

Secure Operating Systems (CYB610)

Master of Science in Cybersecurity

Lecture 9: The Web Security and DoS attacks

Dr. Ibrahim Gomaa

Faculty of Informatics
Midocean University



Lecture 9

Chapter

09

Topics

This chapter covers the following topics and concepts:

- **The Web Security**
 - **Browser attack types**
 - **Email Spam**
- **Denial of Service attacks**
 - **Classes of attacks**
 - **Detection Methods**

Chapter

09

Goals

When you complete this chapter, you will be able to:

- **Describe the web security objectives**
- **Explain the browser attack types**
- **Describe the Email Spam**
- **Explain the General classes of denial-of-service attack**
- **Define the detection of denial-of-service attack methods**



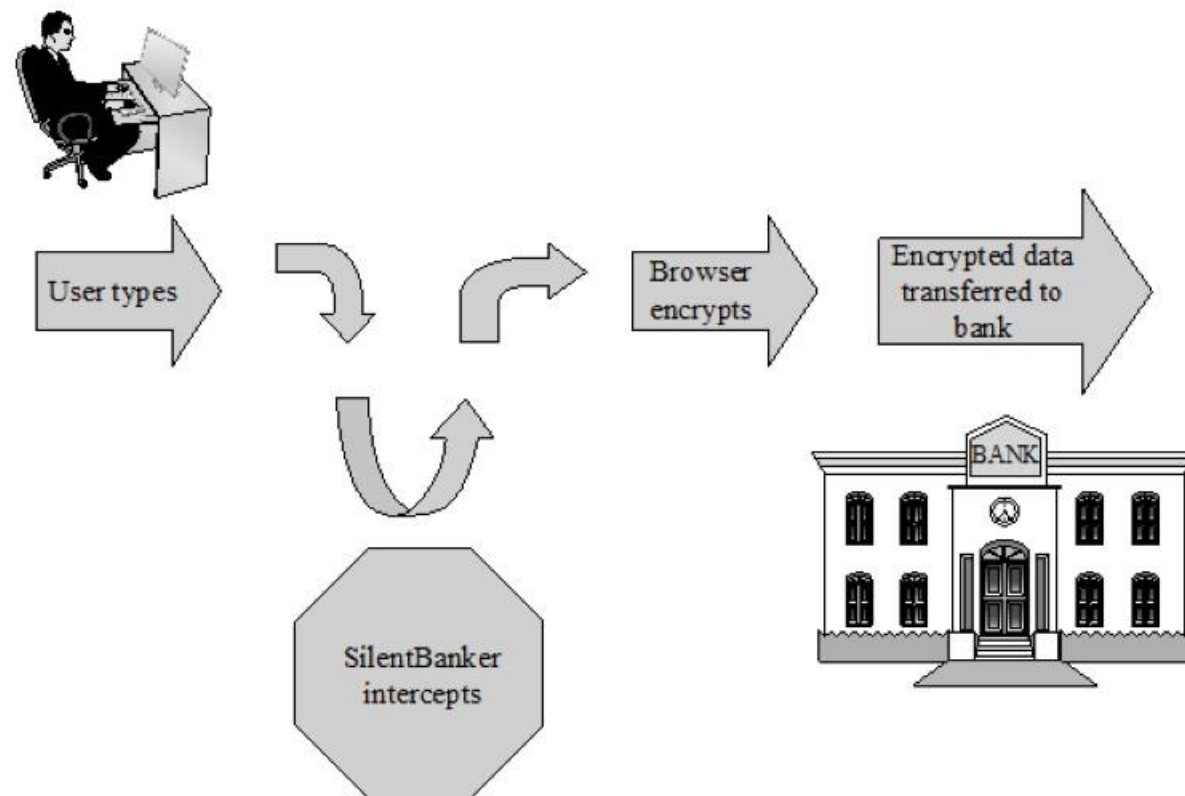
- Attacks against browsers
- Fake and malicious websites
- Attacks targeting sensitive data
- Injection attacks
- Spam
- Phishing attacks



- Man-in-the-browser
- Keystroke logger
- Page-in-the-middle
- Program download substitution
- User-in-the-middle



- **SilentBanker** was a Trojan that generally installed as a browser plug-in. When it detected the user going to a banking URL, it would intercept keystrokes and even modify them so that money transfers would go to attackers' accounts.





- Hardware or software that records all keystrokes
- May be a small dongle plugged into a USB port or can masquerade as a keyboard
- May also be installed as malware
- Not limited to browsers



- User is directed to a different page than believed or intended
- Similar effect to a man-in-the-browser, where attacker can intercept and modify user input



- Attacker creates a page with seemingly innocuous and desirable programs for download
- Instead of, or in addition to, the intended functionality, the user installs malware
- This is a very common technique for spyware



- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf
- CAPTCHAs are used by websites to defeat automation, such as by preventing spammers from scripting the creation of massive numbers of email accounts. By using dummy websites to entice users into solving CAPTCHAs, attackers can effectively defeat the CAPTCHAs at scale.





- The attacks listed before are largely failures of authentication
- Can be mitigated with
 - Shared secret
 - One-time password
 - Out-of-band communication



 **PDF2010**

Home | Download | Members | More Info | Support



The Ultimate PDF Software Pack to
Open, Create & Edit Files
in PDF format

The BEST All in One Office Solution for your PDF files

UPDATE TO 2010 VERSION!

Top Features

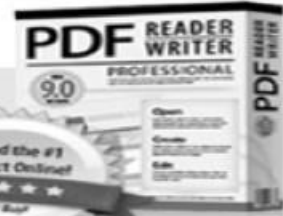
- 50% faster than previous versions
- Search & save online Internet content
- Support for all Operating platforms
- New and improved interface
- Search single or multiple PDF files



FREE OFFICE SUITE INCLUDED!
Download today and receive a FREE copy of the Best **ALL-IN-ONE** Office Solution for Your PDF files! Get Instant access to the Ultimate Office Solution Package! Why wait. Join today and experience the most exciting PDF solution available today!

