

COMPUTER SECURITY

Chapter 6: Network Security

Rise of the Hackers

- [Rise of the Hackers](#)

NETWORKS SECURITY

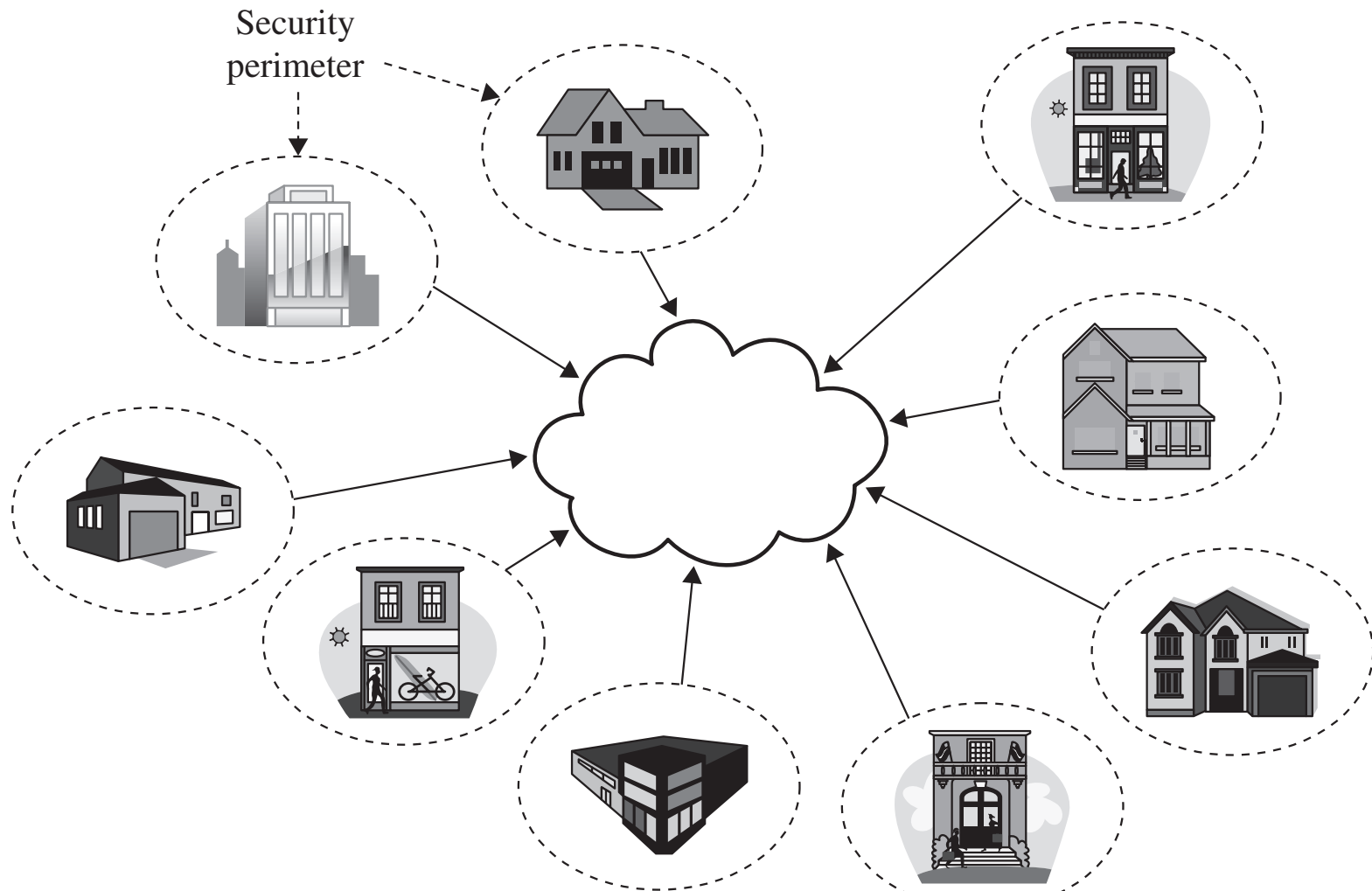
Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Threats to Network Communications

