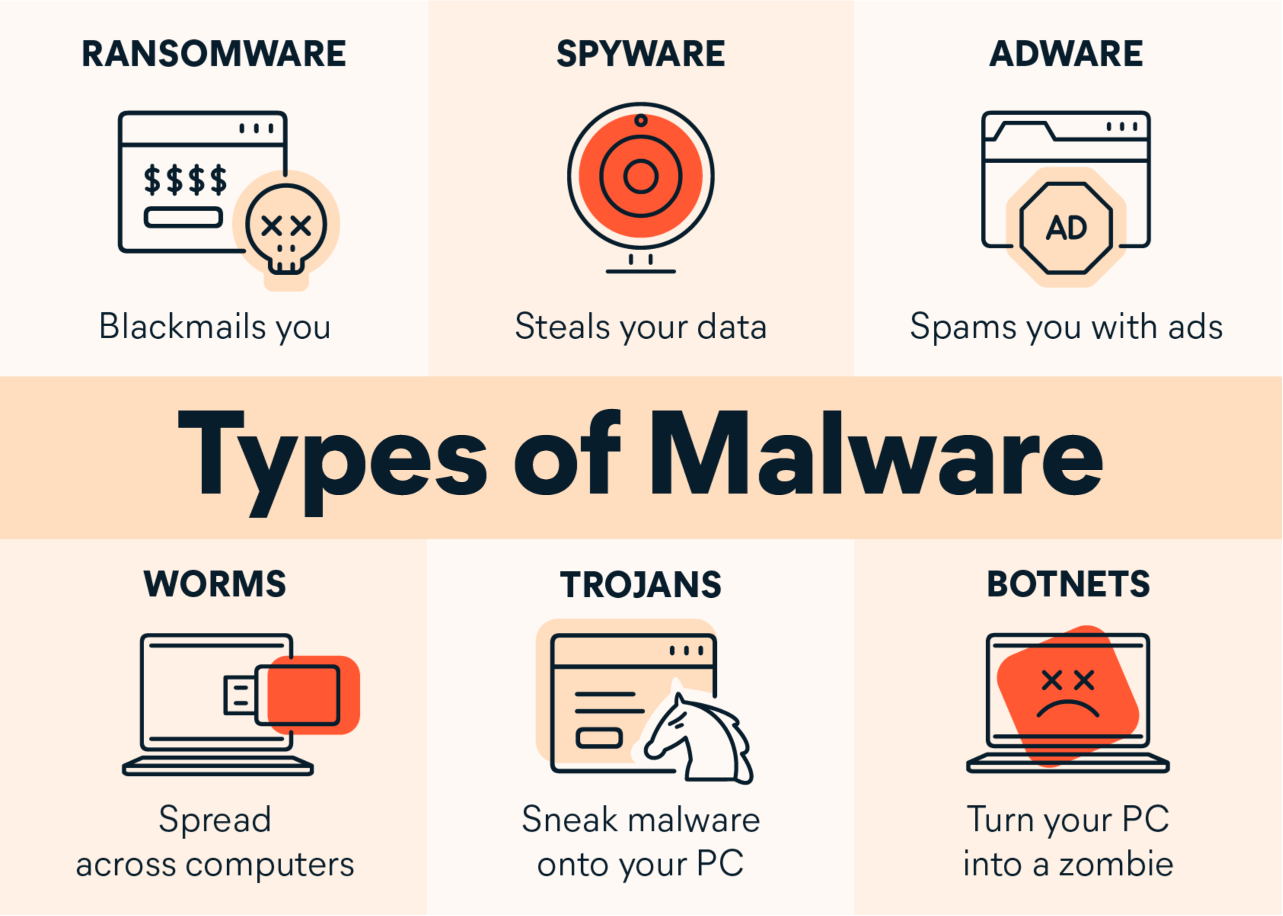
Information Security

Lecture 5: Malwares and Attacks

Mona Taghavi

LaSalle College
Montréal

Common Malwares



Types of Malware

RANSOMWARE
Blackmails you

SPYWARE
Steals your data

ADWARE
Spams you with ads

WORMS
Spread across computers

TROJANS
Sneak malware onto your PC

BOTNETS
Turn your PC into a zombie

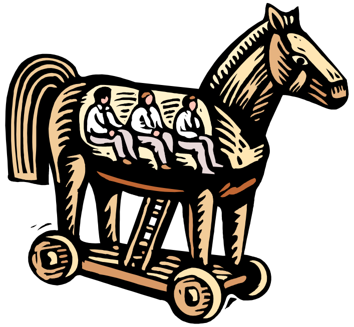
Malwares

- Malware is the general term for malicious software.
- Malware can do a lot of damage:
    - Erase files
    - Deny access to files
    - Create popups
    - Track keystrokes
    - Turn computer into spam email server
    - Disable computer completely
- Malware can be spread through:
    - Email attachments
    - USB drives
    - Programs downloaded off the internet
    - Hackers exploiting vulnerabilities in programs running on your computer

Malware Features

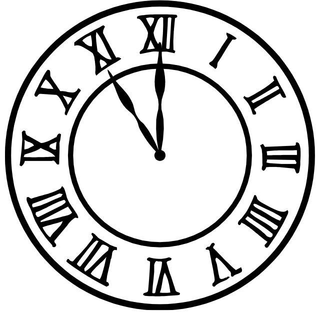
- Infectious:
  - Viruses, worms
- Concealment:
  - Trojan horses, logic bombs, rootkits
- Malware for stealing information:
  - Spyware, keyloggers, screen scrapers
- Malware for profit:
  - Dialers, scarewares, ransomware
- Malware as platform for other attacks
  - Botnets, backdoors (trapdoors)
- Many malwares have characteristics of multiple types

Trojan Horse



- Software that appears to perform a desirable function for the user prior to run or install, but (perhaps in addition to the expected function) steals information or harms the system.
- User tricked into executing Trojan horse
  - Covertly perform malicious acts with user’s authorization
  - Spread occurs when the user installs the “safe” program

Logic Bomb



- Embedded in legitimate programs
- Activated when specified conditions met
  - E.g., presence/absence of some file; Particular date/time or particular user
- When triggered, typically damages system
  - Modify/delete files/disks

Example of Logic Bomb

- In 1982, the Trans-Siberian Pipeline incident occurred. A KGB operative was to steal the plans for a sophisticated control system and its software from a Canadian firm, for use on their Siberian pipeline. The CIA was tipped off by documents in the Farewell Dossier and had the company insert a logic bomb in the program for sabotage purposes. This eventually resulted in “the most monumental non-nuclear explosion and fire ever seen from space”.

Adware

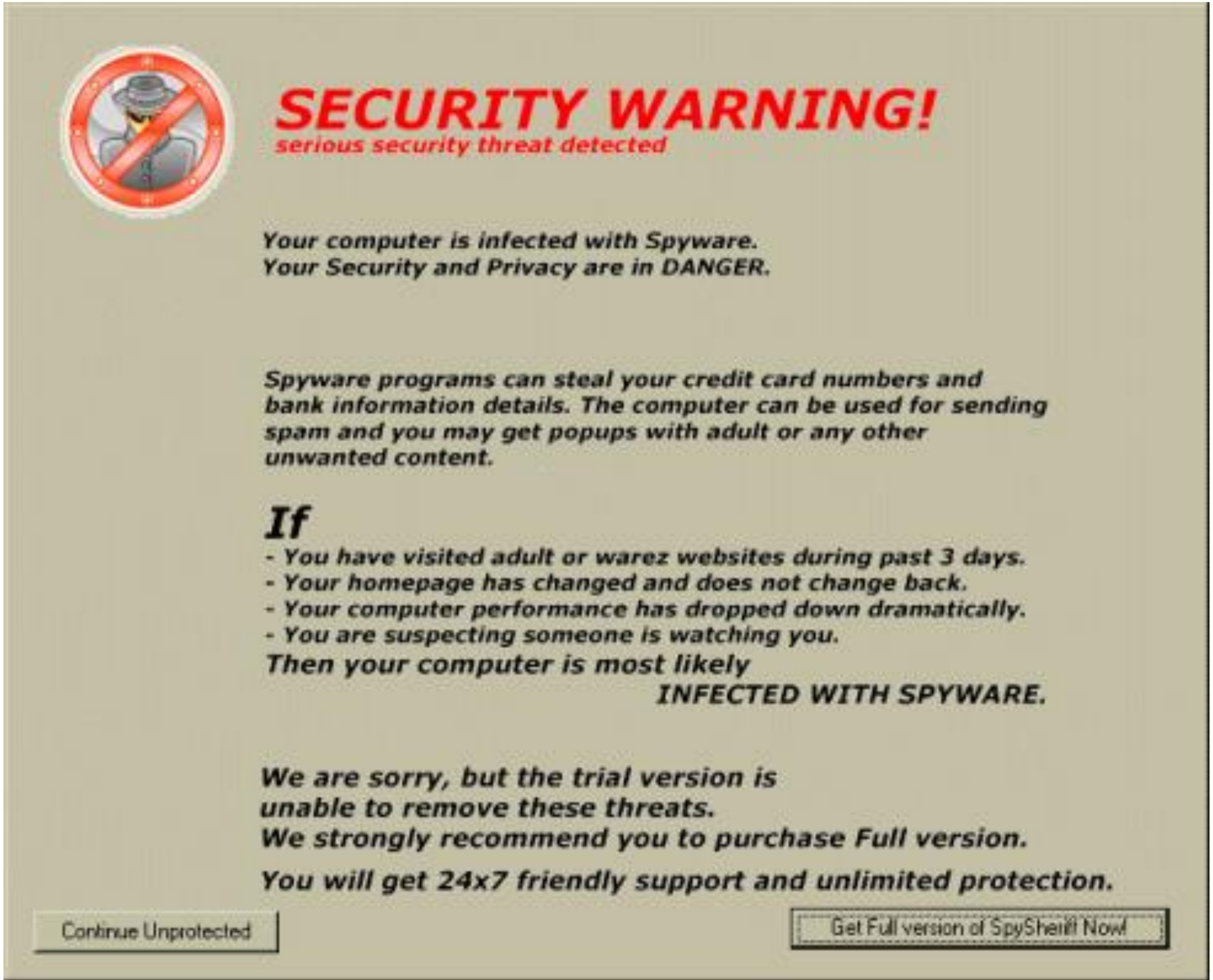
- Serves advertisements in the computer of the user
  - Earn revenues by clicks or visits
  - It can records the users activities and act as spyware

Spyware

- Malware that collects little bits of information at a time about users without their knowledge
  - Keyloggers: stealthly tracking and logging key strokes
  - Screen scrapers: stealthly reading data from a computer display
  - May also tracking browsing habit
  - May also re-direct browsing and display ads

Scareware

- Malware that scares victims into take actions that ultimately end up compromising our own security.
  - E.g., paying for and installing fake anti-virus products



SECURITY WARNING!
serious security threat detected

Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.

Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.

If
- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.

Then your computer is most likely
INFECTED WITH SPYWARE.

We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.

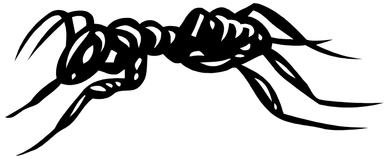
You will get 24x7 friendly support and unlimited protection.

Ransomware

- Holds a computer system, or the data it contains, hostage against its user by demanding a ransom.
  - Disable an essential system service or lock the display at system startup
  - Encrypt some of the user's personal files, originally referred to as **cryptoviruses**, **cryptotrojans** or **cryptoworms**
- Victim user has to
  - enter a code obtainable only after

  wiring payment to the attacker

Virus



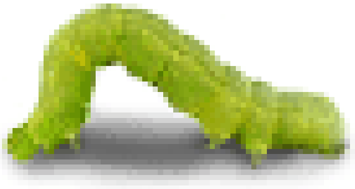
- Self-replicating code
  - Like replicating Trojan horse
  - Alters normal code with “infected” version
- Operates when infected code executed

```
If spread condition then
    For target files
        if not infected then alter to include virus
Perform malicious action
Execute normal program
```

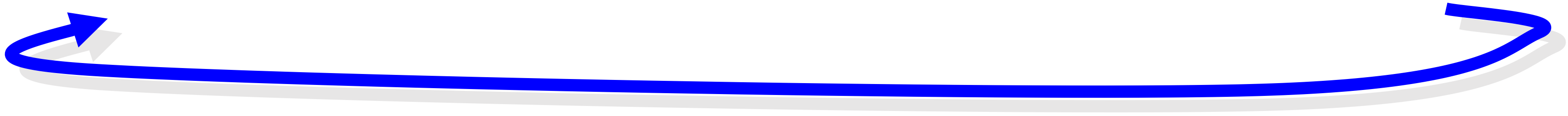
- Useful video to watch:

  http://www.commoncraft.com/video/computer-viruses-and-threats

Worm

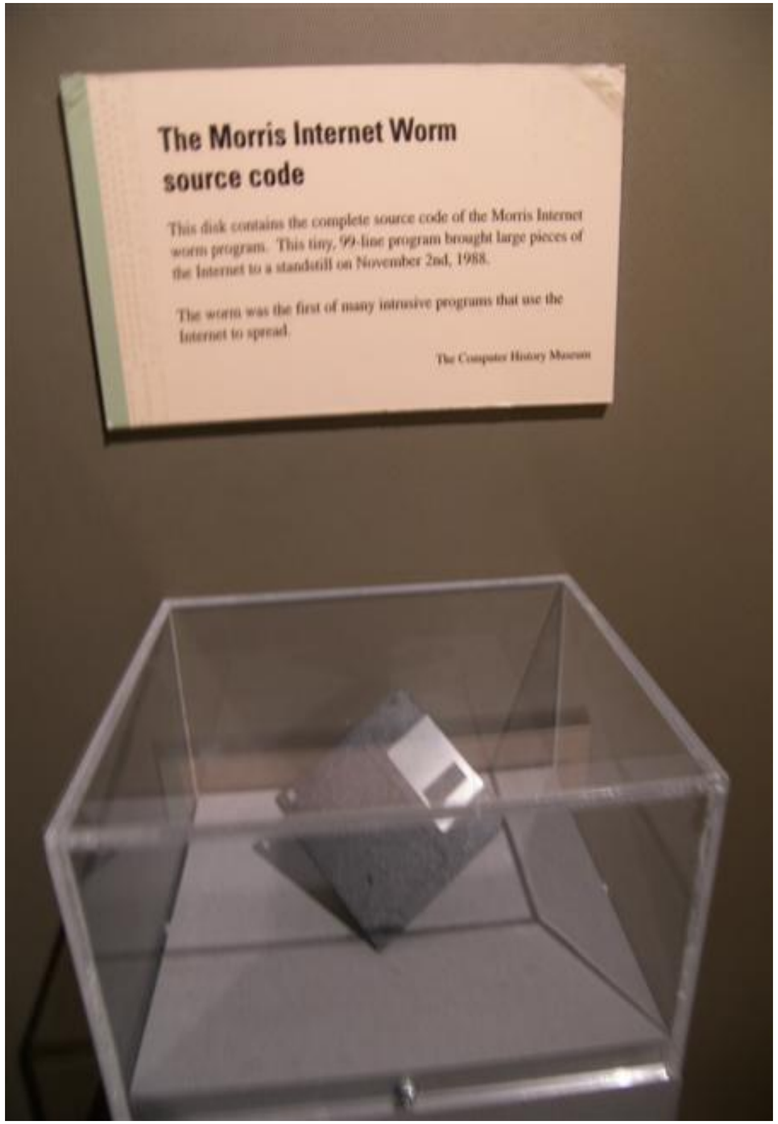


- Runs independently
  - Does not require a host program
- Propagates a fully working version of itself to other machines
- Carries a payload performing hidden tasks
  - Backdoors, spam relays, DDoS agents; …
- Phases
  - Probing ➔ Exploitation ➔ Replication ➔ Payload



Morris Worm (November 1988)

- First major worm
- Written by Robert Morris
  - Son of former chief scientist of NSA’s National Computer Security Center
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup



The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

The Computer History Museum

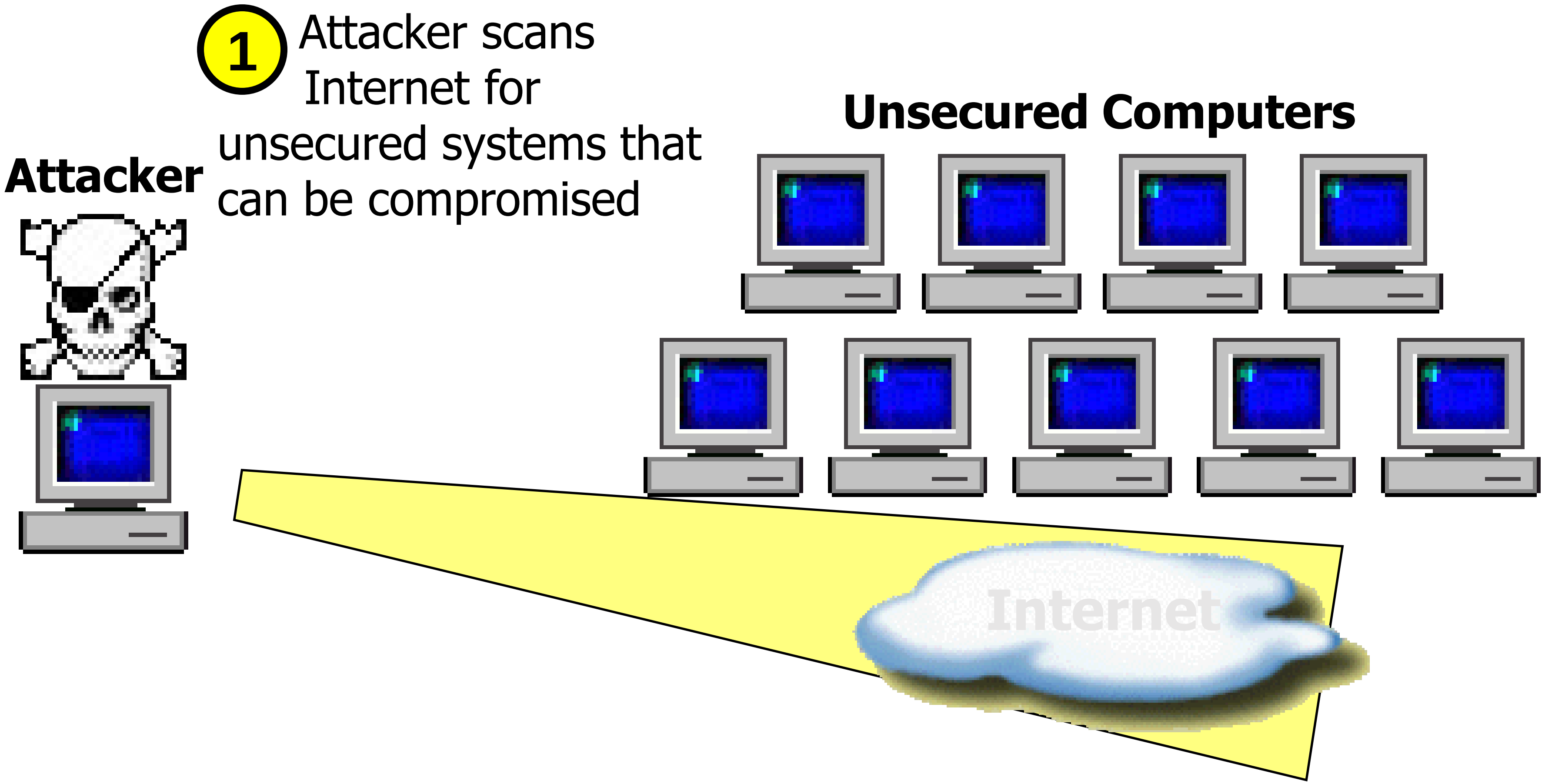
Email Worms: Spreading as Email Attachments

- Love Bug worm (ILOVEYOU worm) (2000):
  - May 3, 2000: 5.5 to 10 billion dollars in damage
- MyDoom worm (2004)
  - First identified in 26 January 2004:
  - On 1 February 2004, about 1 million computers infected with Mydoom begin a massive DDoS attack against the SCO group
- Storm worm & Storm botnet (2007)
  - Identified on January 17
  - gathering infected computers into the Storm botnet.
  - By around June 30th infected 1.7 million computers,
  - By September, has between 1 and 10 million bots

