



Web Security

Secure yourself on the web



What is web security?

Almost everything relies on computers and the Internet now

- communication (email, cell phones)
- transportation (car engine systems)
airplane navigation)
- medicine (equipment, medical records)
- shopping (online stores, credit cards)
- entertainment (digital cable, mp3s)



What is web security?


(contd...)

Web Security, also known as “Cyber security” involves protecting that information by preventing, detecting, and responding to attacks.



What can Web users do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.



Web Security: Terminologies

- **Hacker** – people who seek to exploit weaknesses in software and computer systems for their own gain.
- **Viruses** – It you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.



Web Security: Terminologies


- **Worms** - Worms propagate without user intervention. Once the victim computer has been infected the worm will attempt to find and infect other computers.
- **Trojan horses** - A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes.



Web Security: Terminologies

Ransomware

- A form of trojan that has been around since 1989 (as the “PC CYBORG” trojan)
- It infects the target computer by encrypting the owner's personal files.
- The victim is then contacted and offered a key to decrypt the files in exchange for cash



Web Security: Terminologies

KeyLoggers:

- Traditionally, Keyloggers are software that monitor user activity such as keys typed using keyboard.

Modern keyloggers can,

- Record keystrokes on keyboard
- Record mouse movement and clicks
- Record menus that are invoked
- Take screenshots of the desktop at predefined intervals (like 1 screenshot every second)




Web Security: Terminologies

KeyLoggers: (contd...)

Such recorded data could be uploaded in real-time or when internet connection becomes available, by,

- Email attachment
- IRC Channel
- File Transfer (FTP)



Web Security: Terminologies

KeyLoggers: (contd...)

Keylogger prevention

- ☐ Use Anti-Spyware (prevention)
- ☐ Firewall (manual detection)
- ☐ Automatic Form fillers (protection from keylogging)

In public (insecure) places,

-use on-screen keyboards

(START-> ALL PROGRAMS ->ACCESSORIES ->
ACCESSIBILTY -> ON-SCREEN KEYBOARD)



Web Security: Terminologies

Firewalls:

Mechanism for content regulation and data filtering

- Blocking unwanted traffic from entering the sub-network (inbound)
- Preventing subnet users' use of unauthorised material/sites (outbound)



Aspects of data Security

- Privacy

- ☐ Keeping your information private

- Integrity

- ☐ Knowing that the information has not been changed

- Authenticity

- ☐ Knowing who sent the information



Privacy

- Your personal details are a valuable asset
- Businesses are increasingly looking to target individuals more effectively, data about those individuals is in demand
- Buying and selling lists of email addresses and demographic details is big business



Integrity

- Maintaining the data integrity of any communication is vital.
- Integrity can be preserved by using strong encryption methods.
- Even if an intruder see the transmission, it would be useless since its encrypted.



Authentication

We need to authenticate a message to make sure it was sent by the correct person.

- Digital signature is used for the purpose
- Public key , Private key method can also be used to authenticate.



Authentication , Continued...

Most of us use webmail for email handling.

This simple code can send an email,

```
<? php
```

```
    mail("recipient@yahoo.com", "Hi from Bill Gates", "Hi, I am  
    Bill gates" , "From: billgates@microsoft.com");
```

```
?>
```




Authentication , Continued...

Received email:

From: billgates@microsoft.com

To: recipient@yahoo.com

Subject: Hi from Bill Gates

Hi, I am Bill gates



Authentication , Continued...

- So, anyone can send email from anyone's email address
- Its possible due to the nature of SMTP protocol
- Yahoo! has implemented DomainKeys, a method to authenticate that an email originated from the sender's domain.



Web Security Issues

- Malicious websites
- SPAM
- 419 Scams
- Phishing
- DDOS
- Botnets

(All aspects are inter-related)



Malicious websites

- More than 3 million Web pages on the Internet are malicious.
- According to Neils Provos, senior staff software engineer with Google, the percent is one in 1,000.
- The experts call these attacks "drive-by downloads"

Malicious websites

China	- 67%
US	- 15%
Russia	- 4%
Malaysia	- 2.2%
Korea	- 2%



Malicious websites

Preventive measures

- Use latest browser software
 - Internet Explorer version 7+
 - Mozilla Firefox
 - Opera

Internet Explorer 6 is the most vulnerable as well as the most widely used browser.

It is highly recommended to upgrade from IE 6



SPAM

Spam is unsolicited e-mail on the Internet.

