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,

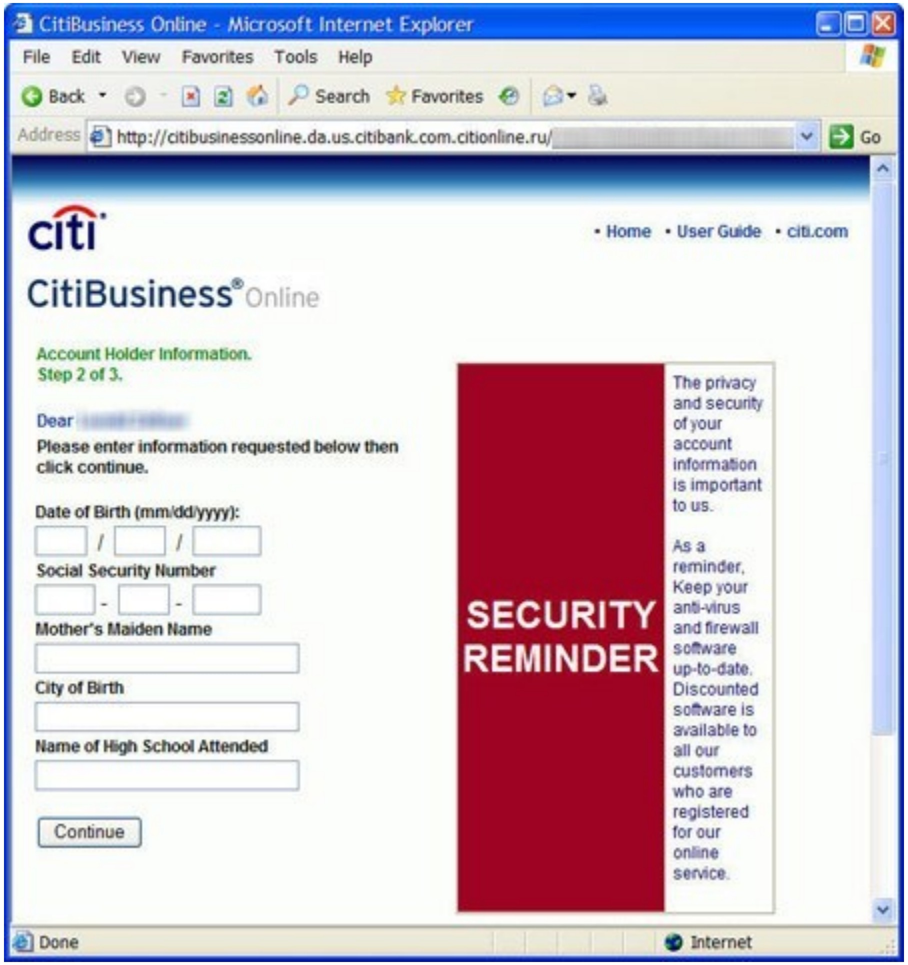
http://citibusinessonline.da.us.citibank.com.citionline.ru/...

Instead of,

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

Phishing

Landing Page


CitiBusiness Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
citi
• Home • User Guide • citi.com
CitiBusiness® Online
Done
Internet

http://citibusinessonline.da.us.citibank.com.citionline.ru/[redacted]

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.

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

What is a denial-of-service attack?

- A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.
- A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

How does a DoS attack work?

- The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall in 2 categories:

- **Buffer overflow attacks**
- An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.
- **Flood attacks**
- By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

What are some historically significant DoS attacks?

- Historically, DoS attacks typically exploited security vulnerabilities present in network, software and hardware design. These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools. In reality, most DoS attacks can also be turned into DDoS attacks.
- A few common historic DoS attacks include:
- Smurf attack - a previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.
- Ping flood - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.
- Ping of Death - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

