Lecture 21: Malware and Cyber Attacks

COSC362 Data and Network Security

Book 2: Chapter 6

Spring Semester, 2021

Motivation

- Attacks have been recurrent.
- Scale extensively varies:
  - From one computer to million computers worldwide.
- Many attempts to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.
- Goals broadly vary:
  - Disabling the target computer or knocking it offline.
  - Getting access to the target computer’s data and perhaps gaining admin privileges on it.

Outline

Attack Classification

Attack Methods

- Social Engineering
- Hacking and Cracking
- Viruses and Worms
- Trojan Horses
- Denial of Service (DoS) Attacks
- Rootkits
- Blended Threats
- Zero-Day Attacks
- Bots and Botnets
- Buffer Overflow

Outline

Attack Classification

Attack Methods

- Social Engineering
- Hacking and Cracking
- Viruses and Worms
- Trojan Horses
- Denial of Service (DoS) Attacks
- Rootkits
- Blended Threats
- Zero-Day Attacks
- Bots and Botnets
- Buffer Overflow

Methods

- *Social engineering:* Persuading somebody to do something.
- *Hacking or cracking:* Guessing, corrupting or stealing information.
- *Viruses and worms (malware):*
  - A virus propagates by inserting a copy of itself into and becoming part of another program.
    - Melissa, CryptoMix.
  - A worm replicates functional copies of itself but does not require a host program's help to propagate.
    - WannaCry, Code-Red, Nimda, Slammer.
- *Trojan horses:* A harmful piece of software that looks legitimate.
  - Backdoor trojan, downloader trojan, ransom trojan.

Methods

- *Network layer attacks:* IP spoofing (masquerading), sequence number prediction, TCP hijacking.
- *Web-based attacks:* Cross-site scripting, cooking poisoning, SQL injection.
- *Denial of service (DoS):*
  - Operating system attacks: Ping of Death, Tear Drop, Land, Snork.
  - Network attacks: SYN flood, TCP fin/rst, Smurf, Coke.
  - Distributed DoS: Cayosin, TCP Flood, Reflection.
- *Others...*

Outline

Attack Classification

Attack Methods
- Social Engineering
- Hacking and Cracking
- Viruses and Worms
- Trojan Horses
- Denial of Service (DoS) Attacks
- Rootkits
- Blended Threats
- Zero-Day Attacks
- Bots and Botnets
- Buffer Overflow

Overview

- Persuading someone to disclose sensitive information:
  - Example: phishing attacks on bank customers.
- Persuading someone to run/install malicious or subverted software.
- Inviting someone to log into a bogus website:
  - Example: spoofed bank website.
- Impersonating a new employee who has forgotten user ID and/or password.
- Impersonating a technical support staff member and requesting a user login to “check” accounts.

Spear Phishing Attacks

- Generally an email appearing to be from an individual or business that users know.
- Looking for credit card and bank account numbers, passwords, and other financial information.
- Example: Westpac Australia (2004):
  - “Dear client of the Westpac Bank,
    The recent cases of fraudulent use of clients accounts forced the Technical Services of the bank to update the software. We regret to acknowledge that some data on users accounts could be lost. The administration kindly asks you to follow the reference given below and to sign in to your online banking account:
    `https://oIb.westpac.com.au/ib/default.asp`.
    We are grateful for your cooperation.”

Overview

- Password discovery: default passwords (“guest”, etc.).
- Password cracking tools, readily available from the Internet for a wide range of password protected systems:
  - UNIX password files, Word documents, ZIP files, Windows password files, etc.
- 15 GB of passwords: `https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm`

Password Attacks

- Brute force attacks: few characters.
- Dictionary attacks: real-word passwords.
- Tools:
  - CRACK: `www.pwcrack.com`
  - L0phtcrack: `www.l0phtcrack.com`
  - John the Ripper: `www.openwall.com/john`
- One-time passwords (OTPs) are valuable!