Spam detection algorithms

- White listing
- Black listing
- Training based algorithms



SPAM

Cost of spam

- Loss of productivity is the main concern
- There is also the cost of bandwidth taken by spam
- Storage and network infrastructure costs.
- Loss of legitimate email messages

SPAM



- Corporate employees are reported to accrue a loss of productivity of 3.1%. - Nucleus Research Analysis
- To increase the effectiveness of SPAM detection, always report any SPAM mail to your SPAM filter.



419 Nigerian Scams

An **advance fee fraud** is a confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a very much larger gain

The number "419" refers to the article of the Nigerian Criminal Code ("Cheating") dealing with fraud.



419 Nigerian Scams

A sample 419 Scam email

Sender: **uk_national_lottery_005@hotmail.com**

Subject: **!!!CONGRATULATIONS YOU ARE A WINNER!!!**

FROM THE LOTTERY PROMOTIONS MANAGER,
THE UNITED KINGDOM INTERNATIONAL LOTTERY,
PO BOX 287, WATFORD WD18 9TT,
UNITED KINGDOM.

We are delighted to inform you of your prize release from the United Kingdom International Lottery program. Your name was attached to Ticket number; 47061725, Batch number; 7056490902, Winning number; 07-14-24-37-43-48 bonus number 29, which consequently won the lottery in the first category....



419 Nigerian Scams

The email asks to send an advance payment to the lottery so that they can release the prize money.

Lots of naive users get fooled by the scammers and end up wasting their money.



419 Nigerian Scams

Prevention:

Awareness is the only tool against such scammers.

Services like 419eater.com has users who pretend to be naive and end up wasting the scammer's efforts.



Phishing

This is a method of luring an unsuspecting user into giving out their username and password for a secure web resource, usually a bank or credit card account.



Phishing

- Usually achieved by creating a website identical to the secure site
- User is sent email requesting them to log in, and providing a link to the bogus site
- When user logs in, password is stored and used to access the account by the attacker
- Difficult to guard against, particularly if using HTML email



Phishing

Phishing Email sample:

Subject: Verify your E-mail with Citibank

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:

https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

Thank you for using Citibank



Phishing

The link uses an anchor text, and the actual website opens as,

<http://citibusinessonline.da.us.citibank.com.citionline.ru/...>

Instead of,

<http://www.citibank.com/us/index.htm>

Phishing

Landing Page

The screenshot shows a Microsoft Internet Explorer window titled "CitiBusiness Online - Microsoft Internet Explorer". The address bar displays "http://citibusinessonline.da.us.citibank.com.citionline.ru/". The page features the Citi logo and "CitiBusiness® Online" text. A navigation bar includes links for "Home", "User Guide", and "citi.com". The main content area is titled "Account Holder Information. Step 2 of 3." and addresses a user as "Dear [redacted]". It prompts the user to "Please enter information requested below then click continue." and lists the following fields: "Date of Birth (mm/dd/yyyy):" with three input boxes, "Social Security Number" with three input boxes, "Mother's Maiden Name" with one input box, "City of Birth" with one input box, and "Name of High School Attended" with one input box. A "Continue" button is located below these fields. On the right side, a red vertical banner reads "SECURITY REMINDER". To the right of the banner, text states: "The privacy and security of your account information is important to us. As a reminder, Keep your anti-virus and firewall software up-to-date. Discounted software is available to all our customers who are registered for our online service." The status bar at the bottom shows "Done" and "Internet".

CitiBusiness Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go

Address http://citibusinessonline.da.us.citibank.com.citionline.ru/

citi

Home User Guide citi.com

CitiBusiness® Online

Account Holder Information.
Step 2 of 3.

Dear [redacted]

Please enter information requested below then click continue.

Date of Birth (mm/dd/yyyy):
[] / [] / []

Social Security Number
[] - [] - []

Mother's Maiden Name
[]

City of Birth
[]

Name of High School Attended
[]

Continue

SECURITY REMINDER

The privacy and security of your account information is important to us.

As a reminder, Keep your anti-virus and firewall software up-to-date. Discounted software is available to all our customers who are registered for our online service.

Done Internet



Phishing

- Unwitting users submit the data, and the data is captured by scammers and all the money in their account will be stolen immediately.
- This method is the main reason for loss of email passwords also.



Denial of Service

It is an attack to make a computer resource unavailable to its intended users.