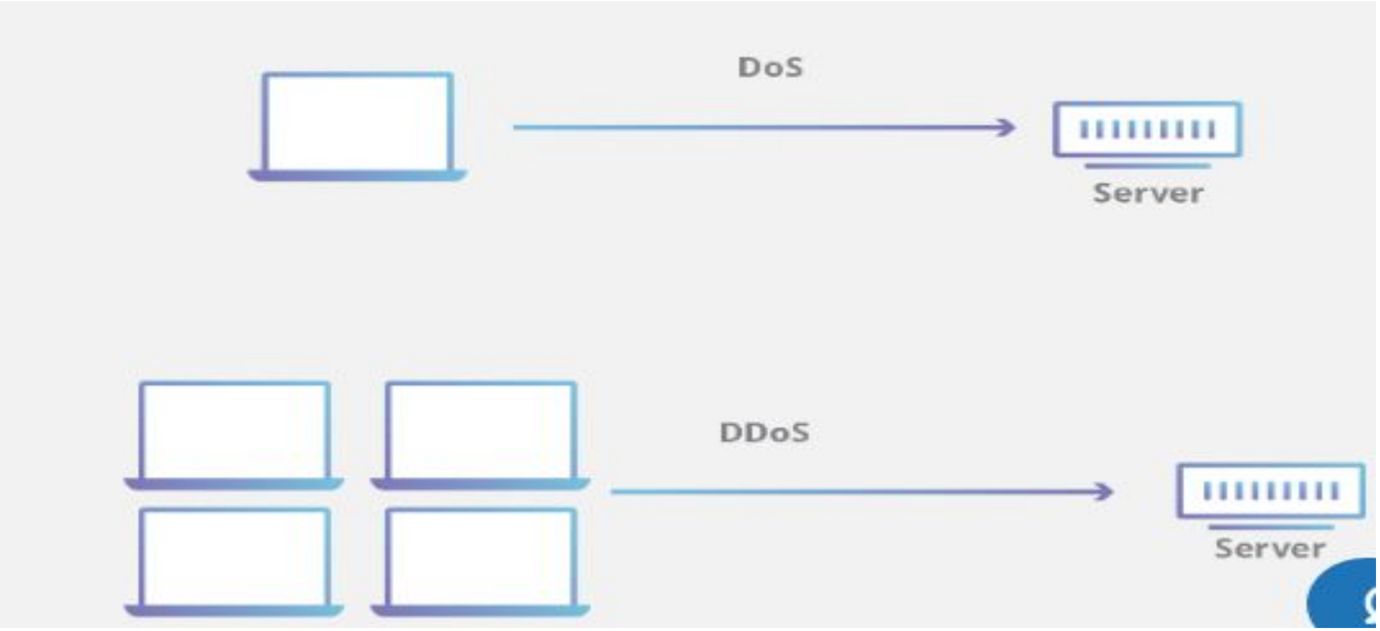
How can you tell if a computer is experiencing a DoS attack?

- While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.
- Indicators of a DoS attack include:
- Atypically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

What is the difference between a DDoS attack and a DOS attack?

- The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as “low and slow” attacks like Slowloris, derive their power in the simplicity and minimal requirements needed to them be effective

- DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic. Learn how Cloudflare's DDoS protection stops denial-of-service attacks