Viruses

- Executable piece of code.
- Travelling and spreading by attaching itself to legitimate executable programs.
- Causing some unexpected and usually undesirable behaviour.
- Automatically spreading to other computer users:
  - Example: By transferring infected files via email attachments.

Worms

- Computer program run independently.
- Propagating a complete working version of itself onto other hosts on a network:
    - Usually by exploiting software vulnerabilities in the target systems.

Overview

- Unlike viruses and worms, not infecting files and not propagating.
- Installing a trojan horse allows an attacker to access a user's machine remotely via the Internet.
- Components:
  - Client application run on the attacker's computer.
  - Server application run on the victim's computer.
- A program pretending to be benign but containing a malicious code.
- Normally waiting to be downloaded or installed by a user, and then executing attack:
  - Example: email attachment.
- Computers on a network are then scanned to locate any with a trojan installed, creating a *botnet*.

Zeus

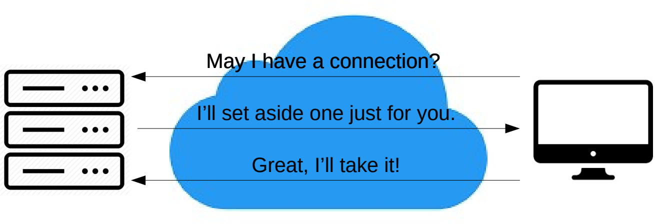
- Stealing banking information by keystroke logging.
- Spreading through drive-by downloads and phishing schemes.
- Compromising thousands of accounts on websites of companies:
  - Examples: Bank of America, NASA, Oracle, Cisco, Amazon.
- Current botnet estimated to include million of compromised computers (3.6 million in USA).
- Currently the largest botnet on the Internet.

Overview

- Intention: Making network services unavailable to users (rather than gaining illegal access).
- Flooding attacks overload servers.
- Examples: Ping o’ Death, SYN flood, ICMP redirect messages.
- Financial incentive and extorsion.
- No magic solution:
  - Sharing services across different servers.
  - Using a properly configured firewall.

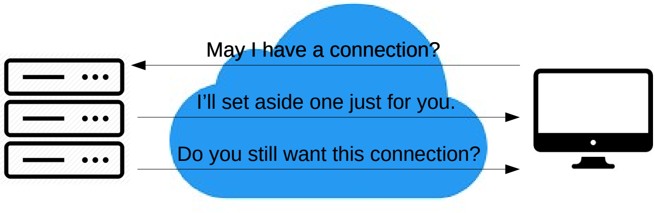
Normal TCP Connection Setup

TCP SYN-ACK Sequence:



Abnormal TCP Connection Setup

TCP SYN-ACK Sequence:



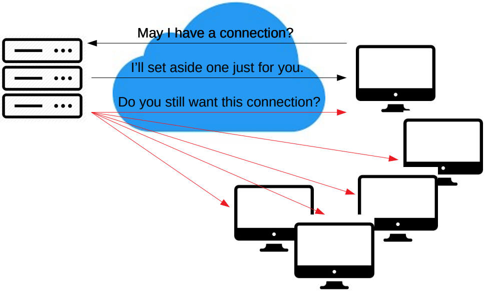
May I have a connection?

I'll set aside one just for you.

Do you still want this connection?

Organised DoS Attack

TCP SYN-ACK Sequence:


May I have a connection?
I'll set aside one just for you.
Do you still want this connection?

- Over time, other requests will not be serviced.
- System locks up, does not really die (just impaired).

Overview

- Collection of programs that hackers use to mask intrusion and obtain admin access.
- An intruder installs a rootkit after obtaining user-level access:
  - By exploiting known vulnerability or cracking password.
- Collecting user IDs and passwords to other machines on the network:
  - Thus giving the hacker root/privilege access.

Utilities

- Monitoring traffic and keystrokes.
- Creating a “backdoor” into the system for hacker’s use.
- Altering log files.
- Attacking other machines on the network.
- Altering existing system tools to circumvent detection.