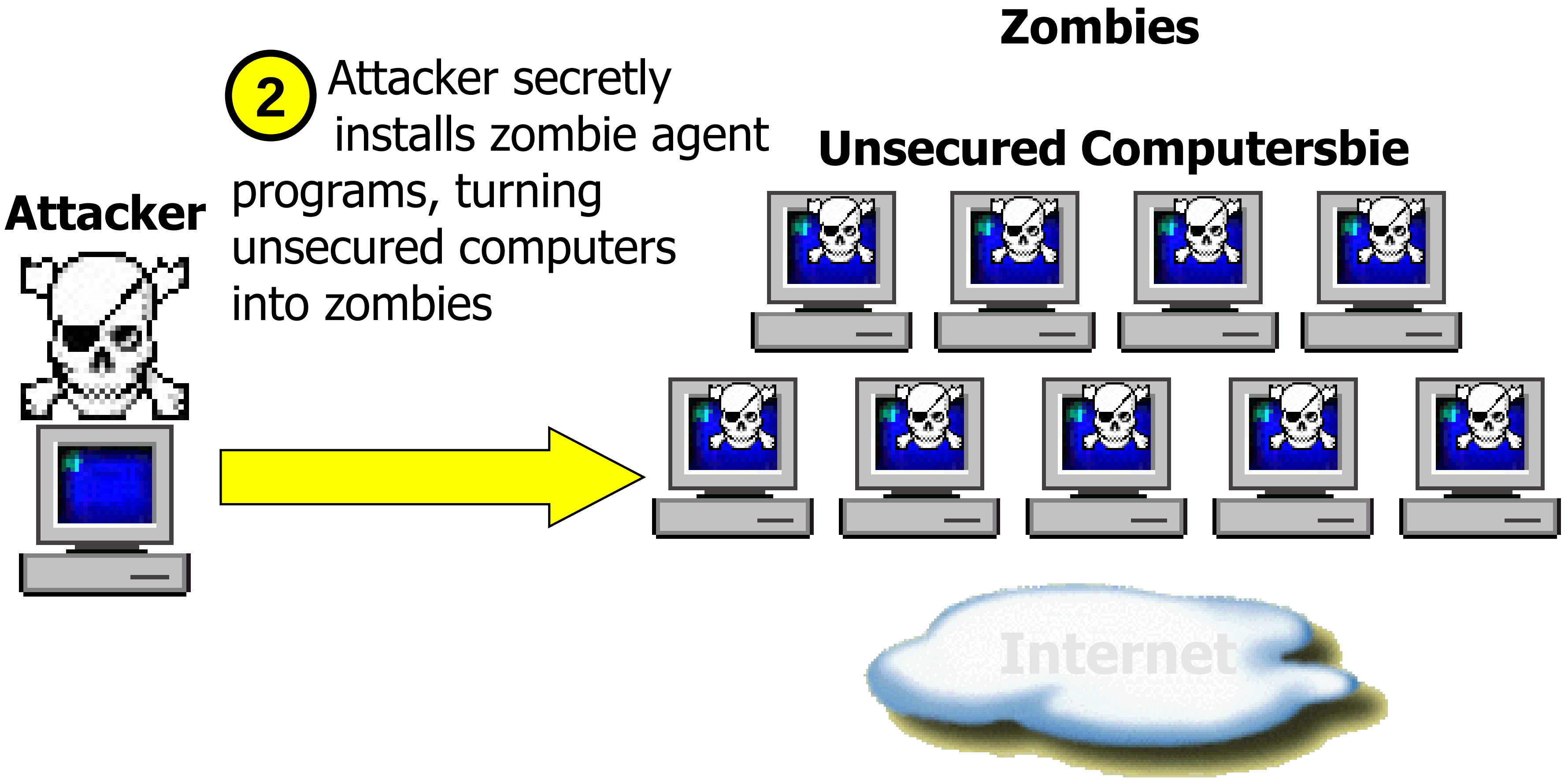
Zombie & Botnet

- Secretly takes over another networked computer by exploiting software flows
- Builds the compromised computers into a zombie network or botnet
  - a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- Uses it to indirectly launch attacks
  - E.g., DDoS, phishing, spamming, cracking

Detailed Steps (1)

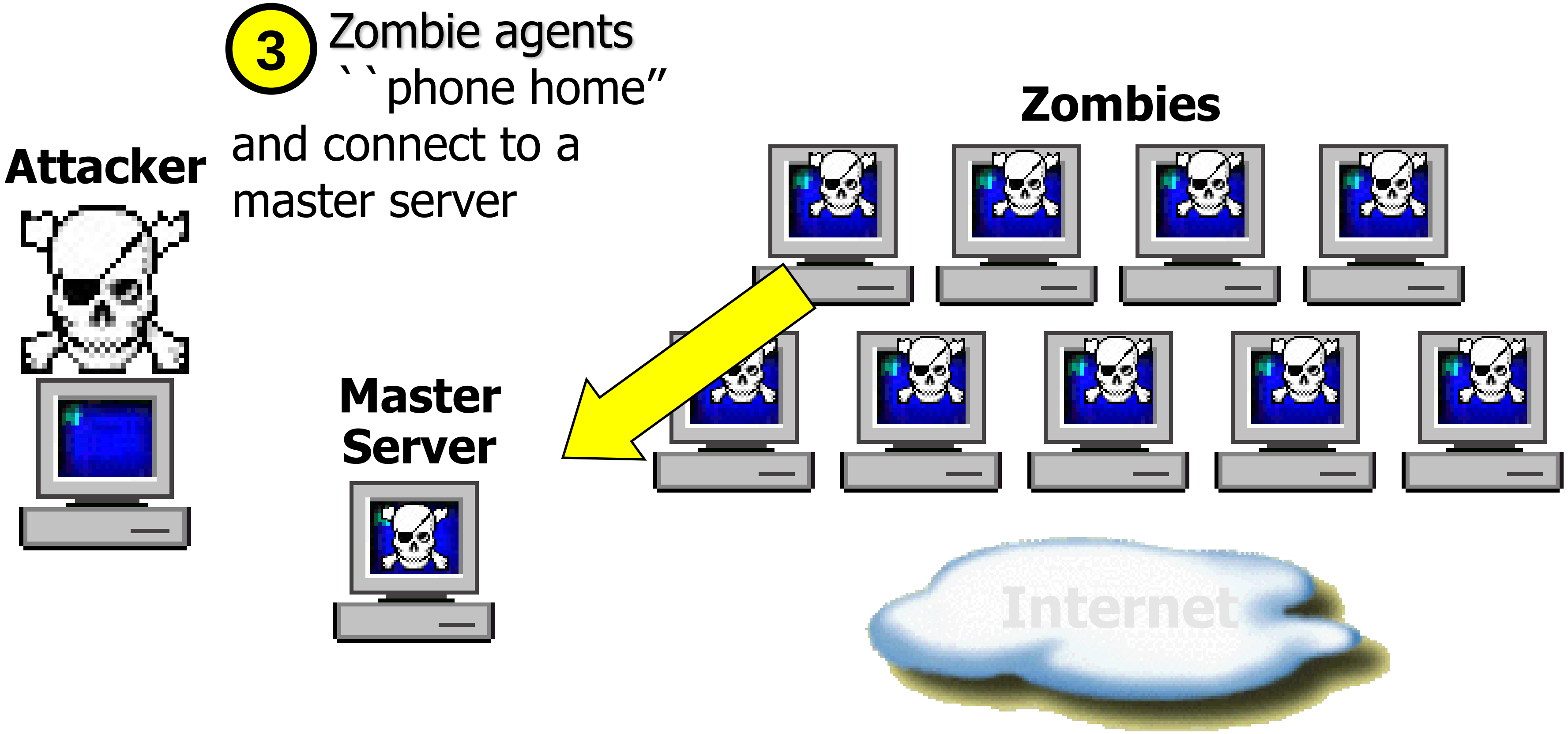

1
Attacker scans Internet for unsecured systems that can be compromised
Unsecured Computers
Attacker
Internet

Detailed Steps (2)



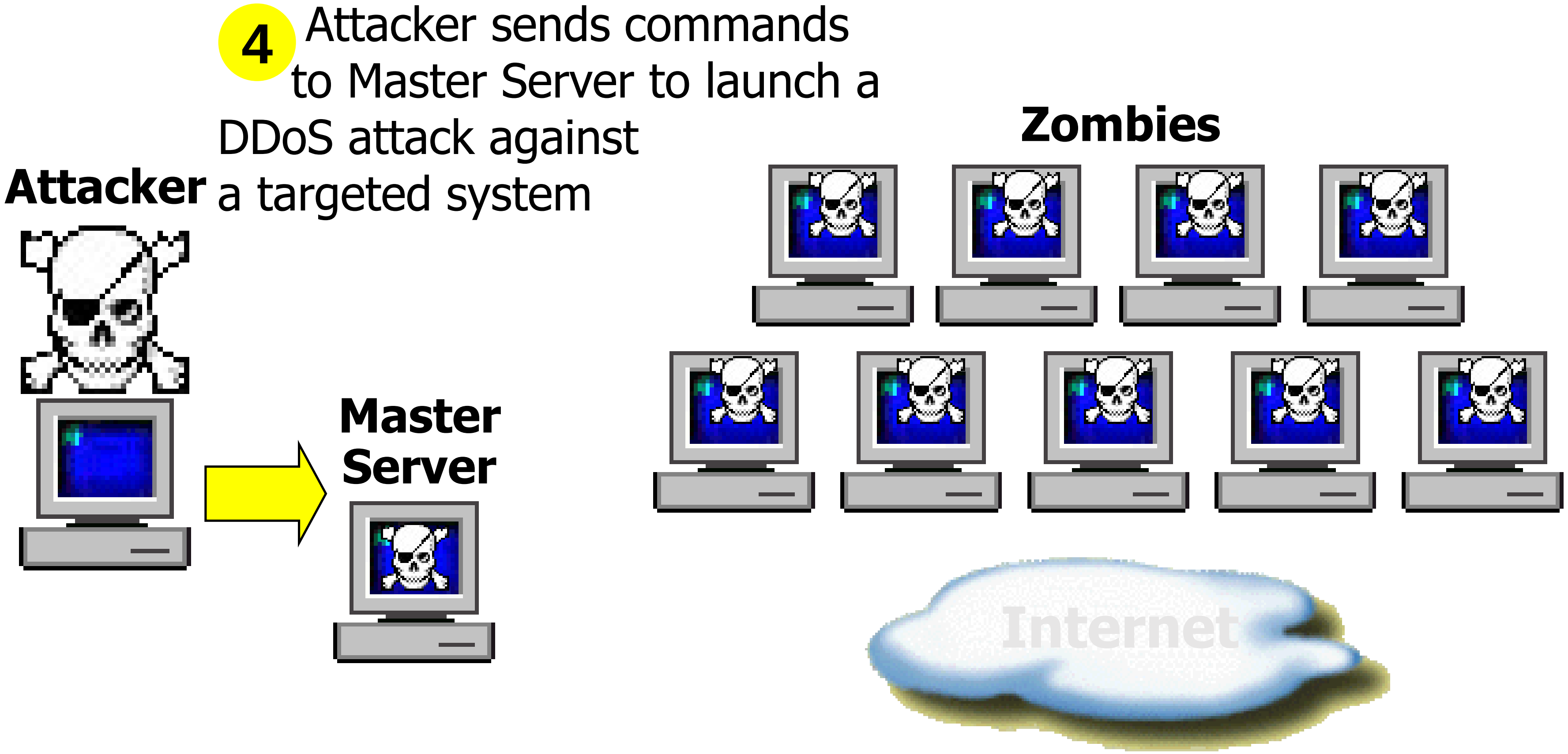
Attacker secretly installs zombie agent programs, turning unsecured computers into zombies

