Attacks

Outlines:

- Crisis
- Computer Crimes
- Hacker Attacks
- Modes of Computer Security
  - Password Security
  - Network Security
  - Web Security
  - Distributed Systems Security
  - Database Security

By: Arash Habibi Lashkari

July - 2010

Topics

- Crisis
- Computer Crimes
- Hacker Attacks
- Modes of Computer Security
  - Password Security
  - Network Security
  - Web Security
  - Distributed Systems Security
  - Database Security

Crisis

- Internet has grown very fast and security has lagged behind.
- Legions of hackers have emerged as impedance to entering the hackers club is low.
- It is hard to trace the perpetrator of cyber attacks since the real identities are camouflaged
- It is very hard to track down people because of the ubiquity of the network.
- Large scale failures of internet can have a catastrophic impact on the economy which relies heavily on electronic transactions

Computer Crime – The Beginning

- In 1988 a "worm program" written by a college student shut down about 10 percent of computers connected to the Internet. This was the beginning of the era of cyber attacks.
- Today we have about 10,000 incidents of cyber attacks which are reported and the number grows.

Computer Crime - 1994

- A 16-year-old music student called Richard Pryce, better known by the hacker alias Datastream Cowboy, is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, Nasa and the Korean Atomic Research Institute. His online mentor, "Kuji", is never found.

- Also this year, a group directed by Russian hackers broke into the computers of Citibank and transferred more than $10 million from customers' accounts. Eventually, Citibank recovered all but $400,000 of the pilfered money.

Computer Crime - 1995

- In February, Kevin Mitnick is arrested for a second time. He is charged with stealing 20,000 credit card numbers. He eventually spends four years in jail and on his release his parole conditions demand that he avoid contact with computers and mobile phones.
- On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Mr Pile, who called himself the Black Baron, was sentenced to 18 months in jail.
- The US General Accounting Office reveals that US Defense Department computers sustained 250,000 attacks in 1995.

Computer Crime - 1999

- In March, the Melissa virus goes on the rampage and wreaks havoc with computers worldwide. After a short investigation, the FBI tracks down and arrests the writer of the virus, a 29-year-old New Jersey computer programmer, David L Smith.

- More than 90 percent of large corporations and government agencies were the victims of computer security breaches in 1999

Computer Crime - 2000

- In February, some of the most popular websites in the world such as Amazon and Yahoo are almost overwhelmed by being flooded with bogus requests for data.
- In May, the ILOVEYOU virus is unleashed and clogs computers worldwide. Over the coming months, variants of the virus are released that manage to catch out companies that didn't do enough to protect themselves.
- In October, Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen.

Why Security?

- Some of the sites which have been compromised
  - U.S. Department of Commerce
  - NASA
  - CIA
  - Greenpeace
  - Motorola
  - UNICEF
  - Church of Christ …
- Some sites which have been rendered ineffective
  - Yahoo
  - Microsoft
  - Amazon …

Why do Hackers Attack?

- Because they can
  - A large fraction of hacker attacks have been pranks
- Financial Gain
- Espionage
- Venting anger at a company or organization
- Terrorism

Types of Hacker Attack

- Active Attacks
  - Denial of Service
  - Breaking into a site
    - Intelligence Gathering
    - Resource Usage
    - Deception
- Passive Attacks
  - Sniffing
    - Passwords
    - Network Traffic
    - Sensitive Information
  - Information Gathering

Modes of Hacker Attack

- Over the Internet
- Over LAN
- Locally
- Offline
- Theft
- Deception

Spoofing

Definition:

An attacker alters his identity so that some one thinks he is some one else

- Email, User ID, IP Address, …
- Attacker exploits trust relation between user and networked machines to gain access to machines

Types of Spoofing:

1. IP Spoofing:
2. Email Spoofing
3. Web Spoofing

IP Spoofing – Flying-Blind Attack

Definition:

