Threats to Information Security

Sanjay Goel

University at Albany, SUNY

February 17, 2006

Course Outline

Unit 1: What is a Security Assessment?

- Definitions and Nomenclature

Unit 2: What kinds of threats exist?

- Malicious Threats (Viruses & Worms) and Unintentional Threats

Unit 3: What kinds of threats exist? (cont'd)

- Malicious Threats (Spoofing, Session Hijacking, Miscellaneous)

Unit 4: How to perform security assessment?

- Risk Analysis: Qualitative Risk Analysis

Unit 5: Remediation of risks?

- Risk Analysis: Quantitative Risk Analysis

Threats to Information Security

Outline for this unit

Module 1: Spoofing

Module 2: Email Spoofing

Module 3: Web Spoofing

Module 4: Session Hijacking

Module 5: Other Threats

Module 1
Spoofing

Spoofing

Outline

- What is spoofing?
- What types of spoofing are there?
- What are the controls to spoofing?
- What is IP spoofing?
- What are the kinds of IP spoofing?
  - Basic Address Change
  - Source Routing
  - UNIX Trust Relations

Spoofing

Basics

- Definition:
  - Computer on a network pretends to have identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network
- Typical Behaviors:
  - Spoofing computer often doesn't have access to user-level commands so attempts to use automation-level services, such as email or message handlers, are employed
- Vulnerabilities:
  - Automation services designed for network interoperability are especially vulnerable, especially those adhering to open standards.

Spoofing

Types

- IP Spoofing:
  - Typically involves sending packets with spoofed IP addresses to machines to fool the machine into processing the packets
- Email Spoofing:
  - Attacker sends messages masquerading as some one else
- Web Spoofing:
  - Assume the web identity and control traffic to and from the web server

Spoofing

Prevention and Detection

- Prevention:
  - Limit system privileges of automation services to minimum necessary
  - Upgrade via security patches as they become available
- Detection:
  - Monitor transaction logs of automation services, scanning for unusual behaviors
  - If automating this process do so off-line to avoid "tunneling" attacks
- Countermeasures:
  - Disconnect automation services until patched
  - Monitor automation access points, such as network sockets, scanning for next spoof, in attempt to track perpetrator