Writer / Reader

- Download the easiest software to view, create, modify and print PDF documents. The PDF format as a global exchange document format is created by Adobe and is the most efficient way to exchange information.



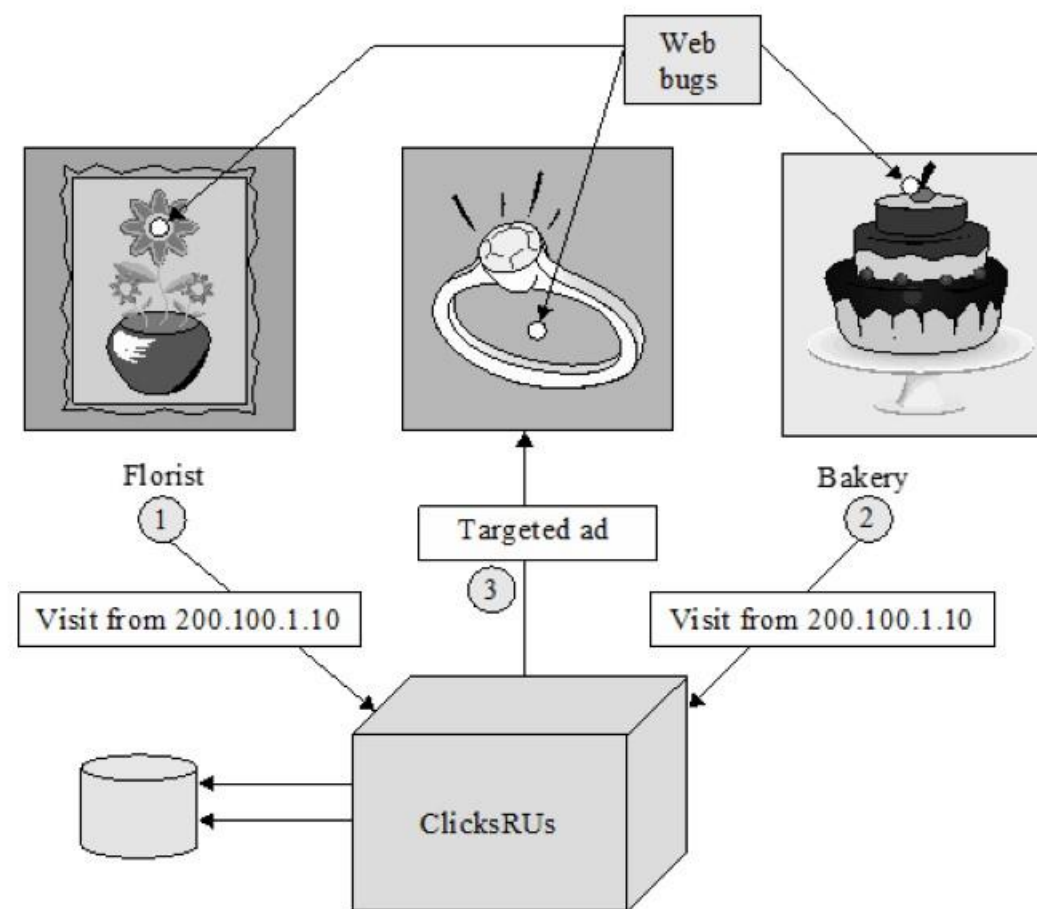
DOWNLOADED NOW!

Average Rating:
★★★★★
Downloads: 267,927
File Size: 14.6 MB
Requirements:
Windows 2000, XP, and Vista

Compatible with all Popular Platforms **Download Now**

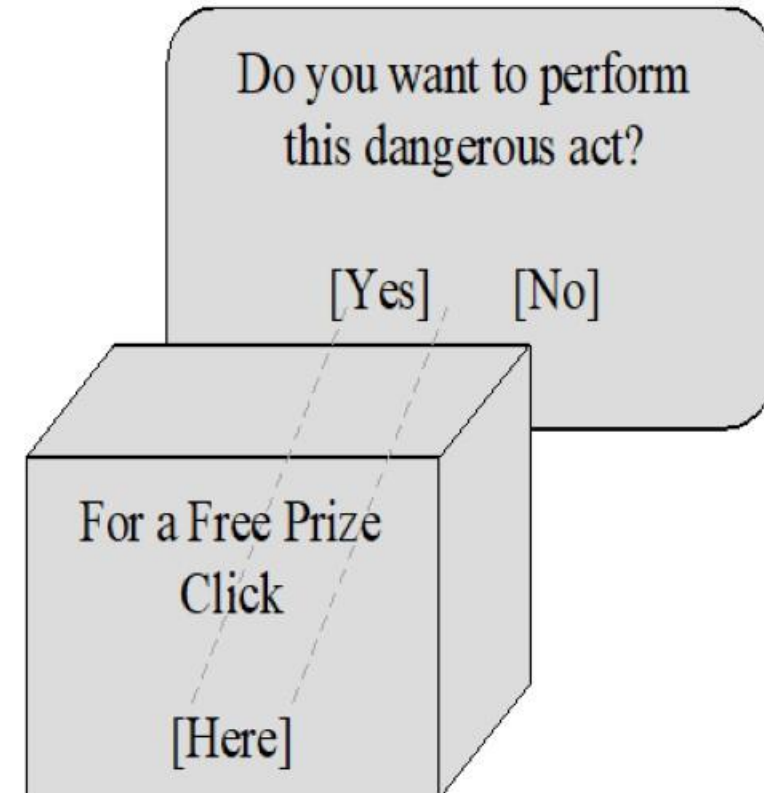


- A tiny image served up from one provider (“ClicksRUs”) that allows user behavior to be tracked across many sites for advertising purposes. You probably notice this when they see web ads that offer up items very similar to ones they’ve recently been shopping for on other sites. Web bugs can also be used to track users’ reading of advertising emails.



