer than full-featured Outlook because Outlook Express generally does not execute content
Figure 9-7: E-Mail Standards

Sending E-Mail Client

Message

RFC 822 or 2822 body
HTML body

Sender’s Mail Server

SMTP to Send

Receiver’s Mail Server

POP or IMAP to Download

Receiving E-Mail Client
Figure 9-6: E-Mail Security

- E-Mail Technology
  - SMTP to send messages from client to mail server or from mail server to mail server
  - To download messages to client e-mail program from receiver’s mail server
    - POP: Simple and popular; manage mail on client PC
    - IMAP: Can manage messages on mail server
Figure 9-6: E-Mail Security

- E-Mail Technology
  - E-mail bodies
    - RFC 822 / RFC 2822: Plain English text
    - HTML bodies: Graphics, fonts, etc.
    - HTML bodies might contain scripts, which might execute automatically when user opens the message
  - Web-based e-mail needs only a browser on the client PC
Figure 9-8: Web-Based E-Mail

- Client’s Browser
- HTTP Request Message
- HTTP Response Message
- Webpage Containing Message
- Client PC
- Almost all client PCs now have browsers. No need to install new software
- Webserver Program
- Webserver with Web-Based E-Mail
Figure 9-6: E-Mail Security

- E-Mail Content Filtering
  - Antivirus filtering and filtering for other executable code
    - Especially dangerous because of scripts in HTML bodies
  - Spam: Unsolicited commercial e-mail
Figure 9-6: E-Mail Security

- E-Mail Content Filtering
  - Volume is growing rapidly: Slowing and annoying users (porno and fraud)
  - Filtering for spam also rejects some legitimate messages
  - Sometimes employees attack spammers back; only hurts spoofed sender and the company could be sued
Figure 9-6: E-Mail Security

- Inappropriate Content
  - Companies often filter for sexually or racially harassing messages
  - Could be sued for not doing so
E-Mail Retention

- On hard disk and tape for some period of time
- Benefit: Can find information
- Drawback: Can be discovered in legal contests; could be embarrassing
- *Must* retain some messages for legal purposes (firing employees, banking, etc.)
Figure 9-6: E-Mail Security

- E-Mail Security
  - Message authentication to prevent spoofed sender addresses
  - Employee training
    - E-mail is not private; company has right to read
    - Your messages may be forwarded without permission
Figure 9-6: E-Mail Security

- E-Mail Security
  - Employee training
    - Never to put anything in a message they would not want to see in court, printed in the newspapers, or read by their boss
    - Never forward messages without permission
    - Don’t open attachments unless expecting it and with all software patched and antivirus scanning on
Figure 9-6: E-Mail Security

- E-Mail Encryption
  - Not widely used because of lack of clear standards
  - IETF has not been able to settle upon a single standard because of in-fighting
  - Three standards are used in corporations
    - TLS
    - S/MIME
    - PGP
Figure 9-6: E-Mail Security

- E-Mail Encryption
  - TLS only requires a digital certificate for servers
  - S/MIME requires a PKI for digital certificates
  - PGP uses trust among circles of friends: If A trusts B, and B trusts C, A may trust C’s list of public keys
    - Dangerous: Misplaced trust can spread bogus key/name pairs widely
Figure 9-9: Cryptographic Protection for E-Mail

TLS is easy to implement
No end-to-end encryption (Mail server sees all mail in plaintext)
Figure 9-9: Cryptographic Protection for E-Mail

Mail Server

S/MIME with PKI
End-to-end encryption
Complex to administer
E-mail programs typically can do it

Sending E-Mail Client

Receiving E-Mail Client
Figure 9-9: Cryptographic Protection for E-Mail

Mail Server

PGP with Circles of Trust
End-to-end encryption
Usually clumsy user interface

Sending E-Mail Client

Receiving E-Mail Client
Figure 9-10: Database and Instant Messaging Security Concerns

- Other Applications
  - There are many other applications
  - Each has its own security issues
Figure 9-10: Database and Instant Messaging Security Concerns

- Database
  - Often used in mission-critical applications
  - Application layer authentication: Many database applications have passwords beyond the computer login password
  - Relational databases: Tables with rows (entities) and columns (attributes)
Figure 9-10: Database and Instant Messaging Security Concerns

- Database
  - Granularity of access control
    - Restrict users to certain columns (attributes) in each row
      - For instance, deny access to salary column to most users
    - Limit access control to rows, for instance, only rows containing data about people in the user’s own department
Figure 9-10: Database and Instant Messaging Security Concerns

- Database
  - Granularity of access control
  - Prevent access to individual data: Allow trend analysts to deal only with sums and averages for aggregates such as departments
Figure 9-10: Database and Instant Messaging Security Concerns