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

Spoofed Address
10.10.20.30

Replies sent back to 10.10.20.30

John
10.10.5.5

From Address: 10.10.20.30
To Address: 10.10.5.5

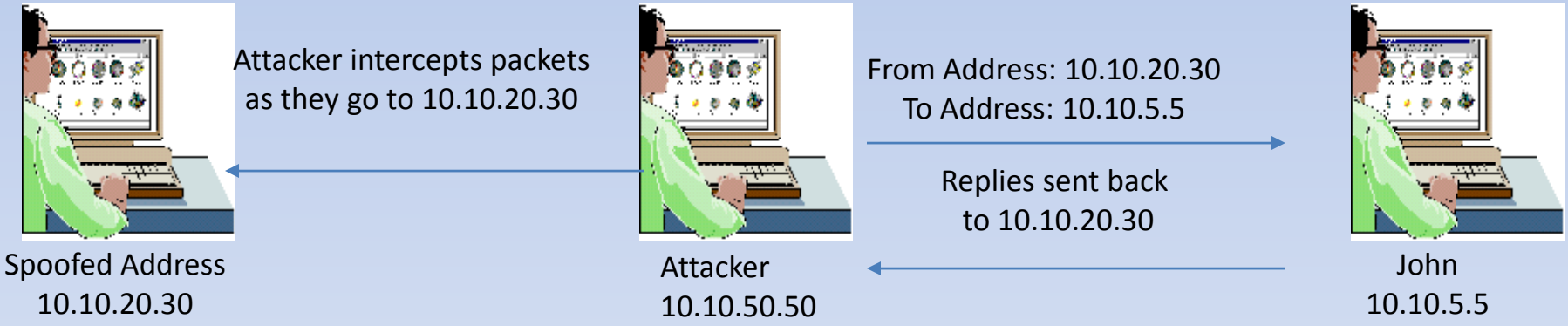
Attacker
10.10.50.50

- Attacker changes his own IP address to spoofed address
- Attacker can send messages to a machine masquerading as spoofed machine
- Attacker can not receive messages from that machine

IP Spoofing – Source Routing

Definition:

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
- To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network

Email Spoofing

Definition:

Attacker sends messages masquerading as some one else

What can be the repercussions?

Types of Email Spoofing:

1. Create an account with similar email address
   - Sanjaygoel@yahoo.com: A message from this account can perplex the students
2. Modify a mail client
   - Attacker can put in any return address he wants to in the mail he sends
3. Telnet to port 25
   - Most mail servers use port 25 for SMTP. Attacker logs on to this port and composes a message for the user.

Web Spoofing

- Basic
  - Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com
- 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
- 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
- Tracking State
  - When a user logs on to a site a persistent authentication is maintained
  - This authentication can be stolen for masquerading as the user

Web Spoofing – Tracking State

- Web Site maintains authentication so that the user does not have to authenticate repeatedly
- Three types of tracking methods are used:
  1. Cookies: Line of text with ID on the users cookie file
     - Attacker can read the ID from users cookie file
  2. 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
  3. Hidden Form Elements
     - ID is hidden in form elements which are not visible to user
     - Hacker can modify these to masquerade as another user