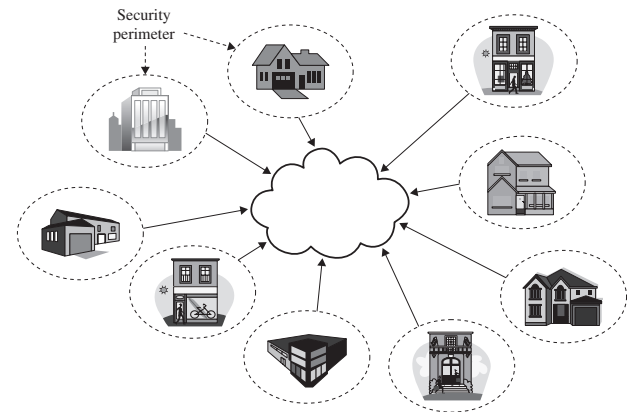
- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Security Perimeters



Interception

- Each of these places is a security perimeter in and of itself
- Within each perimeter, you largely control your cables, devices, and computers
 - because of physical controls
 - => you don't need to worry as much about protection



Interception

- But you have to make connections between security perimeters
 - => exposes you to all sort of cables, devices, and computers you can't control
 - Encryption is the most common and useful control for addressing this threat.

What Makes a Network Vulnerable to Interception?

- Anonymity
 - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
 - Large networks mean many points of potential entry
- Sharing
 - Networked systems open up potential access to more users than do single computers

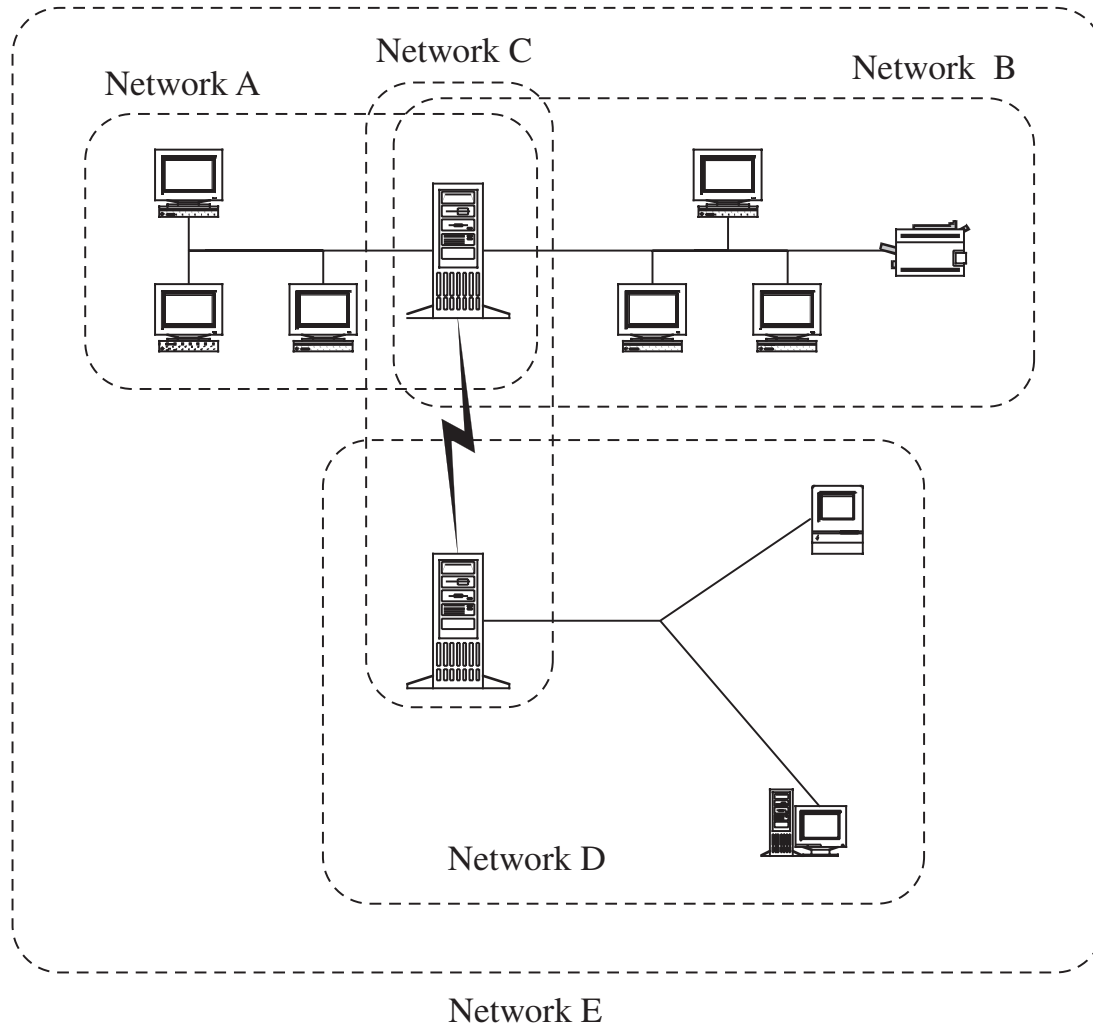
What Makes a Network Vulnerable to Interception?