Detailed Steps (3)



3 Zombie agents ``phone home" and connect to a master server

Detailed Steps (4)



4 Attacker sends commands to Master Server to launch a DDoS attack against a targeted system

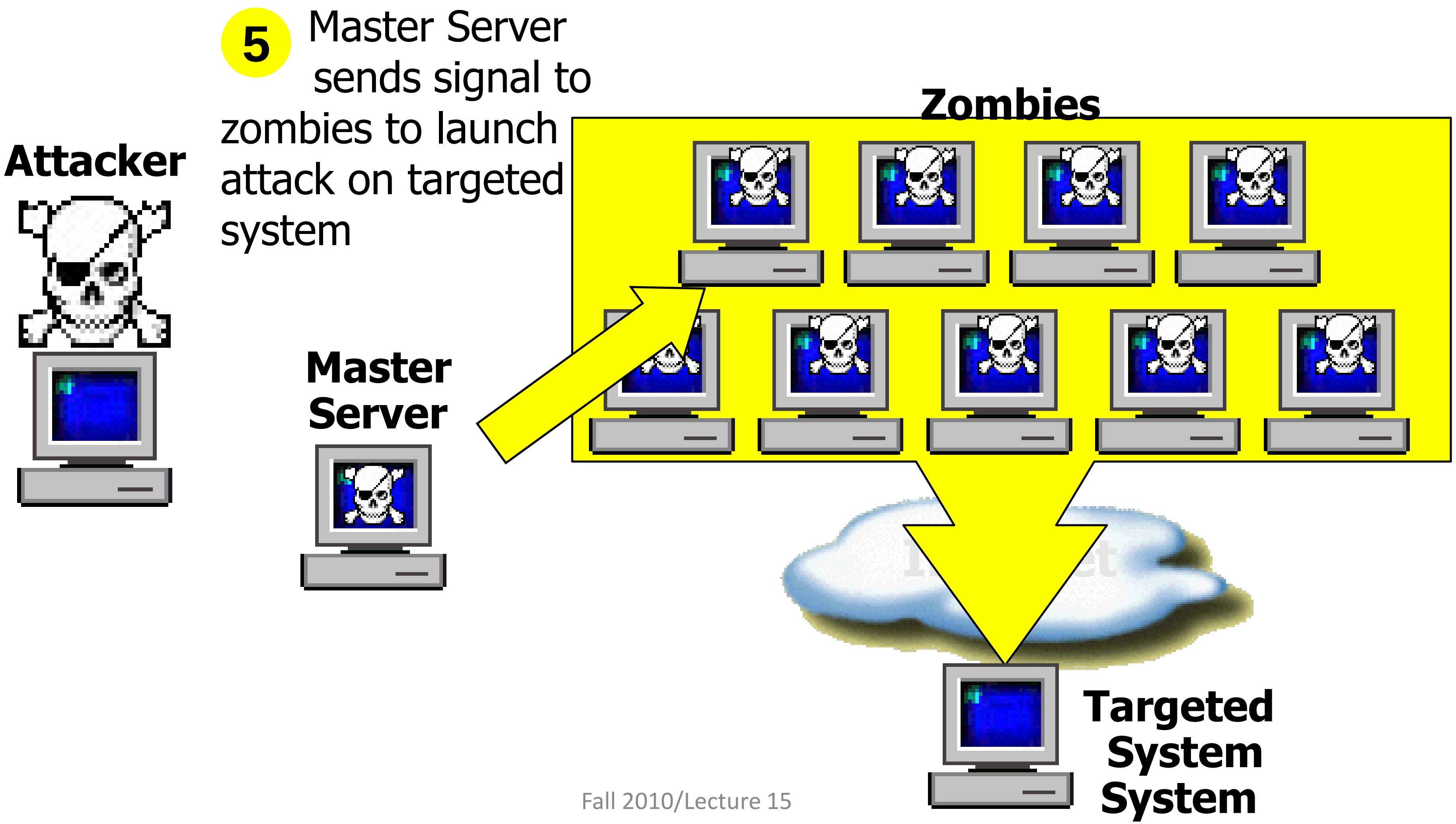
Attacker

Master Server

Zombies

Internet

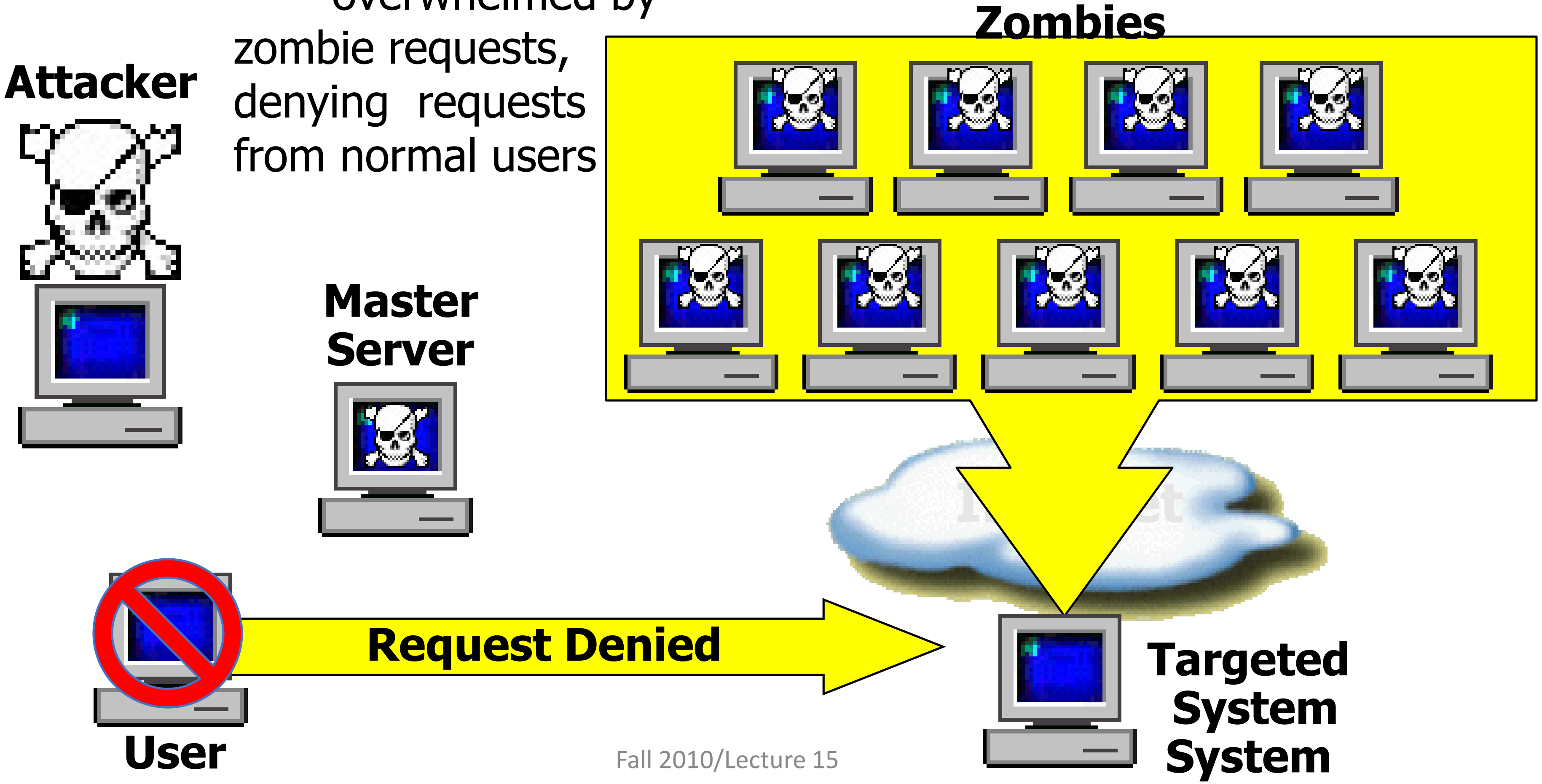
Detailed Steps (5)



5 Master Server sends signal to zombies to launch attack on targeted system

Detailed Steps (6)

6 Targeted system is overwhelmed by zombie requests, denying requests from normal users



Rootkit

- Software used after system compromise to:
  - Hide the attacker’s presence
  - Provide backdoors for easy reentry

- Simple rootkits:
  - Modify user programs (ls, ps)
  - Detectable by tools like Tripwire

- Sophisticated rootkits:
  - Modify the kernel itself
  - Hard to detect from userland

Security Threats

Social Engineering

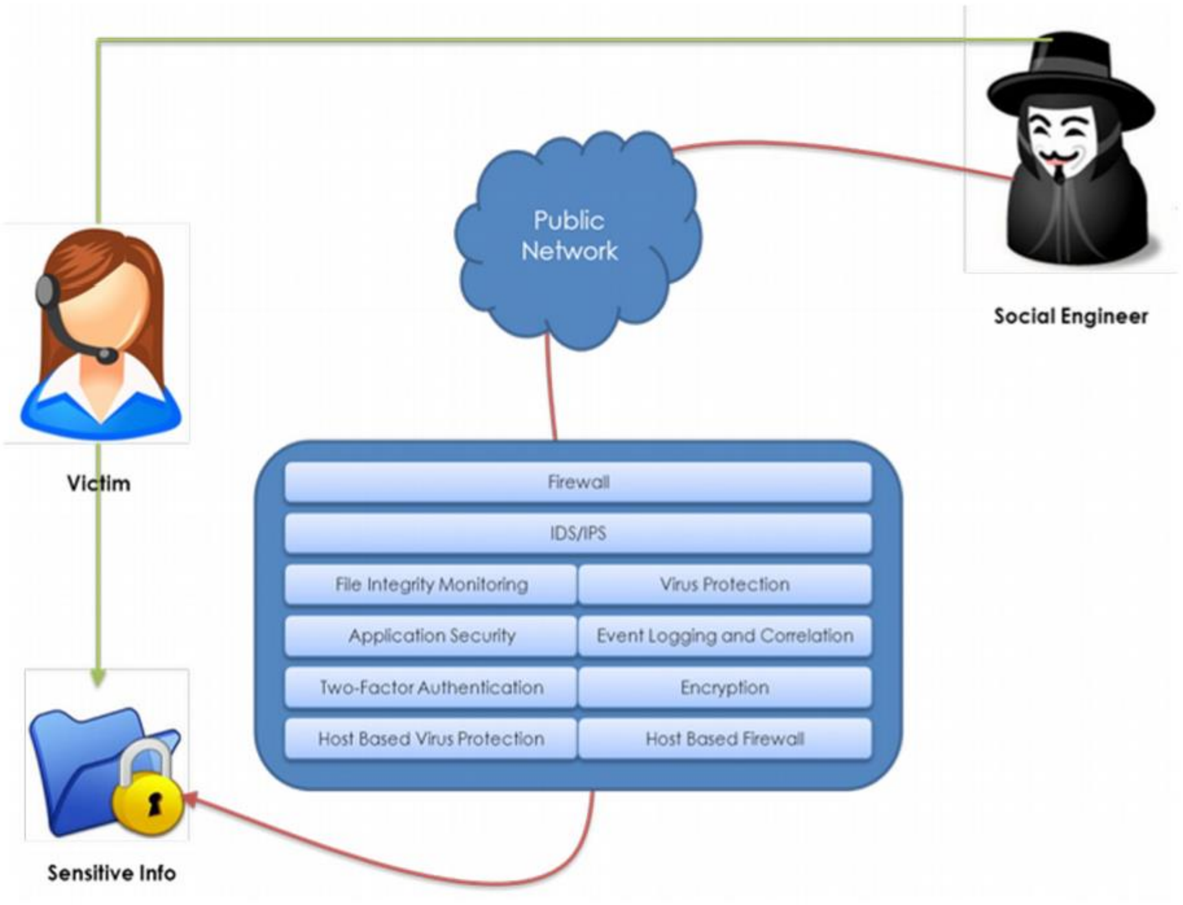
- Social Engineering (SE), however, isn’t a technical skill, though it is seen as the skill of hacking the human; compromising the most complex computer on the planet...the human brain!
- There are numerous definitions of SE but for the purpose of this lesson we've defined it as follows “convincing someone to do something for you that will ultimately lead you to achieve your desired goal, usually without them realizing it.”