Session Hijacking

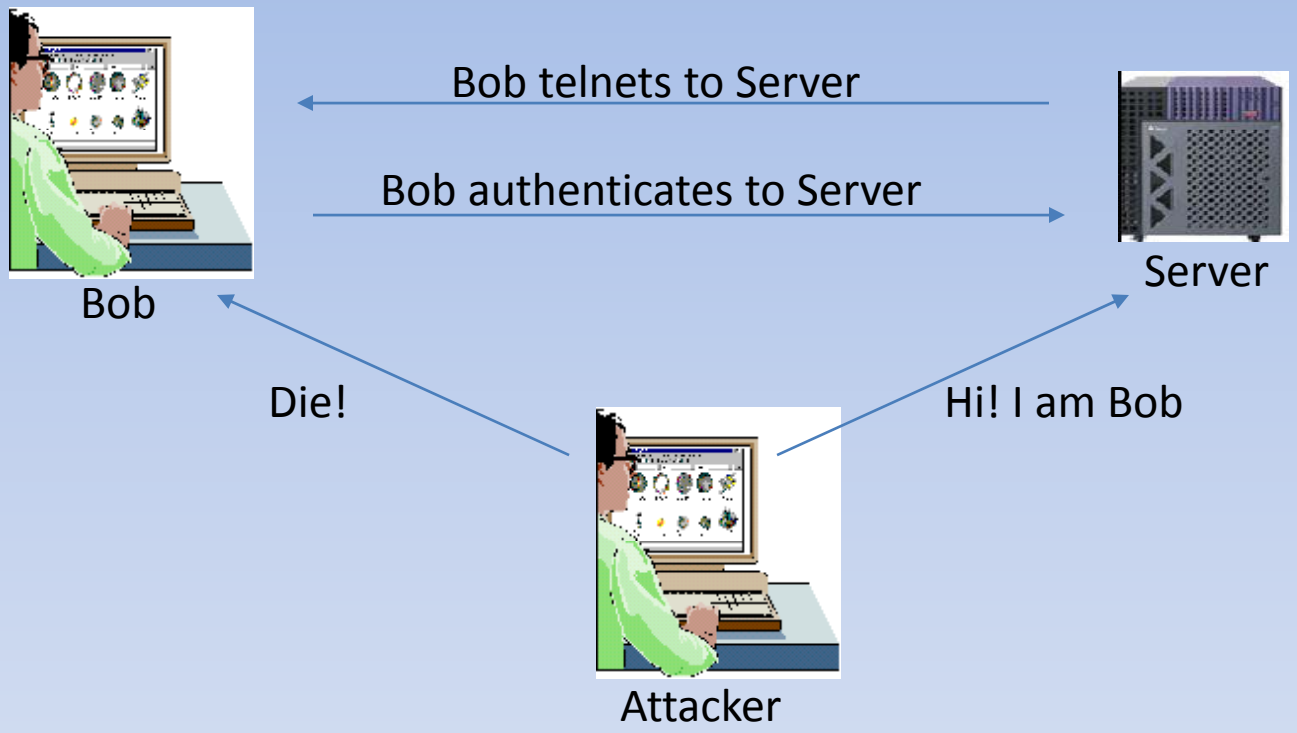
Definition:

Process of taking over an existing active session

Modus Operandi:

1. User makes a connection to the server by authenticating using his user ID and password.
2. After the users authenticate, they have access to the server as long as the session lasts.
3. Hacker takes the user offline by denial of service
4. Hacker gains access to the user by impersonating the user

Session Hijacking



- Attacker can
  - monitor the session
  - periodically inject commands into session
  - launch passive and active attacks from the session

Session Hijacking – How Does it Work?

- Attackers exploit sequence numbers to hijack sessions
- Sequence numbers are 32-bit counters used to:
  - tell receiving machines the correct order of packets
  - Tell sender which packets are received and which are lost
- Receiver and Sender have their own sequence numbers
- When two parties communicate the following are needed:
  - IP addresses
  - Port Numbers
  - Sequence Number
- IP addresses and port numbers are easily available so once the attacker gets the server to accept his guesses sequence number he can hijack the session.

Denial of Service (DOS) Attack

Definition:

Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it.

Types:

1. Crashing the system or network
   - Send the victim data or packets which will cause system to crash or reboot.
2. Exhausting the resources by flooding the system or network with information
   - Since all resources are exhausted others are denied access to the resources
3. Distributed DOS attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks

Denial of Service (DOS) Attack

Types:

1. Ping of Death
2. SSPing
3. Land
4. Smurf
5. SYN Flood
6. CPU Hog
7. Win Nuke
8. RPC Locator
9. Jolt2
10. Bubonic
11. Microsoft Incomplete TCP/IP Packet Vulnerability
12. HP Openview Node Manager SNMP DOS Vulneability
13. Netscreen Firewall DOS Vulnerability
14. Checkpoint Firewall DOS Vulnerability

Buffer Overflow Attacks

- Programs which do not do not have a rigorous memory check in the code are vulnerable to this attack
- Simple weaknesses can be exploited
  - If memory allocated for name is 50 characters, someone can break the system by sending a fictitious name of more than 50 characters
- Can be used for espionage, denial of service or compromising the integrity of the data