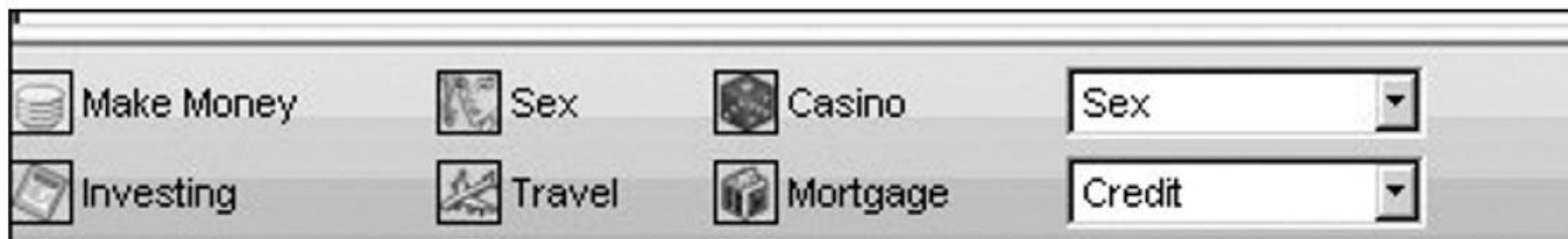


- Clickjacking is a way of tricking users into providing desired input. The attacker makes the input dialog transparent and places an image with an enticement below the transparent dialog. The user ends up answering a question he didn't even know he was being asked, unknowingly authorizing his computer to execute the attacker's will. "Framing"—moving and layering HTML iframes—is an important component of this attack.





- Code is downloaded, installed, and executed on a computer without the user's knowledge
- May be the result of clickjacking, fake code, program download substitution, etc.





- Tricking a client or server into executing scripted code by including the code in data inputs
- Scripts and HTML tags are encoded as plaintext just like user inputs, so they can take over web pages similar to the way buffer overflow attacks can take over programs



- Injecting SQL code into an exchange between an application and its database server
- **Example:**
 - Loading an SQL query into a variable, taking the value of acctNum from an arbitrary user input field:
 - `QUERY = "SELECT * FROM trans WHERE acct = '" + acctNum + "'"; "`
 - The same query with malicious user input:
 - `QUERY = "SELECT * FROM trans WHERE acct = '2468' OR '1'='1'; "`
- The result of this example attack is that the application returns the entire accounts table from the database.



- Also known as “directory traversal,” this is when attackers use the term “../” to access files that are on the target web server but not meant to be accessed from outside
- Most commonly entered into the URL bar but may also be combined with other attacks, such as XSS (Cross-Site Scripting))

```
http://yoursite.com/webhits.htw?CiwebHits&File=../../../../winnt/system32/autoexec.nt
```



- SSI is an interpreted server-side scripting language that can be used for basic web server directives, such as including files and executing commands
- As is the case with XSS, some websites are vulnerable to allowing users to execute SSI directives through text input

```
<!--#exec cmd="/usr/bin/telnet &"-->
```



- Filter and sanitize all user input
 - Need to account for every potentially valid encoding
- Make no assumptions about the range of possible user inputs—**trust nothing, check everything**
- Use **access control** mechanisms on backend servers, such as “stored procedures”
- Stored procedures effectively separate SQL code from SQL data, thus preventing most SQL injection attacks.



- Experts estimate that 60% to 90% of all email is spam
- **Types of spam:**
 - Advertising
 - Pharmaceuticals
 - Stocks
 - Malicious code
 - Links for malicious websites
- **Spam countermeasures:**
 - Laws against spam exist but are generally ineffective
 - Email filters have become very effective for most spam
 - Internet service providers use volume limitations to make spammers' jobs more difficult



- A message that tries to trick a victim into providing private information or taking some other unsafe action
- Spear phishing: A targeted attack that is personalized to a particular recipient or set of recipients





User education

- Limited effectiveness and very subject to co-evolution with attacks
- User education has become more scientific over the years, with products like PhishMe automating the user training process and focusing on the worst offenders.
- **PGP** and **S/MIME** are both solutions for encrypting and signing email.

PGP, which stands for Pretty Good Privacy, is a software program that provides cryptographic privacy and authentication for data communication. It's primarily used for encrypting emails and files

S/MIME, or Secure/Multipurpose Internet Mail Extensions, is a standard for encrypting and digitally signing email messages, enhancing email security



This part explained :

- As web browsers have become a primary focus of users and taken on greater functionality, they've become a focus of many types of attack
- Browser and website weaknesses are often the results of some form of poor authentication
- Many attackers focus on tricking users with fake websites, misleading applications, and phishing emails
- On the server side, injection attacks are a key concern, and countermeasures to prevent them are critical



Denial of Service Attacks



- Definition
- Point-to-point network denial of service
- Distributed denial of service attacks



- DoS attacks are attempts to defeat a system's availability, an explicit attempt by attackers to prevent legitimate users of a service from using that service.
- **Threat model**
 - Consumption of network connectivity and/or bandwidth
 - Consumption of other resources, e.g. queue, CPU
 - Destruction or alteration of configuration information
 - Malformed packets confuse an application, and cause it to freeze
 - Hardware or software failure