- Exploiting vulnerabilities in the user, not the network or device

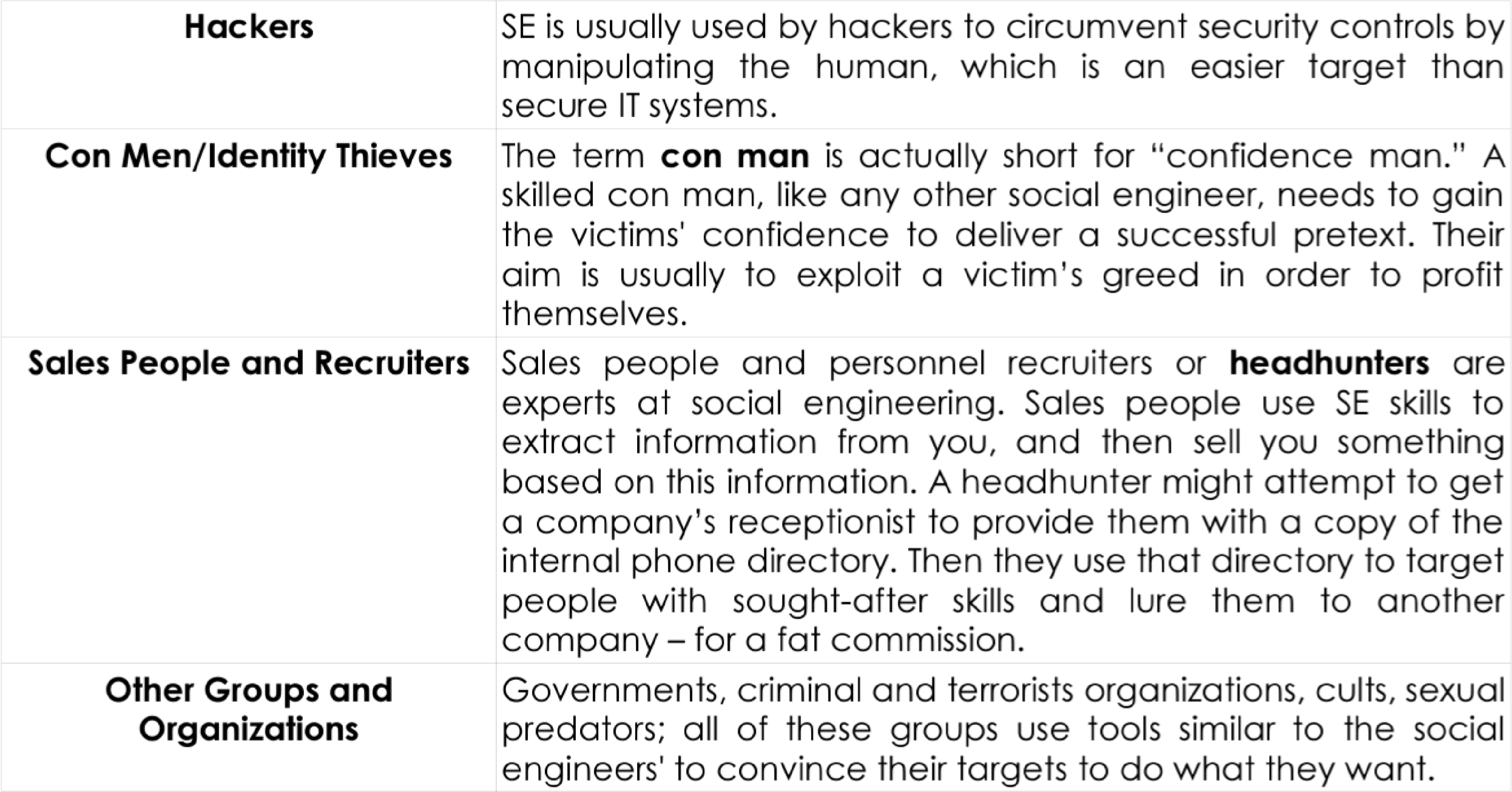
Social Engineering

- Passwords, firewalls, security policies, security doors, man traps, biometric scanners, security guards...all of these security controls are useless against a skilled social engineer. Because ***social engineers prey on the weakest link in the security chain – the human***!
- SE requires a completely different set of skills than any type of hacking you may have ever done. As a SE, you must be convincing, able to think quickly, look the part you are playing, know your target well enough to move around their environment without acting suspicious, and you must be able to control your own fears. Hackers tend to have poor social skills.
- Society has trained most people to be polite, be obedient, help others, avoid conflict and also to trust and believe what they are told.

Why Use Social Engineering

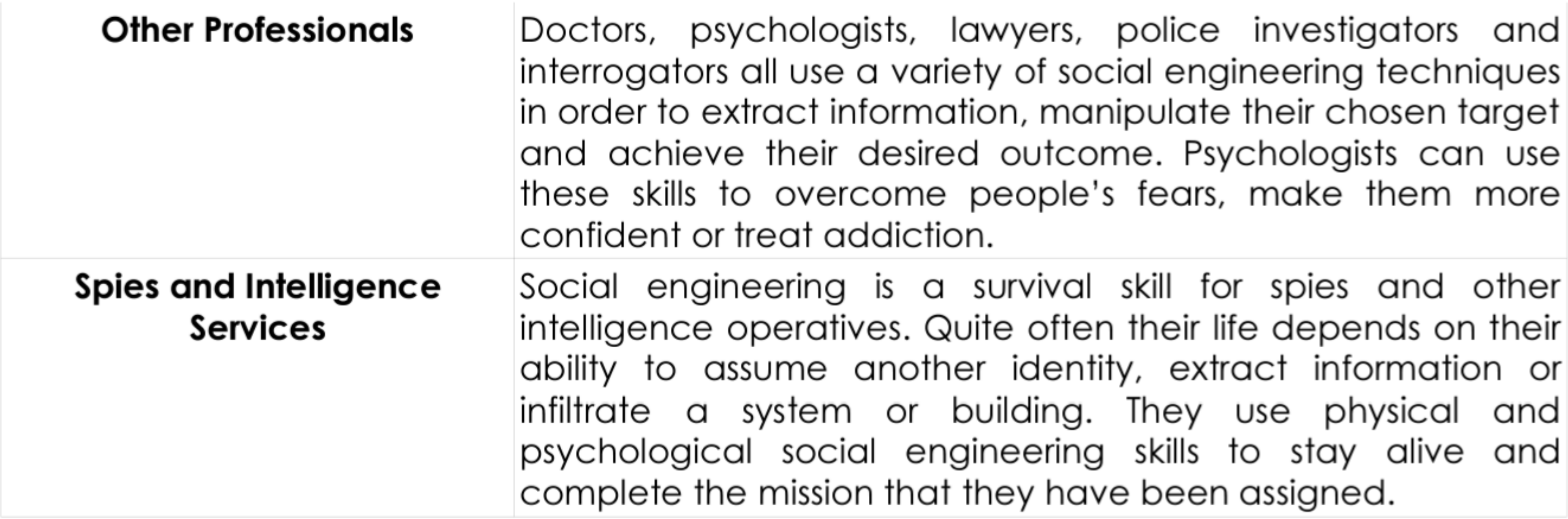


Who Uses Social Engineering



Hackers	SE is usually used by hackers to circumvent security controls by manipulating the human, which is an easier target than secure IT systems.
Con Men/Identity Thieves	The term **con man** is actually short for "confidence man." A skilled con man, like any other social engineer, needs to gain the victims' confidence to deliver a successful pretext. Their aim is usually to exploit a victim's greed in order to profit themselves.
Sales People and Recruiters	Sales people and personnel recruiters or **headhunters** are experts at social engineering. Sales people use SE skills to extract information from you, and then sell you something based on this information. A headhunter might attempt to get a company's receptionist to provide them with a copy of the internal phone directory. Then they use that directory to target people with sought-after skills and lure them to another company – for a fat commission.
Other Groups and Organizations	Governments, criminal and terrorists organizations, cults, sexual predators; all of these groups use tools similar to the social engineers' to convince their targets to do what they want.

Who Uses Social Engineering



Other Professionals	Doctors, psychologists, lawyers, police investigators and interrogators all use a variety of social engineering techniques in order to extract information, manipulate their chosen target and achieve their desired outcome. Psychologists can use these skills to overcome people's fears, make them more confident or treat addiction.
Spies and Intelligence Services	Social engineering is a survival skill for spies and other intelligence operatives. Quite often their life depends on their ability to assume another identity, extract information or infiltrate a system or building. They use physical and psychological social engineering skills to stay alive and complete the mission that they have been assigned.

Social Engineering Examples

Examples:

- “Dear Honorable Sir, I need to transfer $10,000,000,000 to your account”
  - Required to pay a “small” transfer fee

- “You need to update your Paypal account …”
  - Directed to send personal information

- Call computer support and masquerade as a technician
  - “Where is that TFTP server located again?”