Resources:

- Bandwidth & CPU



Distributed DOS

A powerful variant of DOS attack.

- Web server can handle a few hundred connections/sec before performance begins to degrade
- Web servers fail almost instantly under five or six thousand connections/sec



Distributed DOS

- Zombie system is a system that is brought under the attacker's control by using virus/worm/exploits.
- Attack is initiated using compromised Zombie systems.
- Very hard to prevent, since large number of zombie systems will be used.

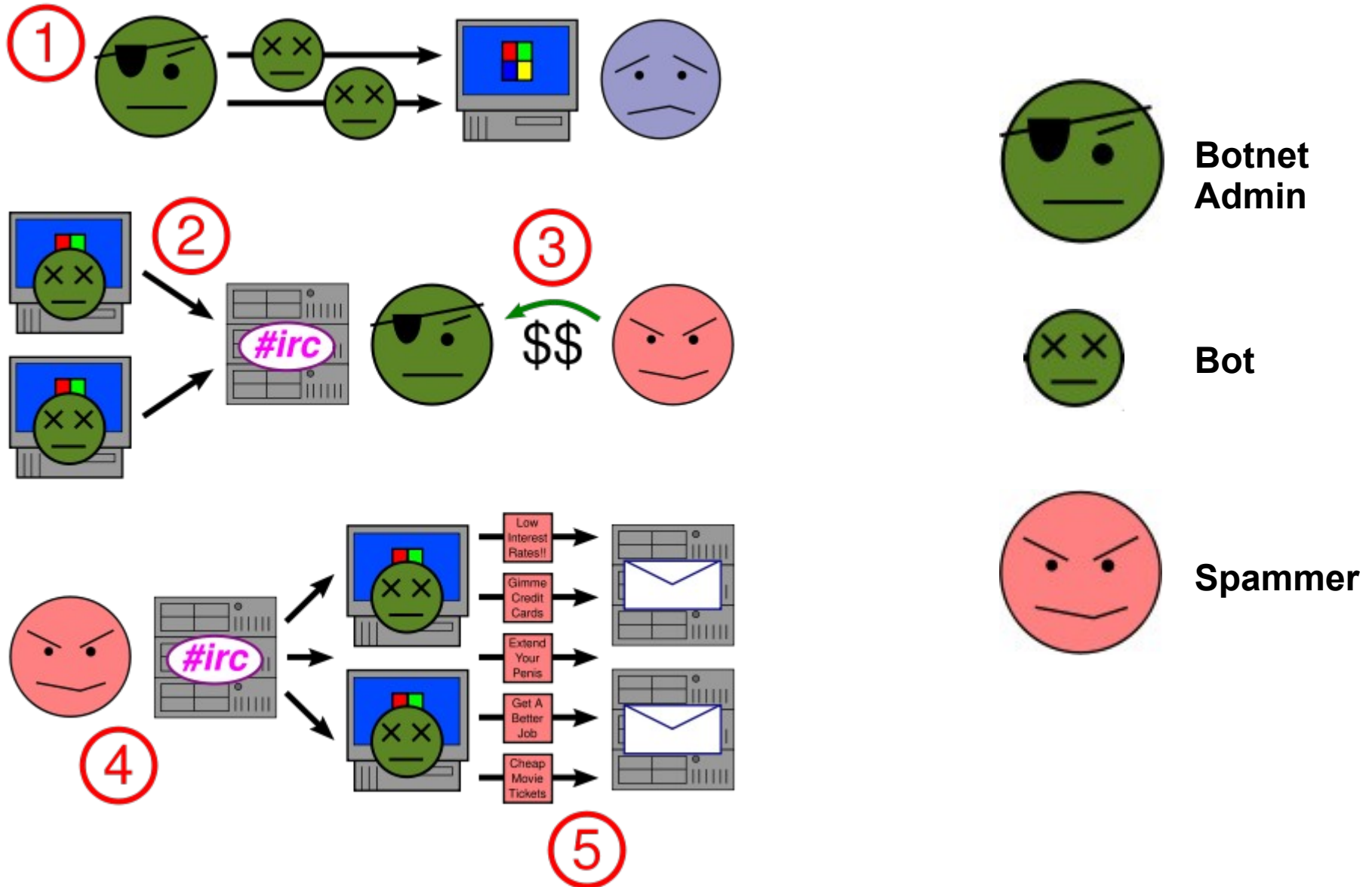


Botnets

A botnet is a collection of compromised computers (called zombie computers) running programs

- Usually installed via worms, Trojan horses, or backdoors,
- Under a common command and control infrastructure.