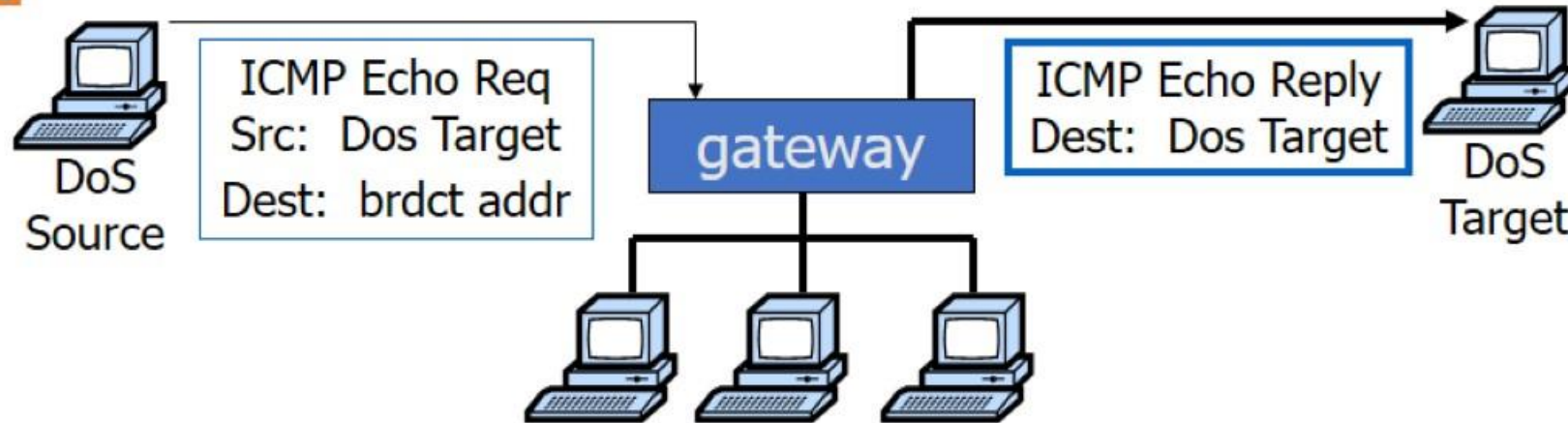


❖ Flooding Attacks

- Point-to-point attacks: TCP/UDP/ICMP flooding, Smurf attacks
- Distributed attacks: hierarchical structures

❖ Corruption Attacks

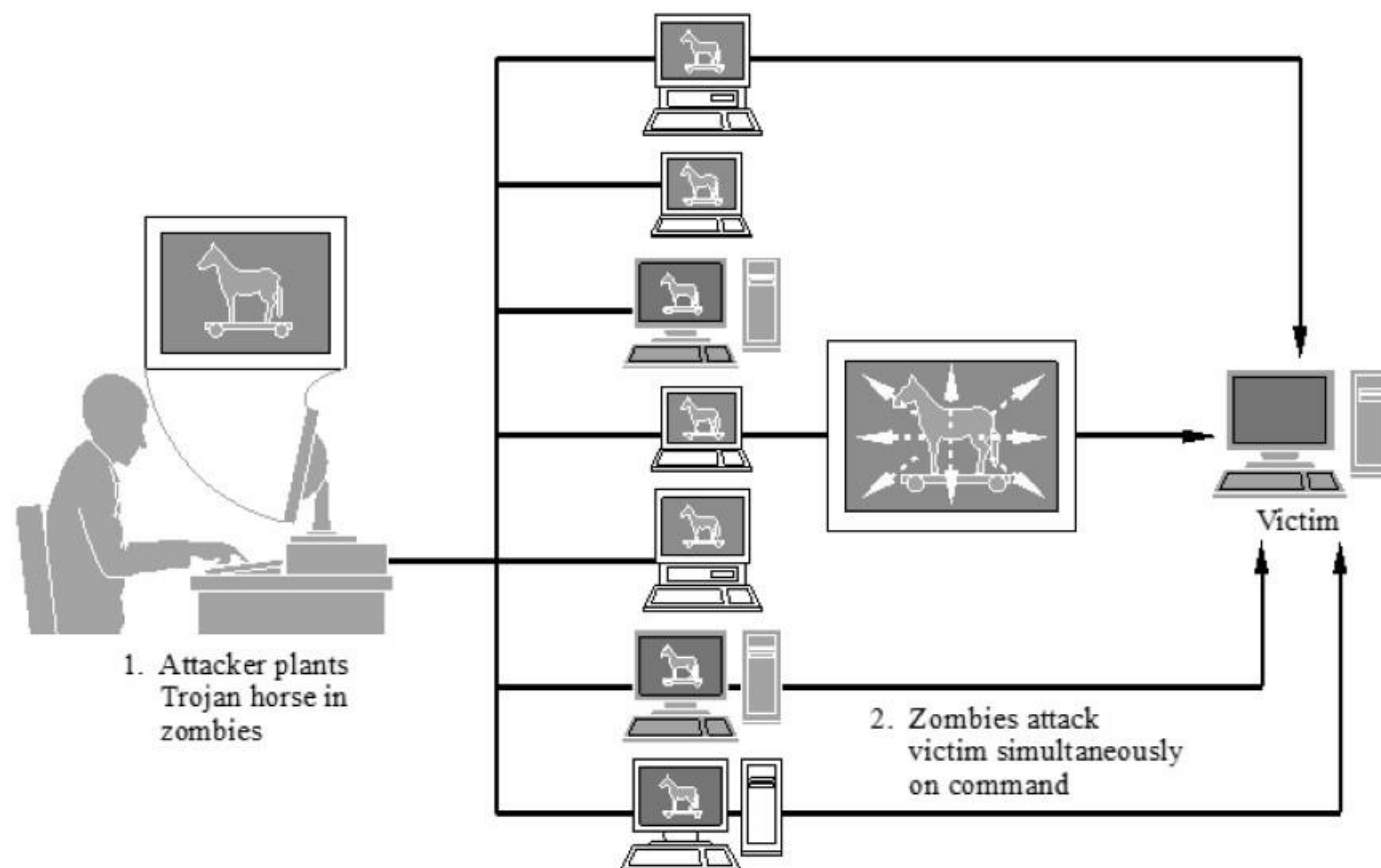
- Application/service specific



- Send ping request to **broadcast address** (ICMP (Internet Control Message Protocol) Echo Request)
- Lots of responses:
 - Every host on target network generates a ping reply (ICMP Echo Reply) to victim
 - Ping reply stream can overload victim



1. Conscript an army of compromised machines to attack a victim.
 2. Choose a victim, and have the whole army unleash a DoS attack at once.
- ❖ DDoS attacks are much more effective than traditional DoS attacks, employing a multiplied version of the same methods.