Remarks:

- Available for a number of operating systems.
- Increasingly difficult to detect on any network.

Overview

Software exploit that involves a combination of attacks against different vulnerabilities:

- Worms dropping parasitic viruses.
- Destructive trojan horses.
- Password stealers.
- Remote access trojans (RATs).
- Trojanised applications replacing legitimate system tools.
- Multiplatform attacks:
  - Payloads affecting multiple platforms.
  - Linux worms with drop.exe trojans.
- Advanced persistent threats (APTs).

Remote Access Trojans (RATs)

- Malware threat previously used in attacks against energy sectors.
- Now aimed at organizations using/developing industrial applications and machines.
- Distributed new version of a RAT, called *Havex*:
  - Discovered in 2013 by F-Secure.
  - Hacking into websites of industrial control system (ICS) manufacturers and poisoning their software downloads.

Advanced Persistent Threats (APTs)

- Set of stealthy and continuous computer hacking processes:
  - Involving humans in real-time.
- Targeting organizations for business motives and nations for political motives.
- Requiring a high degree of covertness over a long period of time.
- Sophisticated techniques using malware to exploit vulnerabilities in systems.
- External command and control, continuously monitoring and extracting data off a specific target.
- Examples: Stuxnet, Duqu, Sandworm, BlackEnergy.

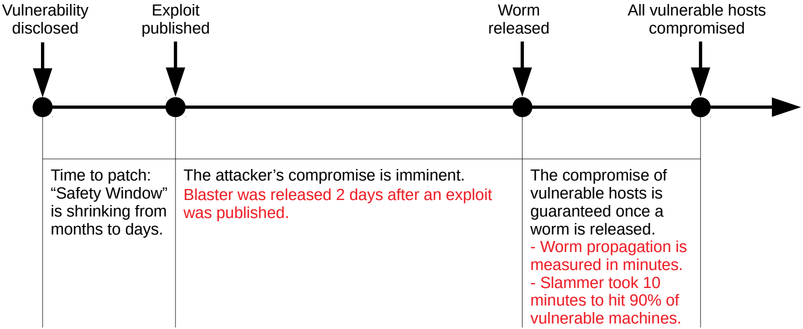
Overview

- Taking advantage of software vulnerabilities for which there is no available fix.
- Taking advantage of flaws before software makers can fix them.
- Emphasizing the importance of safe configuration policies and good incident reporting systems.

Examples

- Malicious hackers are getting faster at exploiting flaws.
- Blaster worm:
  - One of the most virulent ever.
  - Hitting the Internet barely one month after Microsoft released a patch for the flaw it exploited.
- Nachi worm:
  - A variant of Blaster worm.
  - Carrying a dangerous payload.
  - Hitting users less than a week later.
- Timelines are collapsing:
  - Only a matter of time before users see attacks against flaws not yet discovered or for which no patches are available.

Getting Closer



Vulnerability disclosed

Exploit published

Worm released

All vulnerable hosts compromised

Time to patch: “Safety Window” is shrinking from months to days.

The attacker’s compromise is imminent. Blaster was released 2 days after an exploit was published.

The compromise of vulnerable hosts is guaranteed once a worm is released.
- Worm propagation is measured in minutes.
- Slammer took 10 minutes to hit 90% of vulnerable machines.