Spoofing

- Making a fake version of something in order to trick a user
- Often used as part of a social engineering scam

Example:

1. You get an email saying something is wrong with your ebay account.
2. It provides a link to a website www.ebayaccounts.com
3. The website is fake but can look completely real

- Can be done with email addresses and calling trees

Phishing

- **Phishing** is an email sent from an Internet criminal disguised as an email from a legitimate, trustworthy source. The message is meant to lure you into revealing sensitive or confidential information.
- **Spear Phishing** occurs when criminals obtain information about you from websites or social networking sites, and customize a phishing scheme to you.

Preventing Social Engineering

- Don’t trust anyone or any information that you can’t verify

  1. Don’t give critical info to unverified websites/phone numbers
  2. Don’t accept anything (i.e. programs) from unverified sources

- This may be inconvenient

  1. If Citibank calls, you should call them back at a known Number
  2. Can’t purchase online from unknown vendors
  3. Be careful about freeware/shareware

Exercise:

- Create a list of three organizations that you would love to gain access to, stroll around, look at their internal network settings, and eat their donuts. The target organizations must be private, military, or “Mission Impossible” level, so choose well.
- Describe several ways you might be able to gain access to each organization without going through the front door and not using any technology beyond a cell phone. Each organization requires at least one different approach to gain access.
- If you must go through the building front door, you need to explain how you are going to get past the twenty-five burly security guards, their hungry attack dogs, and the eyes that never blink (security cameras). Be realistic. You are not a magician and the laws of physics apply. Your budget for each breach is $1,575 US. No, you do not own a helicopter or inviso-spray.

“Technical” Non-AI Threats

Exploiting vulnerabilities in the computational device or in the network

- Require some technical ability
  - Understand network protocols and components
  - Write code (at least execute scripts)
  - Deeply understand networked applications

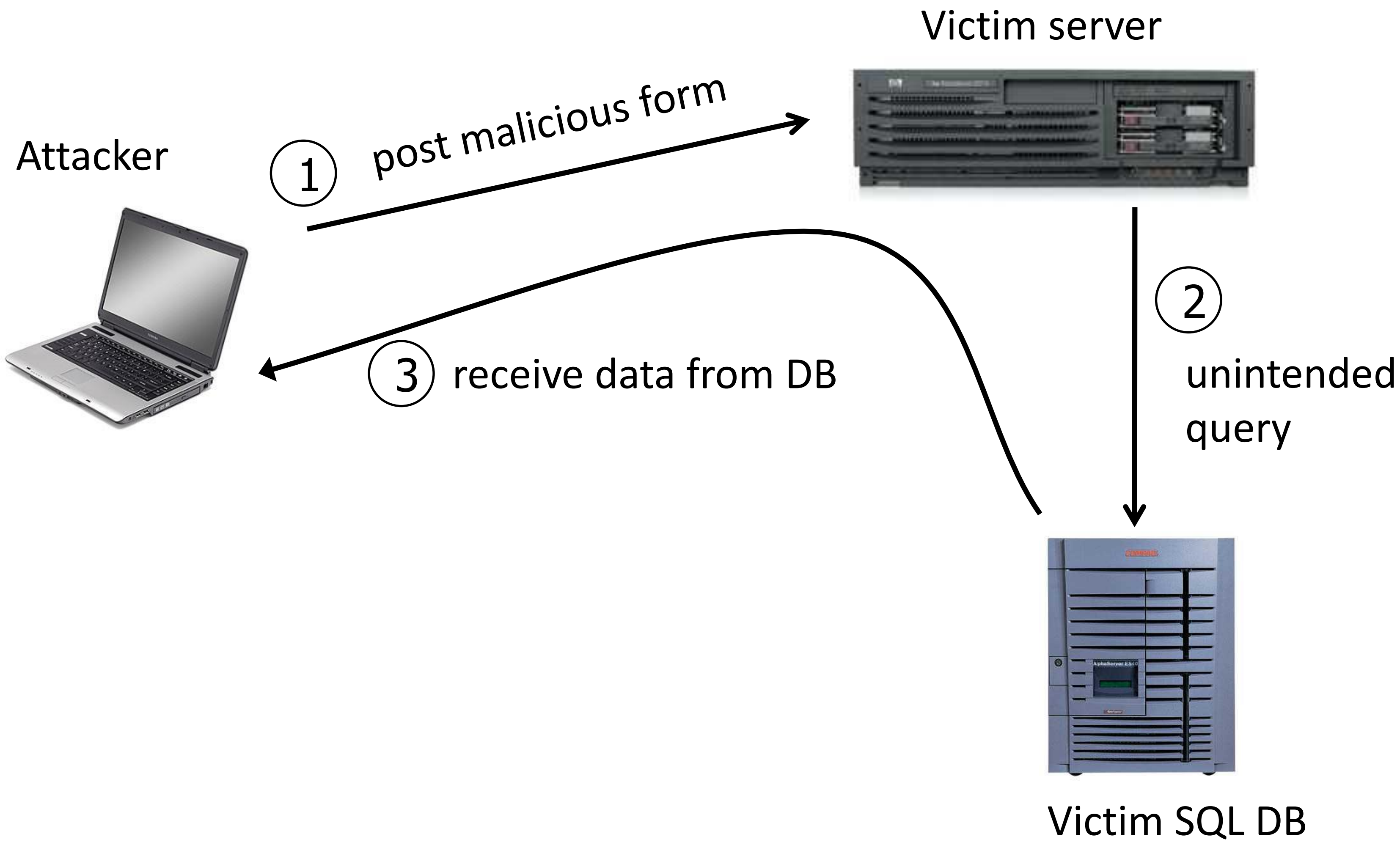
- May be directed at your machine
  - You can defend against these

- May impact you but be directed against other machines
  - You can’t really stop these

Some Famous Technical attacks

- **SQL Injection:** This is a type of web application attack that exploits vulnerabilities in database queries. Attackers can inject malicious SQL code into a form or URL to gain unauthorized access to a database, steal data, or modify it.
- **Denial-of-Service (DoS) Attack:** This attack aims to overwhelm a website or server with traffic, making it unavailable to legitimate users. This can be achieved by flooding the target with a high volume of requests or exploiting vulnerabilities in the system.
- **Man-in-the-Middle Attack:** This attack intercepts communication between two parties, such as a user and a website. The attacker can then eavesdrop on the conversation, steal data, or even modify it. Common methods include exploiting unencrypted Wi-Fi networks or compromising network devices.
- **Zero-Day Attack:** This is an attack that exploits a previously unknown vulnerability in software. Since there is no patch available, these attacks can be very successful.

SQL Injection: Basic Idea

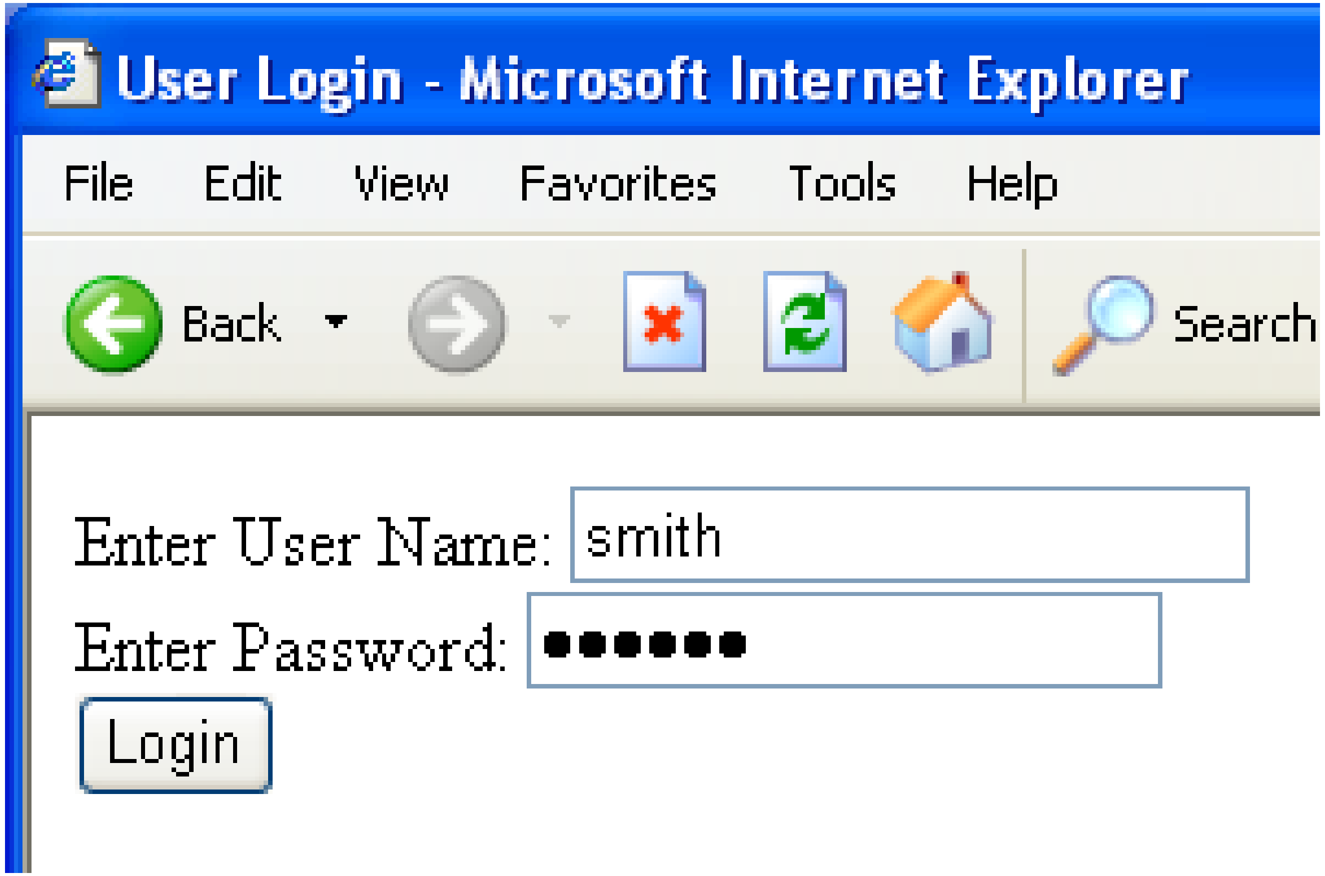


Typical Query Generation Code

```
$selecteduser = $_GET['user'];
$sql = "SELECT Username, Key FROM Key " .
        "WHERE Username='$selecteduser'";
$rs = $db->executeQuery($sql);
```

- What if ‘user’ is a malicious string that changes the meaning of the query?