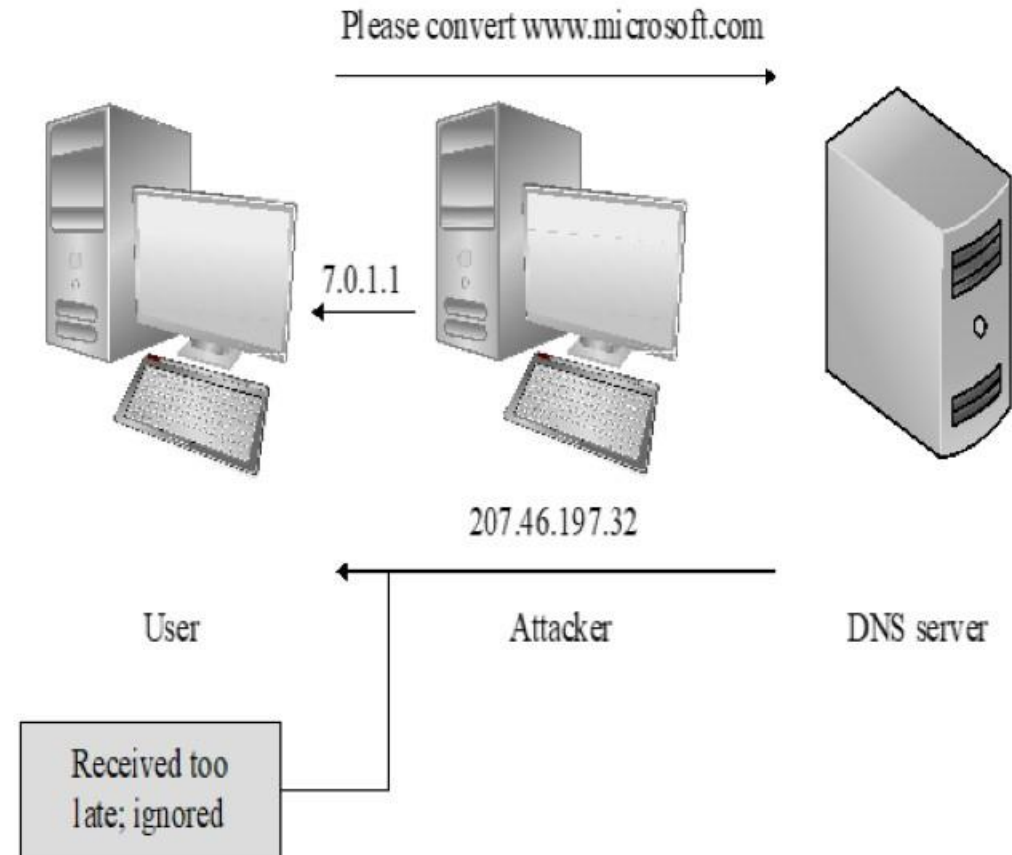
- In August 1999, network of > 2,200 systems took University of Minnesota offline for 3 days
 - scan for known vulnerabilities, then attack with UDP traffic
 - once the host compromised, script the installation of the DDoS master agents
- According to the incident report
 - Took about 3 seconds to get root access
 - In 4 hours, set up > 2,200 agents



- **Spoofed Source Address**
 - random source addresses in attack packets
 - Subnet Spoofed Source Address
 - random address from address space assigned to the agent machine's subnet
 - Route Spoofed Source Address
 - address spoofed in route from agent machine to victim
- **Valid Source Address**
 - used when attack strategy requires several request/reply exchanges between an agent and the victim machine
 - target specific applications or protocol features



- The attacker acts as the DNS (Domain Name Service) server in order to redirect the user to malicious sites





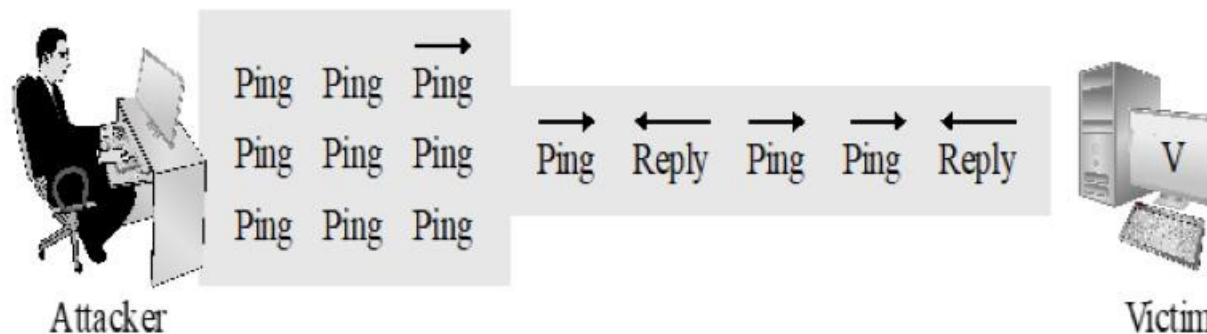
Agent machine sends a stream of packets to the victim