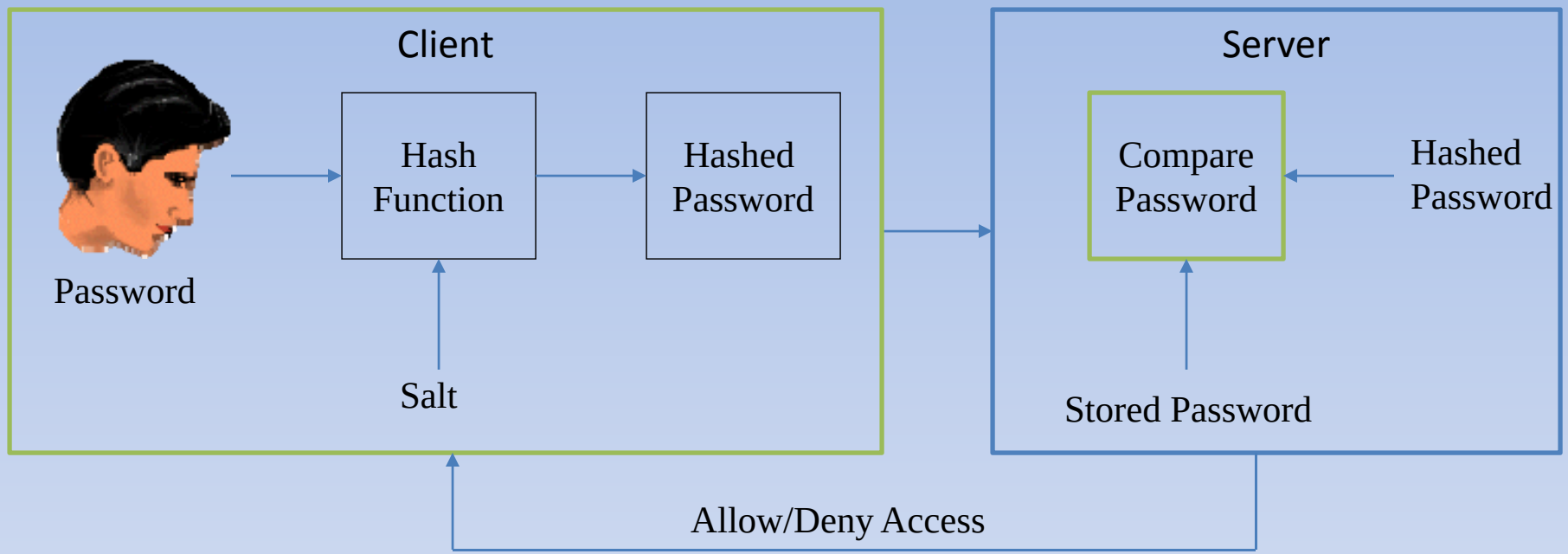
Examples

- NetMeeting Buffer Overflow
- Outlook Buffer Overflow
- AOL Instant Messenger Buffer Overflow
- SQL Server 2000 Extended Stored Procedure Buffer Overflow

Password Attacks

- A hacker can exploit a weak passwords & uncontrolled network modems easily
- Steps
  - Hacker gets the phone number of a company
  - Hacker runs war dialer program
    - If original number is 555-5532 he runs all numbers in the 555-55xx range
    - When modem answers he records the phone number of modem
  - Hacker now needs a user id and password to enter company network
    - Companies often have default accounts e.g. temp, anonymous with no password
    - Often the root account uses company name as the password
    - For strong passwords password cracking techniques exist

Password Security



- Password hashed and stored
  - Salt added to randomize password & stored on system
- Password attacks launched to crack encrypted password

Password Attacks - Process

- Find a valid user ID
- Create a list of possible passwords
- Rank the passwords from high probability to low
- Type in each password
- If the system allows you in – success !
- If not, try again, being careful not to exceed password lockout (the number of times you can guess a wrong password before the system shuts down and won't let you try any more)

Password Attacks - Types

- Dictionary Attack
  - Hacker tries all words in dictionary to crack password
  - 70% of the people use dictionary words as passwords
- Brute Force Attack
  - Try all permutations of the letters & symbols in the alphabet
- Hybrid Attack
  - Words from dictionary and their variations used in attack
- Social Engineering
  - People write passwords in different places
  - People disclose passwords naively to others
- Shoulder Surfing
  - Hackers slyly watch over peoples shoulders to steal passwords
- Dumpster Diving
  - People dump their trash papers in garbage which may contain information to crack passwords

Conclusions

- Computer Security is a continuous battle
  - As computer security gets tighter hackers are getting smarter
- Very high stakes

Questions

Wireshark and monitor the packets of special ports