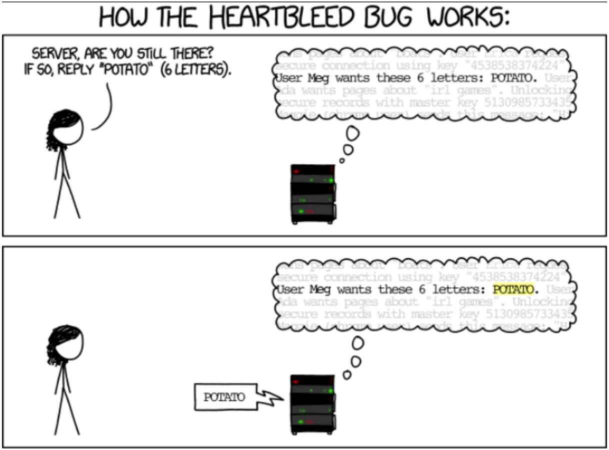
Overview

- Bot:
  - Derived from the word “robot”.
  - Also called *webcrawler*.
  - Software agent interacting with other network services intended for people as if it were a real person.
  - Typical use is gathering information.
- Botnet:
  - Collection of software bots, running autonomously.
  - Usually a collection of compromised machines running worms, trojans or backdoors.

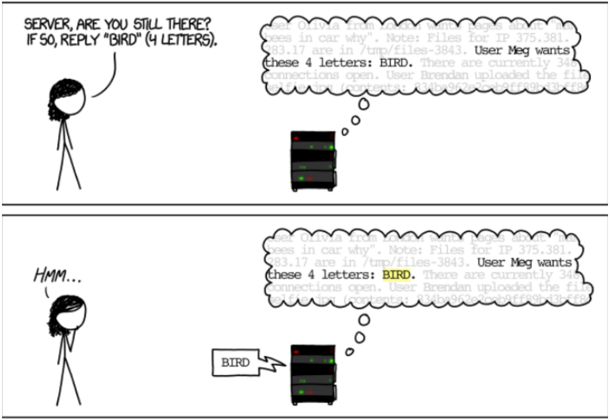
Overview

- Technique used to gain remote execution on host.
- Taking advantage of inadequate buffer boundary checking in applications/services.
- Often involving overwriting return addresses on the stack.
- Involving sending executable code as binary data within the attack data stream:
  - Usually carefully crafted to be located at specific position within a buffer.
- Example: Heartbleed bug:
  - Bug in the OpenSSL's implementation of the SSL/TLS heartbeat extension.
  - When exploited, it leads to the leak of memory contents from the server to the client and from the client to the server.

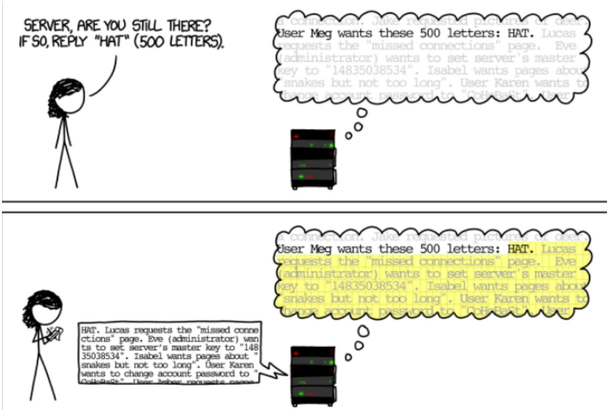
Heartbleed Buffer Overflow


HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
ants pages about "boats". User Erica reques
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Meggie (chrome user) sends this message: "H
ants pages about "boats". User Erica reques
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Meggie (chrome user) sends this message: "H
POTATO

Heartbleed Buffer Overflow


SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
HMM...
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD

Heartbleed Buffer Overflow


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

Heartbleed Attack Scale

- Well-known bug in SSL/TLS.
- Vulnerability exploited to access memory:
  - Secret cryptographic keys.
  - User names, passwords, their contents.
- The bug is public knowledge:
  - Supposed to exist at least 2 years before discovery.
- The highest volume of attacks:
  - Occured when there were more than 300 000 attacks in one day.

In Real World

US hospital hack “exploited Heartbleed flaw“.

- `www.bbc.com/news/technology-28867113`
- 4.5 million healthcare patient data stolen because of delays in patching the 6 vulnerable SSL engines.
- Time between zero-day (i.e. Heartbleed release) and patch day was too long!