- **Constant Rate**

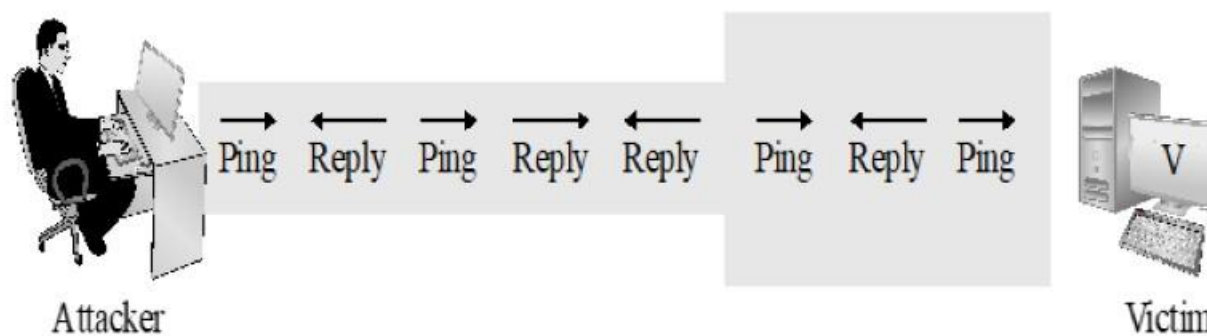
- Attack packets generated at constant rate, usually as many as resources allow

- **Variable Rate**

- Delay or avoid detection and response
- Increasing Rate
 - gradually increasing rate causes a slow exhaustion of the victim's resources
- Fluctuating Rate
 - occasionally relieving the effect
 - The victim can experience periodic service disruptions



(a) Attacker has greater bandwidth



(b) Victim has greater bandwidth

- A Ping flood attack, is An Internet Control Message Protocol (ICMP) flood DDoS attack, in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings), overwhelming its network resources and bandwidth.
- As a result, the target becomes unable to process legitimate requests, causing service disruptions and outages.



- An attacker can trigger the Echo-Chargen attack by **spoofing a conversation between the Echo Request/Reply service and the Chargen service** and then redirecting the output of each service to the other, creating a rapidly expanding spiral of traffic in the network



Victim A



Victim B

Chargen packet → with echo bit on

← Echoing what you just sent me

Chargen another packet → with echo bit on

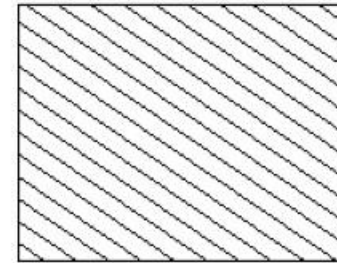
← Echoing that again

Chargen another packet → with echo bit on

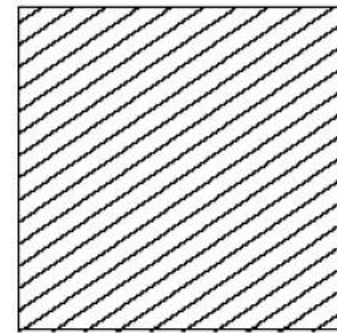


- The attacker **sends packets that cannot possibly be reassembled** (conflicting reassembly instructions). In extreme cases, this can cause the entire OS to lock up.
- The most common teardrop attack example is the attack that happened on The Office of Personnel Management (OPM) in 2014. As a result of the attack, millions of US government employee records went under the control of a Chinese hacker.