- System complexity
 - One system is very complex and hard to protect;
 - Networks of many different systems
 - with disparate OSs, vulnerabilities, and purposes are that much more complex

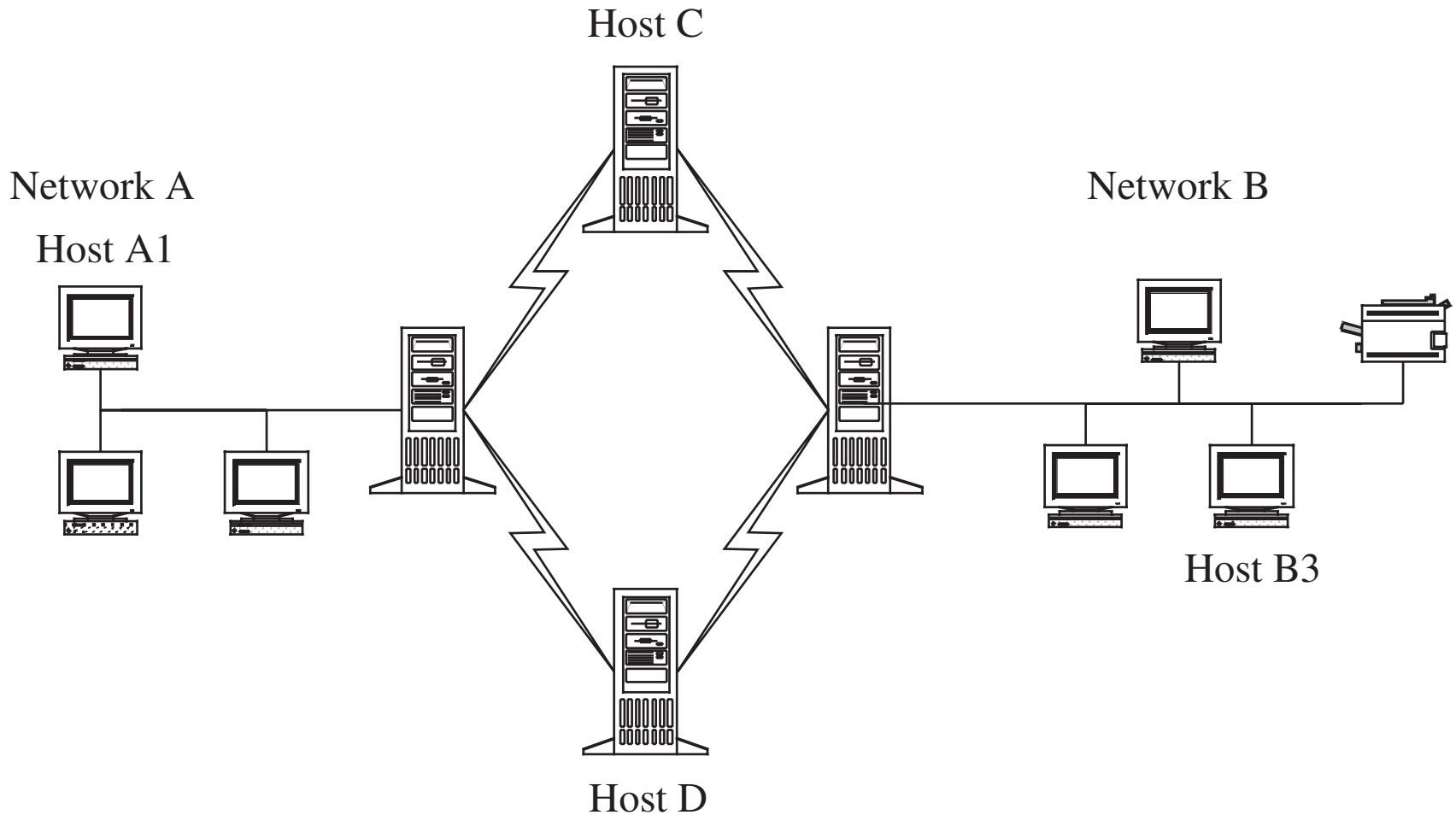
What Makes a Network Vulnerable to Interception?