Spoofing

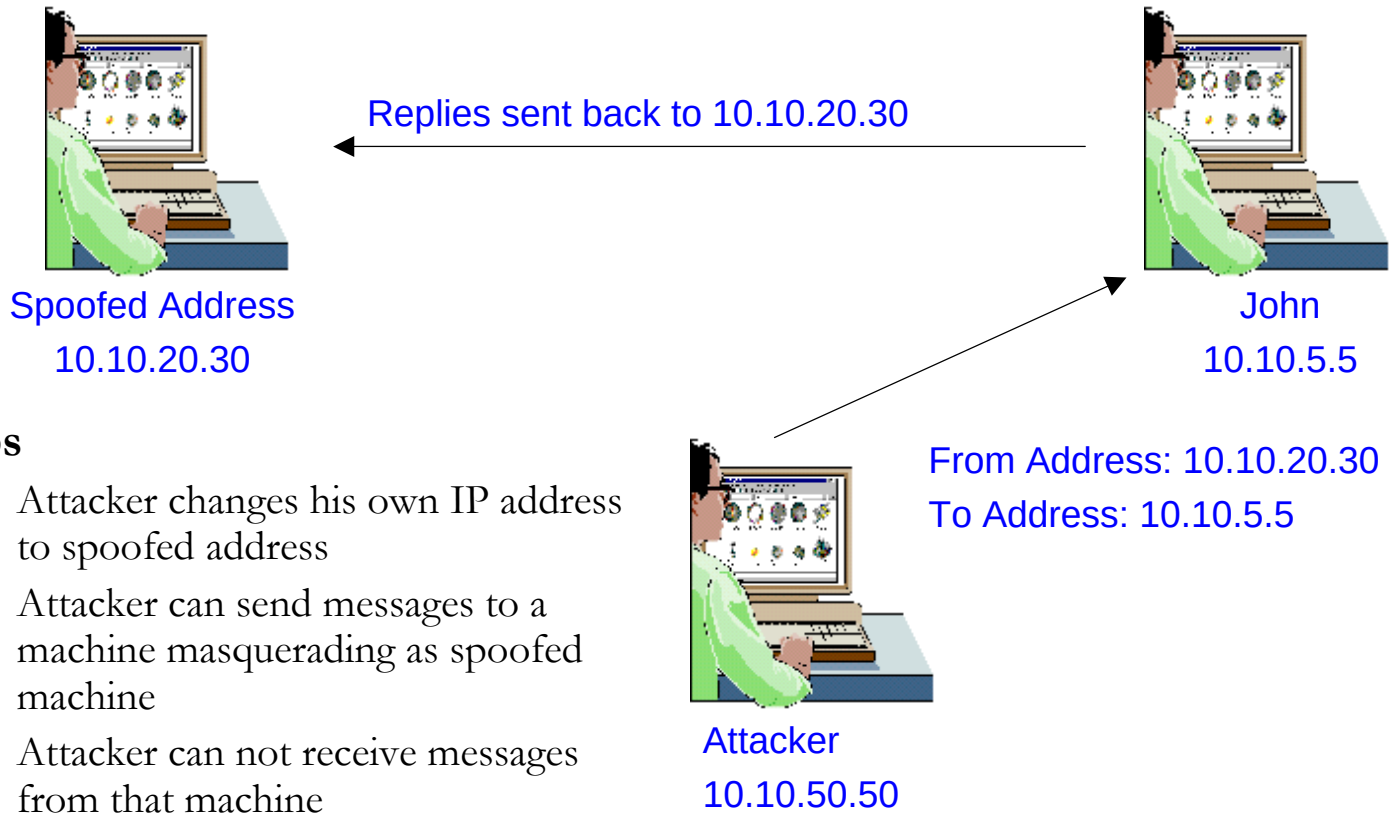
IP Spoofing Types

- Types of IP spoofing
  1. Basic Address Change
  2. Use of source routing to intercept packets
  3. Exploiting of a trust relationship on UNIX machines

Spoofing

IP Spoofing: Basic Address Change

- Attacker uses IP address of another computer to acquire information or gain access to another computer



Steps

1. Attacker changes his own IP address to spoofed address
2. Attacker can send messages to a machine masquerading as spoofed machine
3. Attacker can not receive messages from that machine

Spoofing

IP Spoofing: Basic Address Change, cont'd.

- Simple Mechanism
  - From start menu select settings → Control Panel
  - Double click on the network icon
  - Right click the LAN connection and select properties
  - select Internet Protocol (TCP/IP) and click on properties
  - Change the IP address to the address you want to spoof
  - Reboot the machine
- Limitation
  - Flying Blind Attack (only send packets from own machine, can't get input back)
  - User can not get return messages
- Prevention
  - Protect your machines from being used to launch a spoofing attack
  - Little can be done to prevent other people from spoofing your address

Spoofing

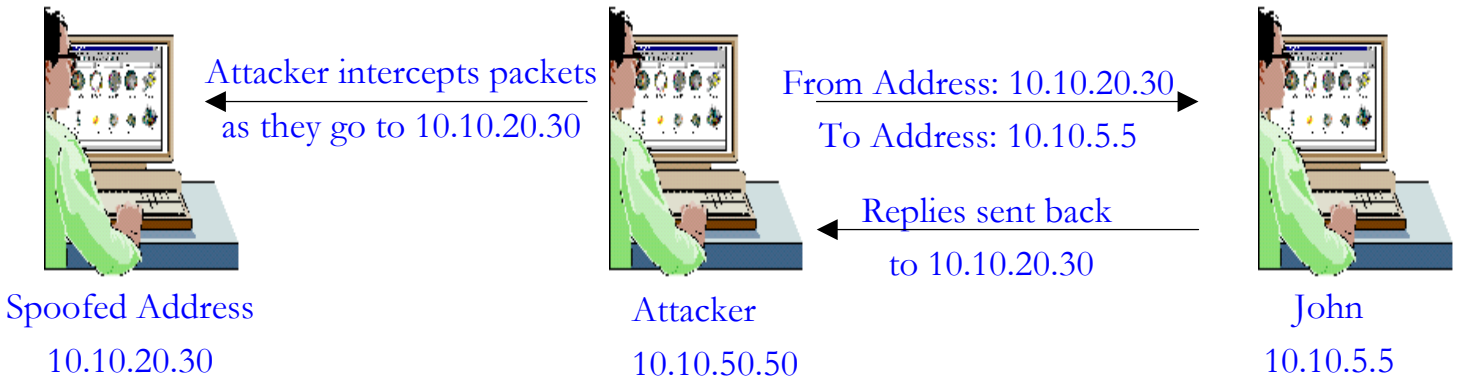
IP Spoofing: Basic Address Change, cont'd.