Fragment start = 10 len = 50



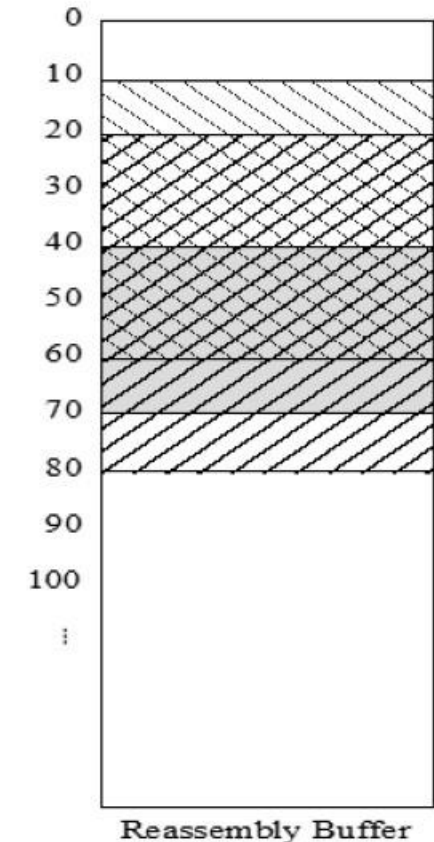
Fragment start = 20 len = 60



Fragment start = 40 len = 30

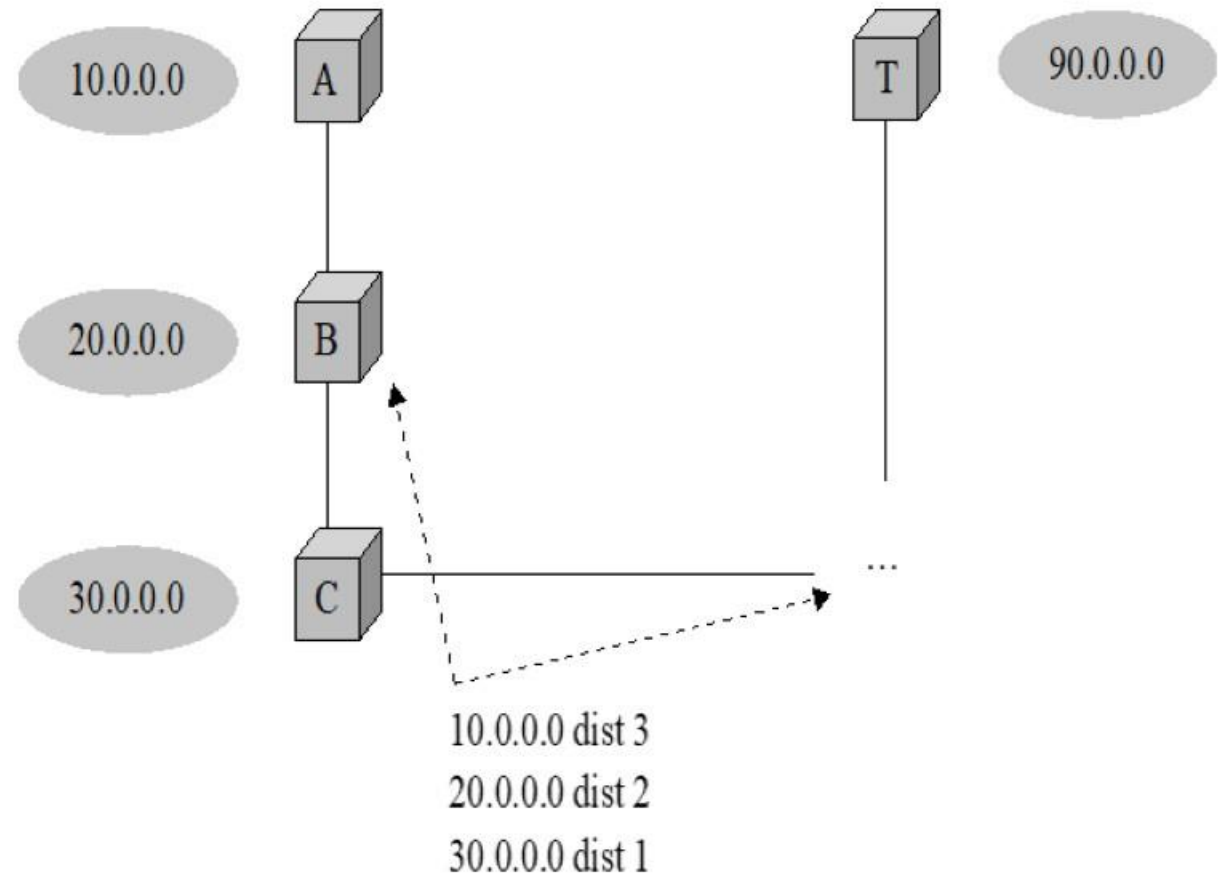


Packet Fragments



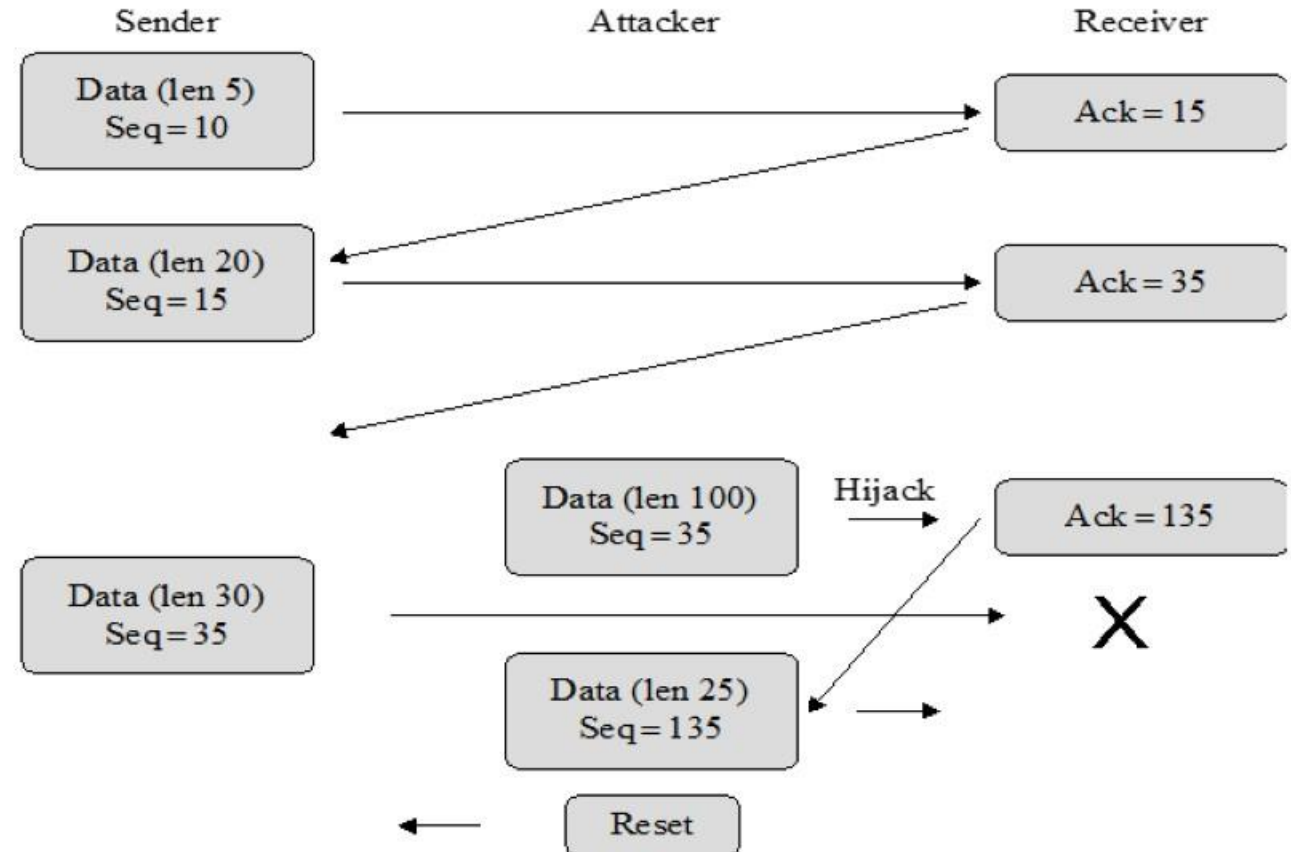


- Rerouting attacks attempt to redirect traffic from its valid destination to a false one.
- This picture doesn't show anything malicious happening. It just shows how one router, C, advertises the routes it knows about to the routers adjacent to it. Routers rely on these advertising messages to be accurate; when they aren't, DoS can ensue.