- Unknown perimeter
 - Networks, especially large ones, change all the time
 - it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
 - There may be many paths, including untrustworthy ones, from one host to another

Unknown Perimeter



Unknown Path



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

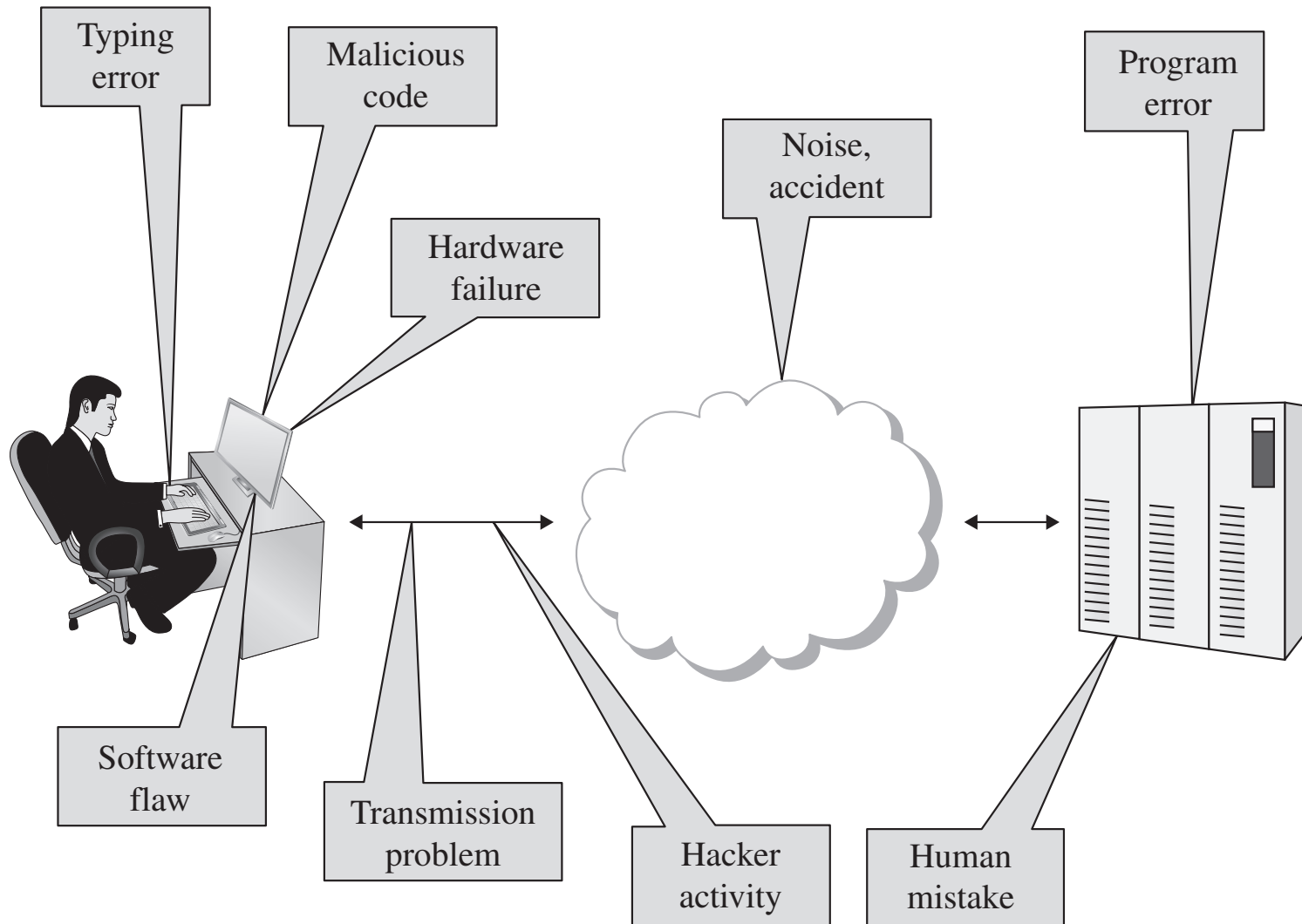
Modification and Fabrication

- Data corruption
 - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
 - Permuting the order of data, such as packets arriving in sequence
- Substitution
 - Replacement of one piece of a data stream with another

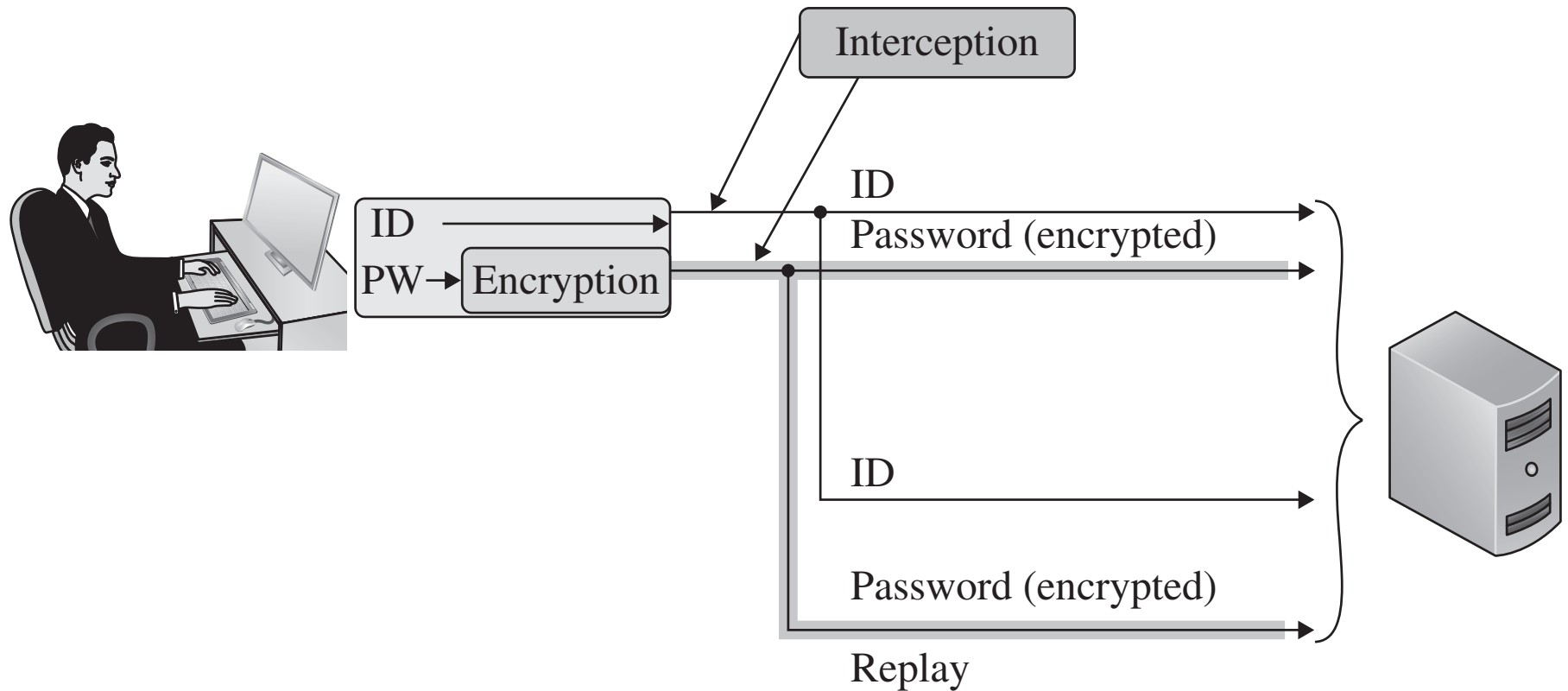
Modification and Fabrication

- Insertion
 - A form of substitution in which data values are inserted into a stream
- Replay
 - Legitimate data are intercepted and reused