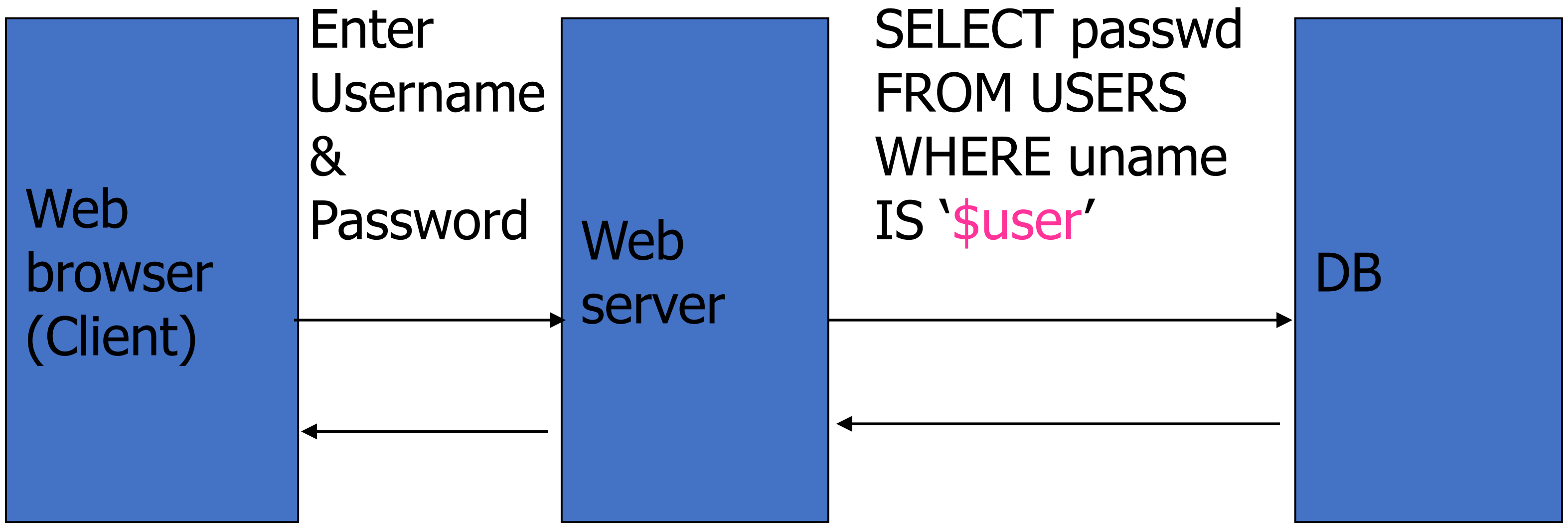
Typical Login Prompt



Enter User Name: smith

Enter Password: ●●●●●●●

User Input Becomes Part of Query



Web browser (Client)

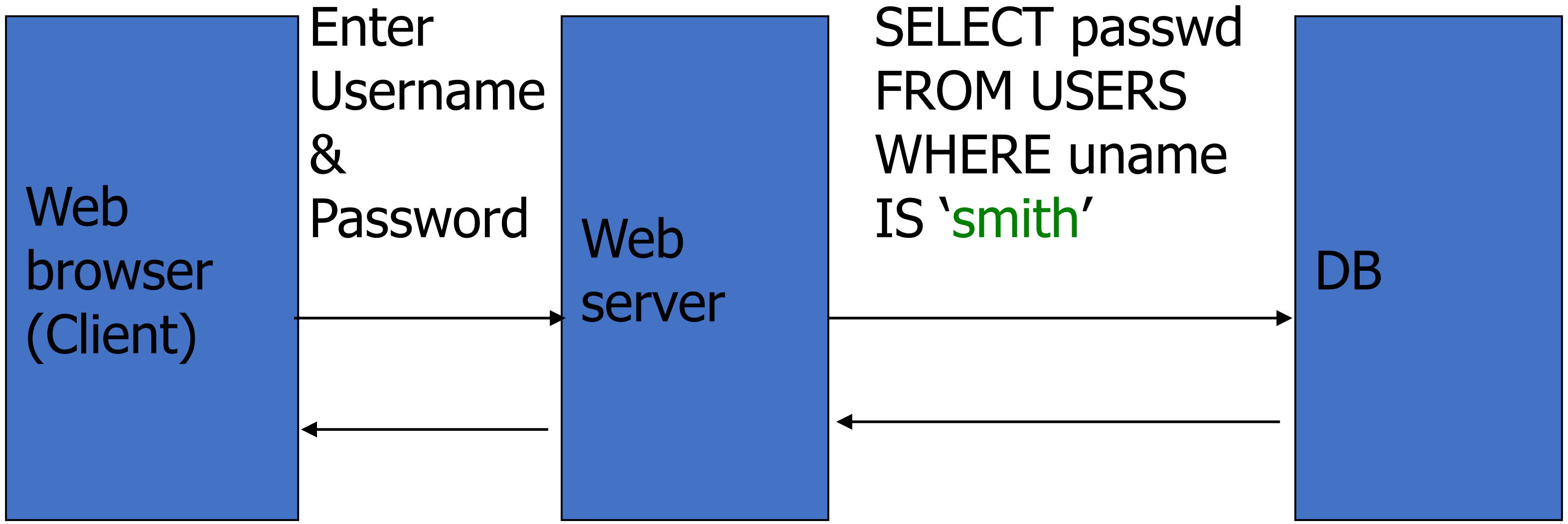
Enter Username & Password

Web server

SELECT passwd FROM USERS WHERE uname IS ‘$user’

DB

Normal Login



Web browser (Client)

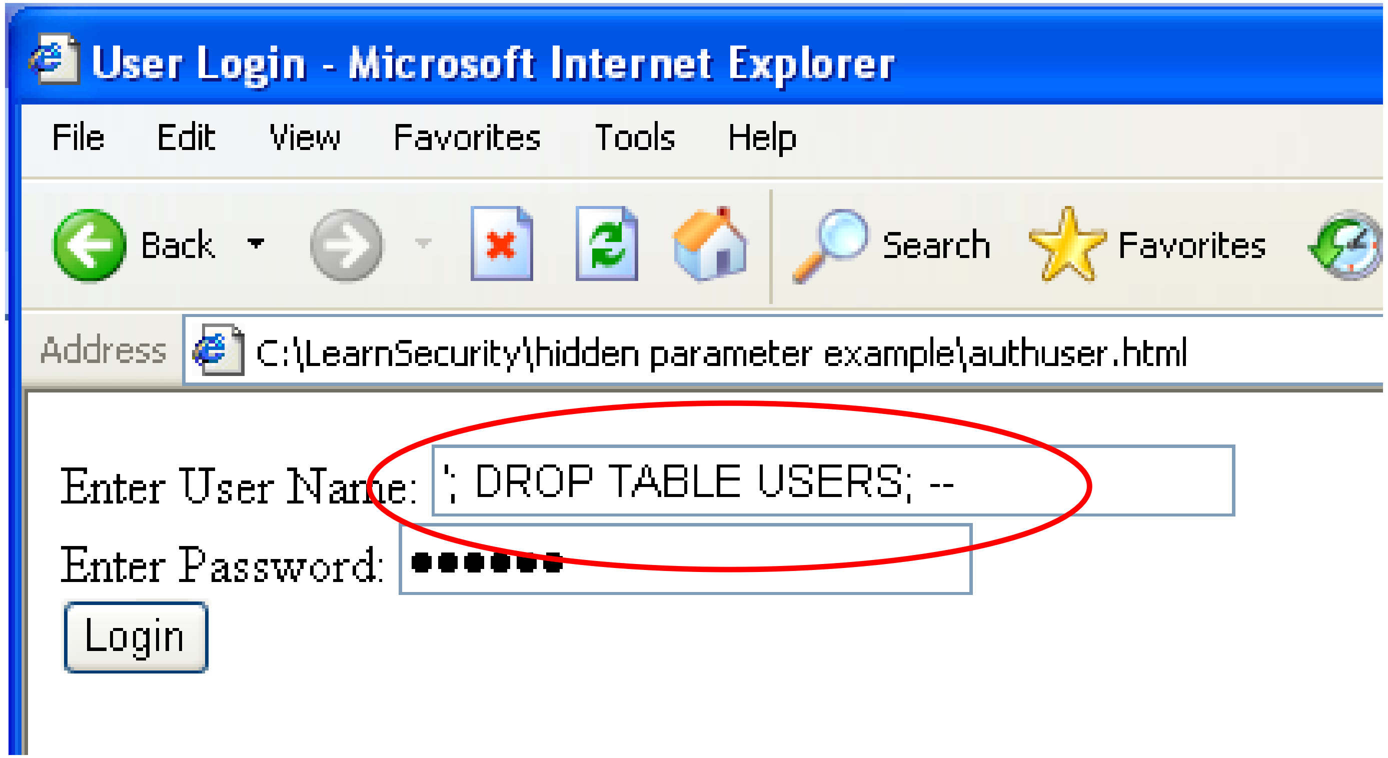
Enter Username & Password

Web server

SELECT passwd FROM USERS WHERE uname IS ‘smith’

DB

Malicious User Input



User Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address

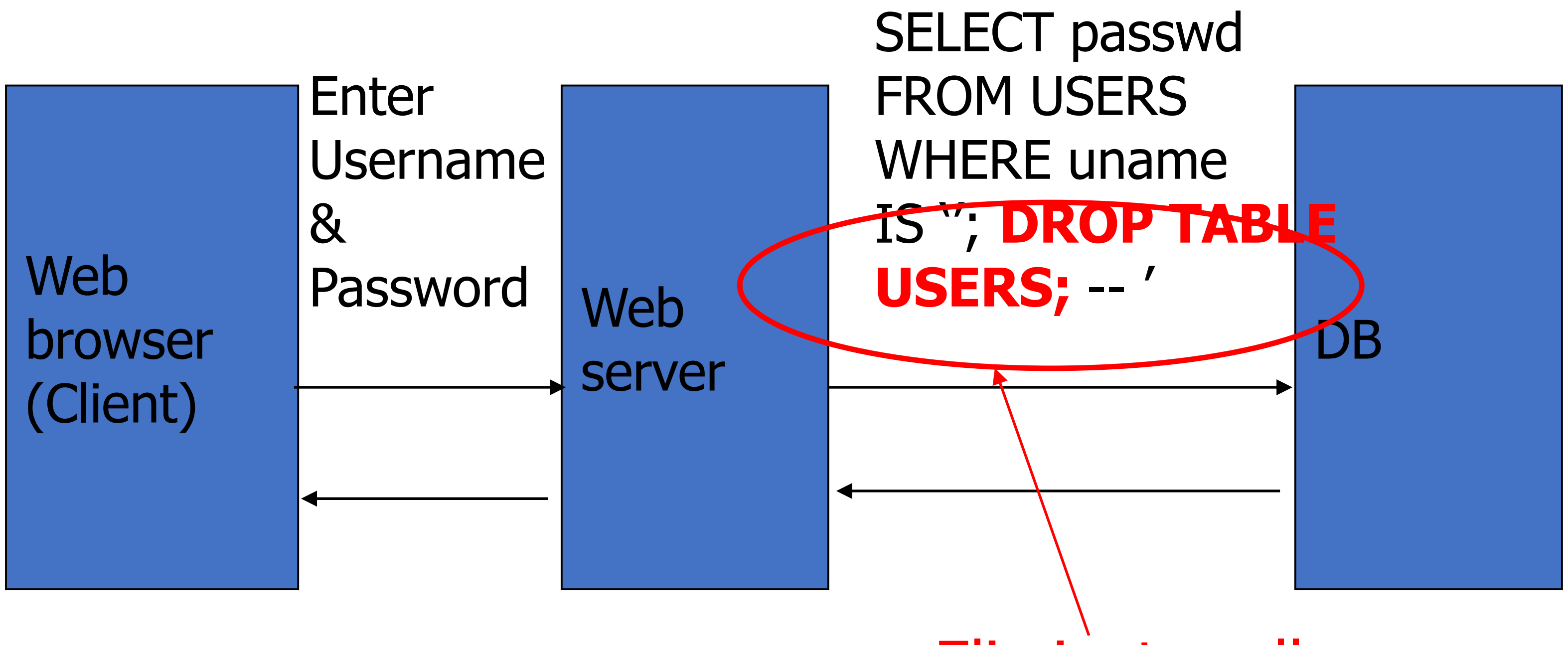
C:\LearnSecurity\hidden parameter example\authuser.html