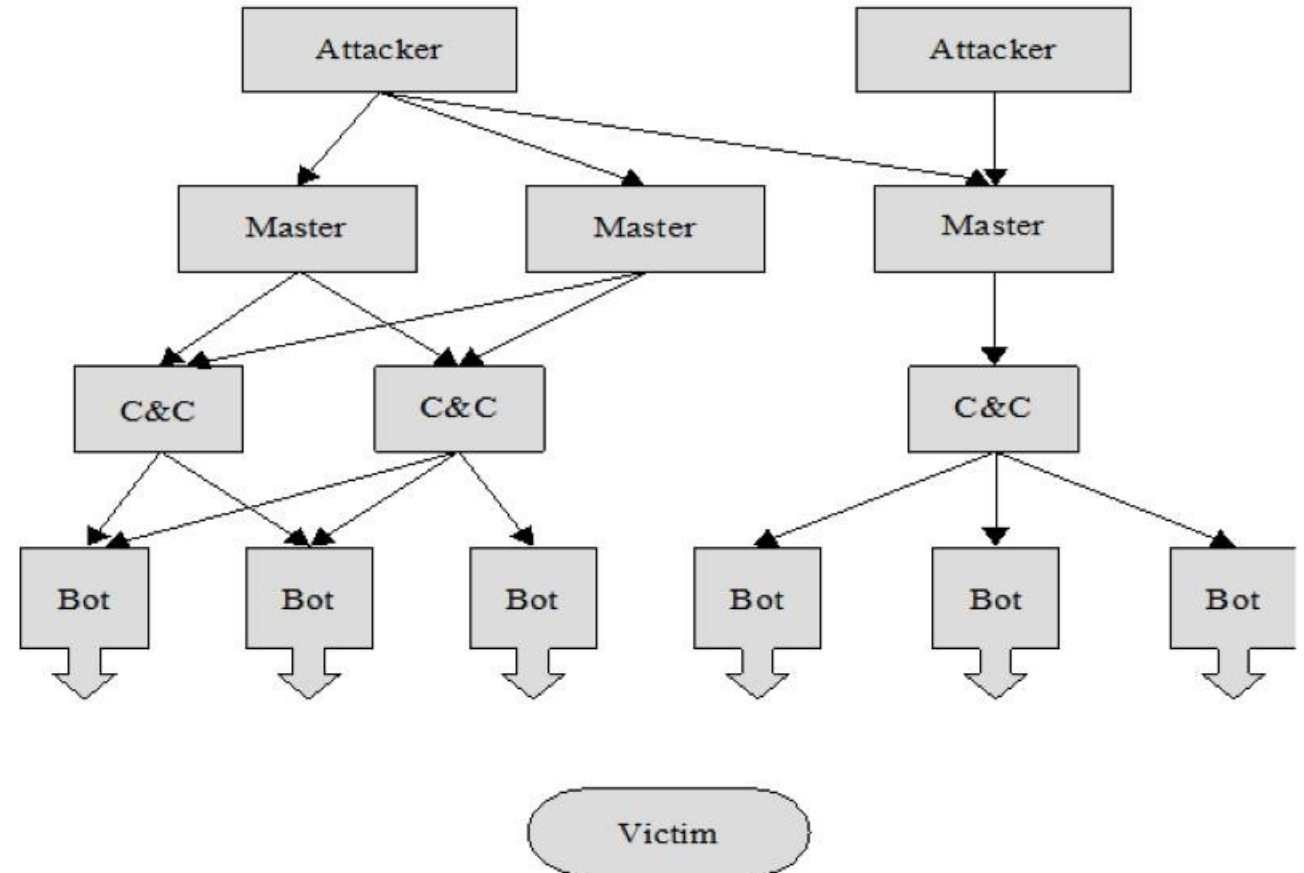


- An attack in which the attacker is able to insert himself between a sender and a receiver subsequent to a successful authentication exchange between the latter two parties.
- The attacker is able to pose as a subscriber to the sender or vice versa to control session data exchange
- In this image of TCP session hijacking, an attacker is able to synchronize with a receiver while breaking synchronization with the sender and resetting the sender's connection. The attacker continues the TCP session while the sender thinks the connection just broke off.





- Botnets are **networks of machines running malicious code under remote control**. They are often undetected because they do little harm to the machines they run on. Botnets are often used to execute DDoS attacks. The image beside shows how Botnet command and control (C&C) updates occur. Multiple layers separate the attacker from the bots, making the attacker challenging to trace. Numerous redundant systems are built so that if one master or C&C node is taken down, the bots can continue to connect to the botnet.





- **Hard to find Bad Guy**
 - The originator of the attack compromised the handlers
 - The originator not active when DDOS attack occurs
- **Can try to find agents**
 - The source IP address in packets is not reliable
 - Need to examine traffic at many points, modify traffic, or modify routers



- Can we maintain states for each connection flow?
- Stateless, simple detection system on edge (leaf) routers desired
- Placement: First/last mile leaf routers
 - First mile – detect large DoS attacker
 - Last mile – detect DDoS attacks that first mile would miss

But high-volume attacks can overwhelm these devices, since they utilize memory-intensive stateful examination methods.



This part explained :

- Two General Classes of Attacks
 - Flooding Attacks
 - Corruption Attacks
- Point-to-point network denial of service
- Distributed denial of service attacks



Thank You