Sources of Data Corruption



Simple Replay Attack



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Interruption: Loss of Service

- Routing
 - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
 - Network capacity is finite and can be exhausted;
 - an attacker can generate enough demand to overwhelm a critical part of a network

Interruption: Loss of Service

- Component failure
 - Component failures tend to be sporadic and unpredictable
 - will cause loss of service if not planned for

Port Scanner

- An application designed to probe a server or host for open ports.
- May be used by:
 - Administrators, to verify security policies of their networks
 - Attackers, to identify network services running on a host and exploit vulnerabilities

Port Scan

- A process that sends client requests to a range of server port addresses on a host
 - with the goal of finding an active port;
 - not a nefarious process in and of itself.
- Port scan can be used to determine services available on a remote machine
- The majority of uses of a port scan are not attacks

Port Scanning

- Port Scanning is a common first step to attacks
- Example: sample output from an NMAP port scan
 - Available Data: port, protocol, state, service, product, and version

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
```

Port	State	Service	Reason	Product	Version	Extra info
21	tcp open	ftp	syn-ack	ProFTPD	1.3.1	
22	tcp filtered	ssh	no-response			
25	tcp filtered	smtp	no-response			
80	tcp open	http	syn-ack	Apache	2.2.3	(CentOS)
106	tcp open	pop3pw	syn-ack	poppassd		
110	tcp open	pop3	syn-ack	Courier	pop3d	
111	tcp filtered	rpcbind	no-response			
113	tcp filtered	auth	no-response			
143	tcp open	imap	syn-ack	Courier	Imapd	released
2004						
443	tcp open	http	syn-ack	Apache	2.2.3	(CentOS)
465	tcp open	unknown	syn-ack			
646	tcp filtered	ldp	no-response			
993	tcp open	imap	syn-ack	Courier	Imapd	released
2004						
995	tcp open		syn-ack			
2049	tcp filtered	nfs	no-response			
3306	tcp open	mysql	syn-ack	MySQL	5.0.45	
8443	tcp open	unknown	syn-ack			

```
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
```

Port	State	Service	Reason	Product	Version	Extra info
21	tcp open	ftp	syn-ack	ProFTPD	1.3.1	
22	tcp filtered	ssh	no-response			
25	tcp filtered	smtp	no-response			
80	tcp open	http	syn-ack	Apache	2.2.3	(CentOS)
106	tcp open	pop3pw	syn-ack	poppassd		
110	tcp open	pop3	syn-ack	Courier	pop3d	
111	tcp filtered	rpcbind	no-response			
113	tcp filtered	auth	no-response			
143	tcp open	imap	syn-ack	Courier	Imapd	released
2004						
443	tcp open	http	syn-ack	Apache	2.2.3	(CentOS)
465	tcp open	unknown	syn-ack			
646	tcp filtered	ldp	no-response			
993	tcp open	imap	syn-ack	Courier	Imapd	released
2004						
995	tcp open		syn-ack			
2049	tcp filtered	nfs	no-response			
3306	tcp open	mysql	syn-ack	MySQL	5.0.45	
8443	tcp open	unknown	syn-ack			