Enter User Name: '; DROP TABLE USERS; --

Enter Password: ●●●●●●●

Login

SQL Injection Attack



Web browser (Client)

Enter Username & Password

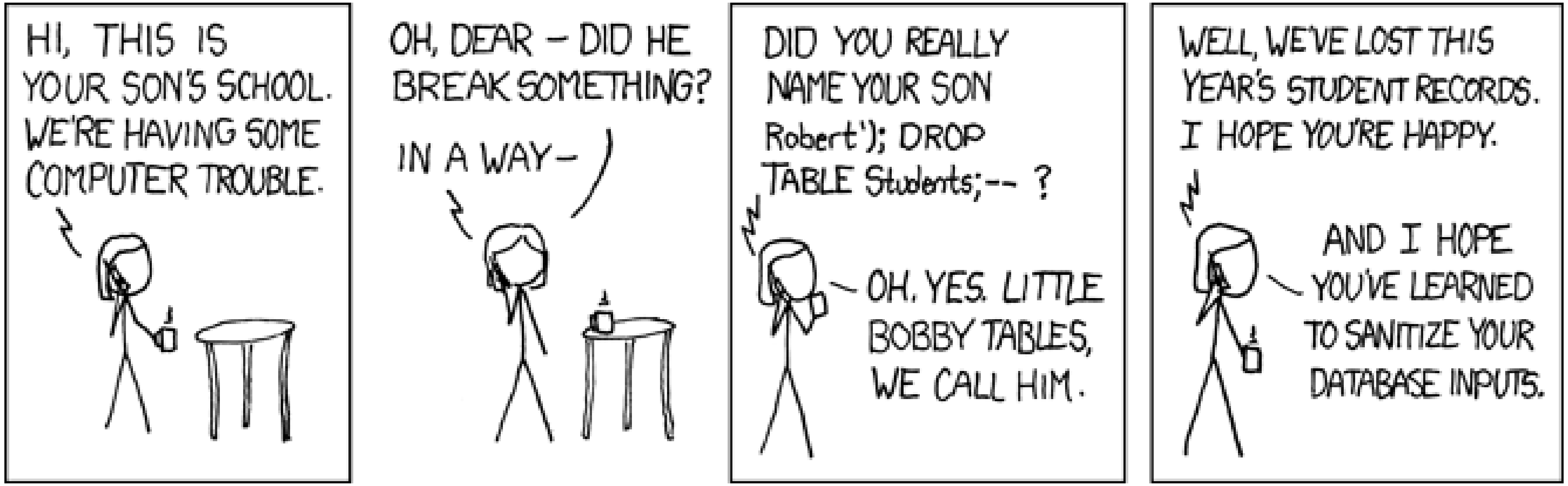
Web server

SELECT passwd FROM USERS WHERE uname IS ‘’; **DROP TABLE USERS;** -- ’

DB

Eliminates all user accounts

Exploits of a mom


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

- Sanitizing user input involves cleaning the data to remove any potentially harmful characters or sequences that could be interpreted as SQL commands.

Using SQL Injection to Log In

- User gives username ’ OR 1=1 --
- Web server executes query

```
set UserFound=execute(
     SELECT * FROM UserTable WHERE
     username=“’ OR 1=1 -- … );
```

Always true!

Everything after -- is ignored!

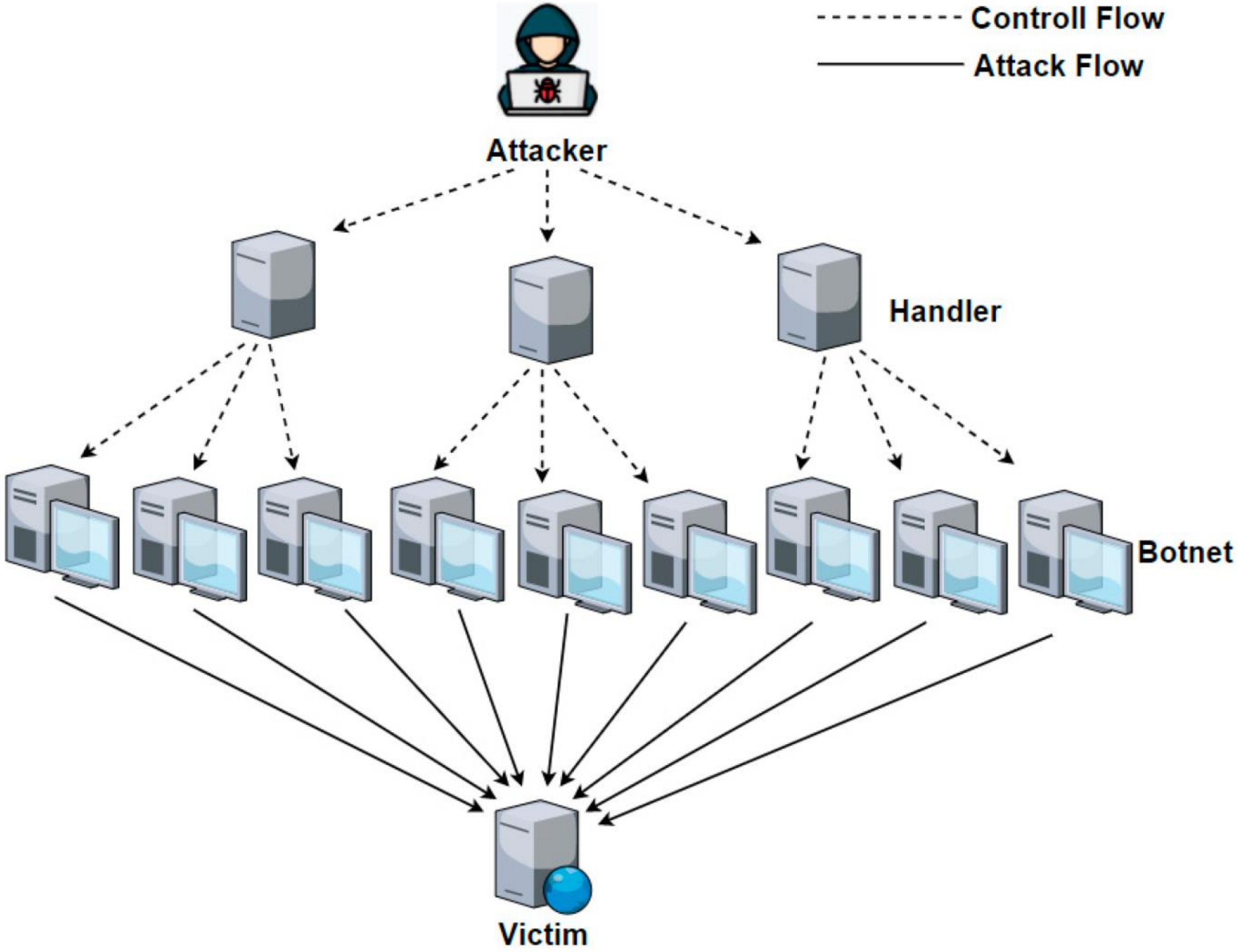
- Now all records match the query, so the result is not empty ⇒ correct “authentication”!

Preventing SQL Injection

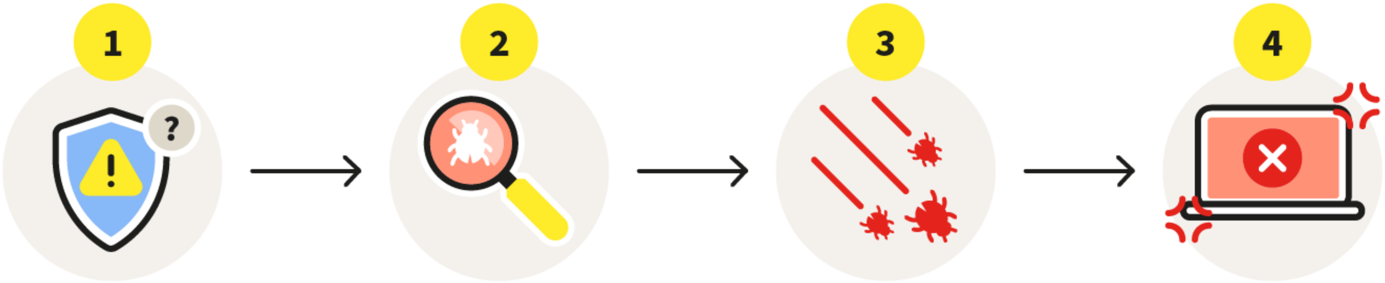
- Validate all inputs
  - Filter out any character that has special meaning
    - Apostrophes, semicolons, percent symbols, hyphens, underscores, …
  - Check the data type (e.g., input must be an integer)
- Whitelist permitted characters
  - Blacklisting “bad” characters doesn’t work
    - Forget to filter out some characters
    - Could prevent valid input (e.g., last name O’Brien)
  - Allow only well-defined set of safe values
    - Implicitly defined through regular expressions

Denial of Service

- A service provided by the device is caused to fail
  - DDOS: Distributed Denial of Service
    - DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IOT devices.



Zero-Day Attacks Explained



1

A security flaw exists but is unbeknown to developers, making it vulnerable to attacks.

2

A hacker discovers the vulnerability and exploits it by malware injection.

3

A cyberattack ensues from the malware, potentially resulting in data loss.

4

Developers detect the attack and have zero days to mitigate it.