- Users can be prevented from having access to network configuration
- To protect your company from spoofing attack you can apply basic filters at your routers
  - Ingress Filtering: Prevent packets from outside coming in with address from inside.
  - Egress Filtering: Prevents packets not having an internal address from leaving the network

Spoofing

IP Spoofing: Source Routing

- Attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies
- The path a packet may change can vary over time so attacker uses source routing to ensure that the packets pass through certain nodes on the network



Spoofing

IP Spoofing: Source Routing

- Two modes of source routing
  - Loose Source Routing (LSR): Sender specifies a list of addresses that the packet must go through but the packet can go through other addresses if required.
  - Strict Source Routing (SSR): Sender specifies the exact path for the packet and the packet is dropped if the exact path can not be taken.
- Source Routing works by using a 39-byte source route option field in the IP header
  - Works by picking one node address at a time sequentially
  - A maximum of 9 nodes in the path can be specified
- Source Routing was introduced into the TCP spec for debugging and testing redundancy in the network

Spoofing

IP Spoofing: Tools for Source Routing

- Tracert: Windows NT utility runs at a Command prompt.
- Traces a path from you to the URL or IP address given along with the tracert command.
- Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

  Options:
  - -d — Do not resolve addresses to hostnames.
  - -h maximum_hops — Maximum number of hops to search for target.
  - -j host-list — Loose source route along host-list.
  - -w timeout — Wait timeout milliseconds for each reply.
- Tracing a URL: tracert www.techadvice.com <enter>

  Tracing route to www.techadvice.com [63.69.55.237]
  over a maximum of 30 hops:
  1 181 ms 160 ms 170 ms border0.Srvf.Rx2.abc [63.69.55.237]
  2 170 ms 170 ms 160 ms 192.168.0.2
  3 .....
- Examples
  - e.g. Tracing an IP-Address: tracert 3.1.6.62
  - e.g. Tracing using loose source routing: tracert –j 3.2.1.44 3.3.1.42
- Protection: Disable source routing at routers

Spoofing

IP Spoofing: Unix Trust Relations

- In UNIX trust relationships can be set up between multiple machines
  - After trust becomes established the user can use Unix r-commands to access sources on different machines
  - A .rhosts file is set up on individual machines or /etc/hosts.equiv is used to set it up at the system level
- Trust relationship is easy to spoof
  - If user realizes that a machine trusts the IP address 10.10.10.5 he can spoof that address and he is allowed access without password
  - The responses go back to the spoofed machine so this is still a flying blind attack.
- Protection
  - Do not use trust relations
  - Do not allow trust relationships on the internet and limit them within the company
  - Monitor which machines and users can have trust without jeopardizing critical data or function

Spoofing

Questions 1 and 2

1) What is spoofing?

2) What types of spoofing exist?

Spoofing

Questions 3, 4 and 5

3) What are the limitations to the basic address change type of IP spoofing?

4) What are the two modes of the source routing type of IP spoofing?

5) Why are UNIX trust relationships easy to spoof?

Module 2
Email Spoofing

Email Spoofing

Outline

- What is email spoofing?
- Why do people spoof email?
- What are the types of email spoofing?
  - Similarly named accounts
  - Email configuration changes
  - Telnet to Port 25

Email Spoofing

Basics

Definition:

Attacker sends messages masquerading as some one else

What can be the repercussions?