```
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port      State      Service Reason      Product      Version      Extra info
21        tcp        open        ftp          220 2.3.4-1  2.3.4-1
```

NMAP Scanning

- [NMap Scanning](#)

NMAP Scanning

- Nmap Firewall Scanning

Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi access

Vulnerabilities in Wireless Networks

- Confidentiality

- Because every message in WiFi is a broadcast
 - unencrypted messages can be read by anyone who's listening and within range

- Integrity

- When WiFi access points receive two streams of communication claiming to be the same computer
 - they necessarily accept the one with greater signal strength
 - This allows attackers to take over and forge sessions by spoofing legitimate computers and boosting signal strength

Vulnerabilities in Wireless Networks

- Availability
 - In addition to the obvious availability issues, WiFi creates new availability problems
 - such as session hijacking, forced disassociation, and jamming.
- Unauthorized WiFi access:
 - Some form of cryptographic control is necessary to solve this

Wireless Security

- What are the current security options for protecting WIFI networks?
- Originally WEP was introduced as part of the original 802.11
- Designed to protect packets from eavesdroppers
- Not used today
 - Covered for historical reasons

Failed Countermeasure: WEP

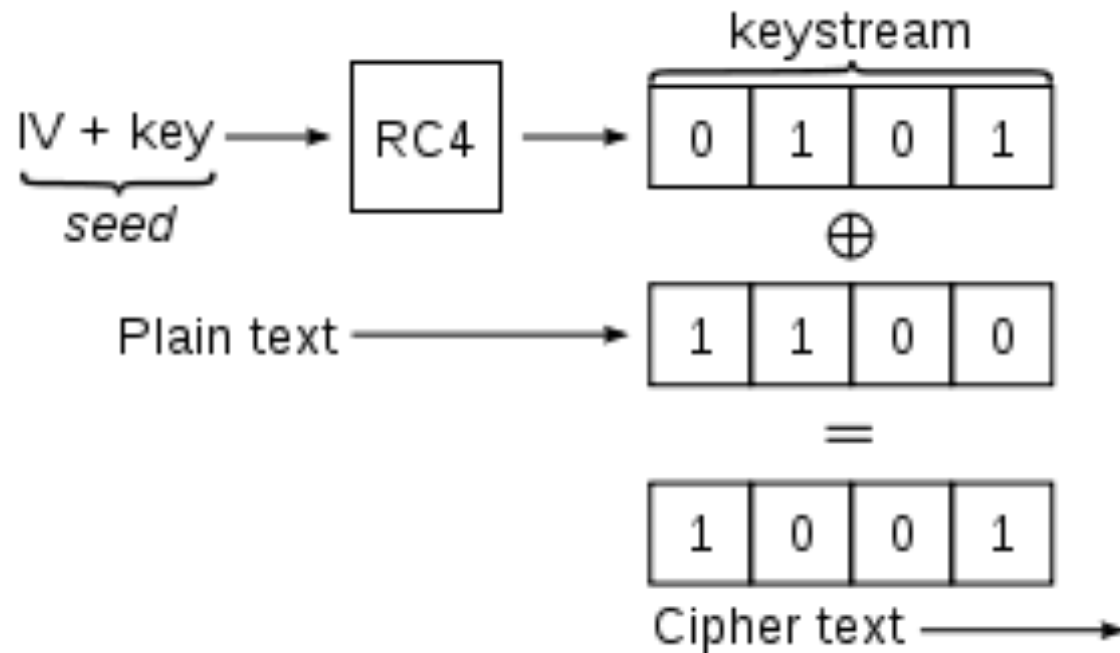
- Wired equivalent privacy (WEP), designed as the mechanism for securing those communications
 - Designed to provide similar security to wired communication
 - at the same time as the original 802.11 WiFi standards

Failed Countermeasure: WEP

- Weaknesses in WEP first identified in 2001, four years after release
- More weaknesses were discovered over the course of years
 - until any WEP-encrypted communication could be cracked in a matter of minutes

WEP

- Basic WEP encryption: RC4 keystream XORed with plaintext



https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

How WEP Works

- Supported two system modes:
 - Open System Authentication
 - Clients did not supply credentials
 - Clients had to have pre-shared key to communicate with the AP
 - Or to be able to decrypt frames coming from AP
 - Shared Key Authentication

WEP Shared Key Authentication

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client
 - which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it's the same number
 - to authenticate the client

WEP Shared Key Authentication (cont.)

- Once the client is authenticated, the AP and client communicate
 - using messages encrypted with the key
- Any issues with this?
 - Key and encrypted key sent in the clear
 - Vulnerable to cryptanalysis attack
 - Both plaintext and ciphertext sent in the clear
 - However, not the main weakness in WEP

WEP Weaknesses

- Weak encryption key
 - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV)
 - => reducing effective key size to 40 or 104 bits
 - Keys were either alphanumeric or hex phrases that users typed in
 - => therefore vulnerable to dictionary attacks

WEP Weaknesses

- Static key
 - the key was a value user typed in at the client and AP
 - users rarely changed those keys
 - => one key would be used for many months of communications
- Weak encryption process
 - A 40-bit key can be brute forced easily