- Database
  - Problems with commercial database servers
    - Empty administrative password for Microsoft’s SQL Server allowed break-ins
    - New version of SQL Server will be more locked down
Figure 9-10: Database and Instant Messaging Security Concerns

- Instant Messaging (IM)
  - Allows instant text communication and voice if has “click to talk”
  - Retention problem: Not integrated into retention schedules
  - File transfer problem: File transfers are not checked by antivirus programs, although a few popular antivirus programs check file transmissions for a few popular IM programs.
Figure 9-10: Database and Instant Messaging Security Concerns

- Relay Servers and IM
  - Some IM systems send all messages through a relay server
    - This makes retention possible
    - It makes filtering possible
    - For many security vulnerabilities, only the relay server needs to be updated, not all clients
Topics Covered

- Applications are the most common target for hacking break-ins
  - If hacker takes over an application, has the permissions of that application, often root permissions
  - Few operating systems but many applications
  - Hardening applications is much harder than managing operating systems (Chapter 6)
Topics Covered

- Buffer Overflow Attacks
  - Attacker sends “data” for a field that contains a program to be executed
  - Data is longer than the program’s memory buffer for that variable
  - When program instructions in the overflowed areas are executed, the attacker’s code executes
Topics Covered

- Hardening Applications
  - The server should be hardened and backed up
  - Patches should be installed for vulnerabilities
    - However, many applications exist, so just learning about vulnerabilities and patches can be a problem
  - Minimize applications
    - Main applications
    - Subsidiary applications
    - Be guided by security baselines
Topics Covered

- Hardening Applications (Continued)
  - Add application layer authentication
  - Implement cryptographic systems
  - Minimize the permissions of applications so that successful hackers will not own the machine
Topics Covered

- Webserver and E-Commerce Security
  - Importance of these applications to the firm
  - Damage to firm if taken over (including the revelation of private client data)
  - Webservice dominated by Microsoft Internet Information Server (IIS) and Apache on UNIX

- E-Commerce Attacks
  - Defacement
  - Take-overs through buffer overflow attacks
  - IIS directory traversal attacks
Topics Covered

- E-Commerce service has multiple applications
  - All must be patched and otherwise hardened

```
1. 6
  \)
+ 201
  )
+ 201
  )
  ) 3
  \n  )
  3)
+ 419
  443
  467
  470
  494
  494
  402
  43
  8
  3)
+ 402
  443
  467
  470
  494
  494
```
Topics Covered

- Dynamic Webpages
  - Accept user data
  - Create webpage on the fly, then send back to the user
  - If not programmed properly, will have vulnerabilities that can be exploited
  - Deployment through development server, testing server, and then production server—each will specific permissions for developers
Topics Covered

- User Authentication
  - None: No burden on customer (e.g., traditional SSL/TLS)
  - Username and password provide some protection but may be given out without checking customer quality
  - Customer digital certificates: Expensive and difficult for customers
Topics Covered

- Attacks on Browsers
  - Very widespread
    - Many Internet Explorer Vulnerabilities
  - Client-side scripting executes code on the user PC
    - If vulnerabilities are found, these scripts can do extensive damage
  - Malicious Links
    - May download attack programs to user PCs and execute them
Topics Covered

- Attacks on Browsers
  - Programs exploiting browser vulnerabilities can do considerable damage
    - Delete files
    - Install pop-up ads, redirect to pornography sites, steal credit card numbers, etc.
    - Intrusive cookies
    - Web bugs
    - Attack URLs similar to legitimate URLs
Topics Covered

- Enhancing Browser Security
  - Patches and updates
  - Set strong security options
  - Remotely managing browsers on employee client PCs
Topics Covered

- E-Mail Security
  - Vulnerabilities in mail servers (SENDMAIL, Exchange)
  - Need antivirus filtering
  - Need spam filtering (sometimes filters out legitimate messages)
  - Inappropriate content (harassment)
  - Need to retain certain e-mail, but retaining too much leave a firm open to legal discovery searches
Topics Covered

- E-Mail Security
  - User Education
    - E-mail is not private
    - Your messages may be forwarded without permission
    - Never to put anything bad in a message
    - Never forward messages without permission
    - Never open attachments unless expecting them and all your software is patched and your antivirus scanning on
Topics Covered

- E-Mail Encryption
  - Not widely used
  - No single standard
  - Three standards are used in corporations
    - TLS
    - S/MIME
    - PGP (used circles of trust for public keys)
Topics Covered

- Database Security
  - Application authentication beyond login authentication for defense in depth
  - Restrict users to certain data
  - May prohibit access to individual data for privacy reasons
  - Commercial database servers have suffered from vulnerabilities that must be patched
Topics Covered

- Instant Messaging
  - Messages not retained properly
  - File transfers usually not subject to antivirus filtering
  - Relay servers may have all messages pass through them
    - Allows filtering
    - Can stop some vulnerabilities without updating all clients