Reasons:

- Attackers want to hide their identity while sending messages (sending anonymous emails)
  - User sends email to anonymous e-mailer which sends emails to the intended recipient
- Attacker wants to impersonate someone
  - To get someone in trouble
- Social engineering
  - Get information by pretending to be someone else

Email Spoofing

Types

- Types of email spoofing
  - Fake email accounts
  - Changing email configuration
  - Telnet to mail port

Email Spoofing

Similar Name Account

- Create an account with similar email address
  - SanjayGoel@yahoo.com: A message from this account can perplex the students
  - Most mailers have an alias field (this can be used to prescribe any name.
- Example

  Class:

  I am too sick to come to the class tomorrow so the class is cancelled.

  The assignments that were due are now due next week.

  Sanjay Goel

Email Spoofing

Similar Name Account

- Protection
  - Educating the employees in a corporation to be cautious
  - Make sure that the full email address rather than alias is displayed
  - Institute policy that all official communication be done using company email
  - Use PKI where digital signature of each employee is associated with the email

Email Spoofing

Mail Client

- Modify a mail client
  - When email is sent from the user no authentication is performed on the from address
  - Attacker can put in any return address he wants to in the mail he sends
- Protection
  - Education
  - Audit Logging
  - Looking at the full email address

Email Spoofing

Telnet to Port 25

- Telnet to port 25
  - Most mail servers use port 25 for SMTP.
  - An attacker runs a port scan and gets the IP address of machine with port 25 open
  - telnet IP address 25 (cmd to telnet to port 25)
  - Attacker logs on to this port and composes a message for the user.
- Example:

  Hello

  mail from:spoofed-email-address

  Rcpt to: person-sending-mail-to

  Data (message you want to send)

  Period sign at the end of the message

Email Spoofing

Telnet to Port 25

- Mail relaying is the sending of email to a person on a different domain
  - Used for sending anonymous email messages
- Protection
  - Make sure that the recipients domain is the same as the the mail server
  - New SMTP servers disallow mail relaying
  - From a remote connection the from and to addresses are from the same domain as the mail server
  - Make sure that spoofing and relay filters are configured

Email Spoofing

Questions 1 and 2

1) Why is email spoofing done?

2) List the different types of email spoofing.

Email Spoofing

Questions 3, 4 and 5

3) How do you prevent receiving mail from a configuration-changed mail client?

4) What is type of email spoofing is this an example of?

Real address for John Doe: johndoe@hotmail.com

Fake address set for John Doe: johndoe@aol.com

5) Try to use telnet email spoofing in your own home computer to send a "fake" email message to yourself.

Module 3
Web Spoofing

Web Spoofing

Outline

- What are the types of web spoofing?
  - Basic
  - Man-in-the-middle
  - URL Rewriting
  - Tracking state (maintaining authentication within a site)
- What are the ways to track state?
  - Cookies
  - URL encoding
  - Hidden form fields
- How to protect against web spoofing?

Web Spoofing

Types

- Types of Web Spoofing
  - Basic
  - Man-in-the-Middle Attack
  - URL Rewriting
  - Tracking State

Web Spoofing

Basic

- No requirement against registering a domain
  - Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com
- Process
  - Hacker sets up a spoofed site
  - User goes to the spoofed site
  - Clicks on items to order and checks out
  - Site prompts user for credit card information
  - Gives the user a cookie
  - Puts message – Site experiencing technical difficulty
  - When user tries back spoofed site checks cookie
  - Already has credit card number so directs the user to legitimate site

Web Spoofing

Basic, cont'd.

- Protection
  - Use server side certificates
  - Certificates much harder to spoof
  - Users need to ensure that the certificates are legitimate before clicking on OK to accept certificate

Web Spoofing

Man in the Middle Attack

- Man-in-the-Middle Attack
  - Attacker acts as a proxy between the web server and the client
  - Attacker has to compromise the router or a node through which the relevant traffic flows
- Protection
  - Secure the perimeter to prevent compromise of routers

Web Spoofing

URL Rewriting

- URL Rewriting
  - Attacker redirects web traffic to another site that is controlled by the attacker
  - Attacker writes his own web site address before the legitimate link
  - e.g. <A href="http://www.hacker.com/http://www.albany.edu/index.html">
  - The user is first directed to the hacker site and then redirected to the actual site
- Protections
  - Web browsers should be configured to always show complete address
  - Ensure that the code for the web sites is properly protected at the server end and during transit