Botnets





Botnets

1. A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application -- the bot.
2. The bot on the infected PC logs into a particular IRC server (or in some cases a web server). That server is known as the command-and-control server (C&C).
3. A spammer purchases access to the botnet from the operator.
4. The spammer sends instructions via the IRC server to the infected PCs causing them to send out spam messages to mail servers.



Botnets

- A botnet's originator (aka "bot herder") can control the group remotely, usually through a means such as IRC.
- A botnet is more power than a supercomputer in terms of its processing capacity.
- As of 2007, the average size of a botnet was estimated at 20,000 computers, although larger networks continued to operate.



Botnet Case Study

STORM BOTNET

- The Storm botnet is a remotely-controlled network of "zombie" computers (or "botnet") that has been linked by the Storm Worm, a Trojan horse spread through e-mail spam.
- Sources have placed the size of the Storm botnet to be around 250,000 to 1 million compromised systems.



Botnet Case Study

STORM BOTNET

- Detected in January 2007
- 1.2 billion virus messages have been sent by the botnet till September 2007
- The Storm botnet has been used in a variety of criminal activities.
- Its controllers, and the authors of the Storm Worm, have not yet been identified.



Botnet Case Study

STORM BOTNET

- The botnet has specifically attacked the online operations of some security vendors and researchers who attempted to investigate the botnet
- The botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet,
- The Storm botnet's operators control the system via peer-to-peer techniques, making external monitoring and disabling of the system more difficult
- There is no central "command-and-control point" in the Storm botnet that can be shut down



Botnet Case Study

STORM BOTNET

Action plan:

- Microsoft update to the Windows Malicious Software Removal Tool (MSRT) may have helped reduce the size of the botnet by up to 20%.
- But, most of the Windows systems are not configured for Automatic updates.
- Consider our country as example, where most home users use pirated copies of windows.
- Pirated copies will get disabled when updated online, because of Windows Genuine Advantage (WGA) program.



More Botnets

Name	Size	Spam sent / day
SRIZBO	315,000	60 billion
BOBAX	185,000	9 billion
RUSTOCK	150,000	30 billion
CUTWAIL	125,000	16 billion
GRUM	50,000	2 billion
OZDOK	35,000	10 billion
NUCRYPT	20,000	5 billion
WOPLA	20,000	600 million
SPAMTHRU	12,000	350 million



Botnet Attacks

Example 1:

Cyber Assault on Estonia

Estonia is a small and one of the most internet enabled country in Europe.



Botnet Attacks

Example 1:

It was attacked by a massive DDOS attempt on May 2007.
Attacked sectors include

- government
- banks
- telecommunications companies
- Internet service providers
- news organizations



Botnet Attacks

Example 1:

- Attack effectively shut down email systems and online banking.
- Attack originated from Russia after Russian govt got angry with Estonia for relocating a Soviet war memorial.
- More than a million zombie computers made the attack possible.



Botnet Attacks

Example 2: April 23, 2008

- Slideshare is a service that lets you upload and embed PowerPoint presentations on the web.
- There were several presentations relating to corruption in the chinese government.
- Chinese authorities requested those slides to be removed.



Botnet Attacks

Example 2: April 23, 2008

- Slideshare was down for a few days due to DDOS attack that originated from China.
- The attack reached a peak of 2.5GB/sec and consisted entirely of packets sent from China
- SlideShare insists that it will do everything it can to protect its users' freedom of speech. As such, it has no plans to remove any of the content in question.



Botnet Attacks

In both examples, botnets were the main attack vehicles.

There are several more examples.

So,

Cyber wars \Leftarrow DDOS \Leftarrow Botnets \Leftarrow Virus/Worm \Leftarrow Ignorant web user



Take Action

If everyone keep their systems secure, such threats can never happen.

Small gestures can avoid gigantic problems in our context.



Action Plan

- Use Anti-virus
- Use Anti-Spyware
- Be aware not to fall for scams and phishing attacks
- Report SPAM



Further Action

- www.419eater.com
- www.antiphishing.org



Web Security

This presentation can be downloaded from
www.bharath.name

For any queries or doubts or help,
bharath@bharath.name



Thank You