DoS
Server
DDoS
Server

Distributed DOS

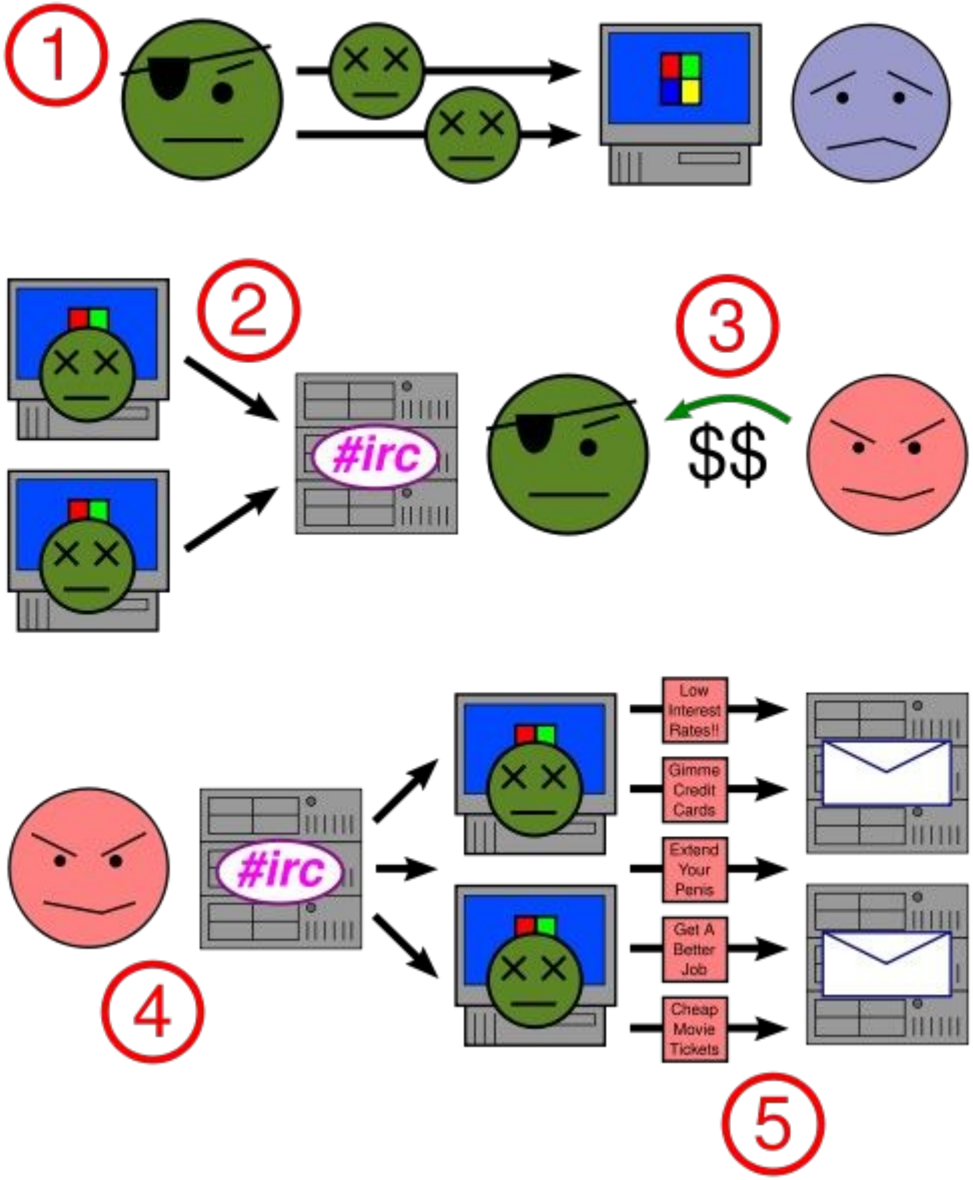
- Zombie system is a system that is brought under the attacker’s control by using virus/worm/exploits.
- Attack is initiated using compromised Zombie systems.
- Very hard to prevent, since large number of zombie systems will be used.

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



Botnet Admin

Bot

Spammer

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

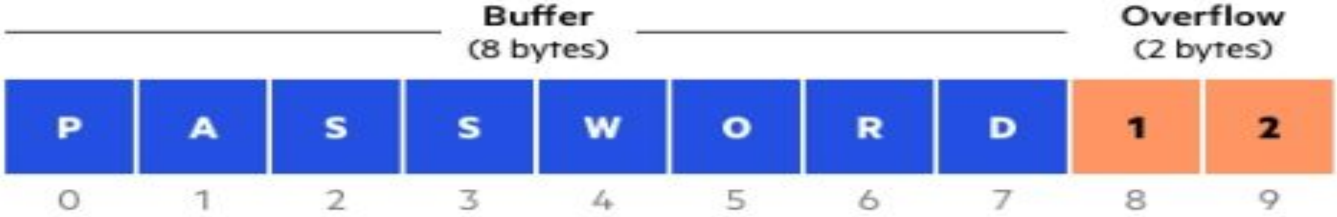
- A botnet's originator (aka "bot herder") can control the group remotely, usually through a means such as IRC.
- A botnet is more power than a supercomputer in terms of its processing capacity.
- As of 2007, the average size of a botnet was estimated at 20,000 computers, although larger networks continued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

- **Buffer Overflow Attack**

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.



Buffer overflow example

What is a Buffer Overflow Attack

- Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.
- If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.
-

Types of Buffer Overflow Attacks

- **Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.
- **Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

How to Prevent Buffer Overflows

- Developers can protect against buffer overflow vulnerabilities via security measures in their code, or by using languages that offer built-in protection.
- In addition, modern operating systems have runtime protection. Three common protections are:
- Address space randomization (ASLR)—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.

- Data execution prevention—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- Structured exception handler overwrite protection (SEHOP)—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

Security measures in code and operating system protection are not enough. When an organization discovers a buffer overflow vulnerability, it must react quickly to patch the affected software and make sure that users of the software can access the patch.

Thank You