Web Spoofing

Tracking State

- Web Sites need to maintain persistent authentication so that user does not have to authenticate repeatedly
- Http is a stateless protocol
  - Tracking State is required to maintain persistent authentication
- This authentication can be stolen for masquerading as the user

Web Spoofing

Tracking State

- Three types of tracking methods are used:
  - Cookies: Text containing ID of the user stored in the cookie file
    - Attacker can read the ID from users cookie file
  - URL Session Tracking: An id is appended to all the links in the website web pages.
    - Attacker can guess or read this id and masquerade as user
  - Hidden Form Elements
    - ID is hidden in form elements which are not visible to user
    - Hacker can modify these to masquerade as another user

Web Spoofing

Tracking State Cookies

- Cookies are pieces of information that the server passes to the browser and the browser stores on the user's machine.
  - Set of name value pairs
- Web servers place cookies on user machines with id to track the users
- Two types of cookies
  - Persistent cookies: Stored on hard drive in text format
  - Non-persistent cookies: Stored in memory and goes away after you reboot or turn off the machine
- Attacker gets cookies by:
  - Accessing the victim hard drive
  - Guessing Ids which different web servers assign

Web Spoofing

Tracking State Cookies

- For protection, website designers should use:
  - Physical protection of hard drives is best protection
  - Non-persistent cookies since hacker has to access and edit memory to get to it.
  - Random hard to guess ID (could be a random number in between 1 to 1000)

Web Spoofing

Tracking State URL Encoding

- http:// www.address.edu:1234/path/subdir/file.ext?query_string
  - Service → http
  - Host → www. Address. edu
  - Port → 1234
  - /path/subdur/file.ext → resource path on the server
  - query_string → additional information that can be passed to resource
- HTTP allows name value pairs to be passed to the server
  - http://www.test.edu/index.jsp?firstname=sanjay+lastname=goel
- The server can place the id of a customer along with the URL
  - http://www.fake.com/ordering/id=928932888329938.823948
- This number can be obtained by guessing or looking over some one's shoulder
  - Timeout for the sessions may be a few hours
  - User can masquerade as the owner of the id and transact on the web

Web Spoofing

URL Encoding Protection

- Server Side
  - Use large hard to guess identifiers
  - Keep the session inactivity time low
- User Side
  - Make sure that no one is looking over your shoulder as you browse
  - Do not leave terminals unattended
- Use server side certificates
  - A server side certificate is a certificate that the server presents to a client to prove identity
  - Users should verify the certificates prior to clicking OK on the accept button

Web Spoofing

Tracking State Hidden Form Fields

- HTML allows creation of hidden fields in the forms
- Developers exploit this to store information for their reference
- ID can be stored as a hidden form field
  - <Input Type=Hidden Name="Search" Value="key">
  - <Input Type=Hidden Name="id" Value="123429823">
- Protection
  - Hard to guess ids
  - Short expiration times for cookies

Web Spoofing

General Protection

- Disable JavaScript, ActiveX and other scripting languages that execute locally or in the browser
- Make sure that browser's URL address line is always visible
- Educate the users
- Make hard-to-guess session IDs
- Use server side certificates
  - A server side certificate is a certificate that the server presents to a client to prove identity
  - Users should verify the certificates prior to clicking OK on the accept button

Web Spoofing

Questions 1a and 1b

1a) Why is web spoofing done?

1b) List the various types of web spoofing.

Web Spoofing

Question 2 and 3

2) What would be controls for preventing URL rewriting?

3) Describe how the man-in-the-middle attack works.

Web Spoofing

Questions 4 and 5

4) Why is tracking state important?

5) What are the different ways to track state?

Module 4
Session Hijacking

References

Sources & Further Reading

- CERT & CERIAS Web Sites
- Information Security Guideline for NSW Government- Part 2: Examples of Threats and Vulnerabilities
- Security by Pfleeger & Pfleeger
- Hackers Beware by Eric Cole
- NIST web site
- Other web sources