 - Flaws eventually discovered in the RC4 encryption algorithm WEP uses
 - made the 104-bit keys easy to crack as well

WEP Weaknesses

- Weak encryption algorithm
 - WEP used RC4 in a strange way (always a bad sign)
 - => resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
 - There were only 16 million possible values of IV
 - in practice, this is not that many to cycle through for cracking.
 - IV's were not as randomly selected as desired
 - some values were much more common than others
 - IV's were sent in plaintext

WEP Weaknesses (cont.)

- Faulty integrity check
 - WEP messages included a checksum to identify transmission errors
 - but did not use one that could address malicious modification
- No authentication
 - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WEP Weaknesses

- Today open source tools can show attacks on WEP key in minutes
 - Aircrack-ng, etc.
- Some legacy systems may still run WEP
 - Should not be used



Tutorial: Simple WEP Crack

Version: 1.20 January 11, 2010

By: darkAudax

Introduction

This tutorial walks you through a very simple case to crack a WEP key. It is intended to build your basic skills and get you familiar with the concepts. It assumes you have a working wireless card with drivers already patched for injection.

The basic concept behind this tutorial is using aireplay-ng replay an ARP packet to generate new unique IVs. In turn, aircrack-ng uses the new unique IVs to crack the WEP key. It is important to understand what an ARP packet is. This **"What is an ARP?"** section provides the details.

https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

WPA (WiFi Protected Access)

- WPA was designed as a replacement for WEP (2003)
 - quickly followed by WPA2 (in 2004), the algorithm that remains the standard today
 - Designed to be compatible with old WPA-compatible hardware
 - With simple firmware update

WPA (WiFi Protected Access)

- Temporal Key Integrity Protocol (TKIP):
 - A secure key-derivation protocol
 - Incorporating IV into per-packet encryption key
 - A sequence counter implemented
 - Rejecting out-of-order packets, prevent replay attack
 - A 64 Message Integrity Check(MIC) introduced
 - Prevent forging or corruption of packets

WPA (WiFi Protected Access)

- Used RC4 cipher
 - But in a more secure way
 - Used key-mixing function to generate unique keys per packet
 - Generated 256-bit keys

WPA (WiFi Protected Access)

- Non-static encryption key
 - WPA uses a hierarchy of keys:
 - New keys are generated for confidentiality and integrity of each session
 - encryption key is automatically changed on each packet
 - The keys that are most important are used in very few places and indirect ways
 - protecting them from disclosure
 - The user WI-FI password is used as one of the factors when deriving the encryption keys.

WPA (WiFi Protected Access)

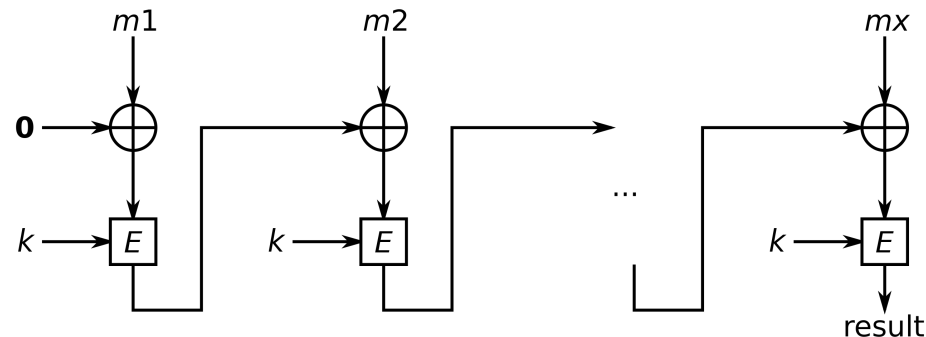
- Authentication
 - WPA allows authentication by password, token, or certificate
- Strong encryption
 - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
 - WPA includes a 64-bit cryptographic integrity check

WPA (cont.)

- Session initiation
 - WPA sessions begin with authentication and a four-way handshake
 - => results in separate keys for encryption and integrity on both ends
- There are some attacks against WPA
 - they are either of very limited effectiveness or require weak passwords

WPA2

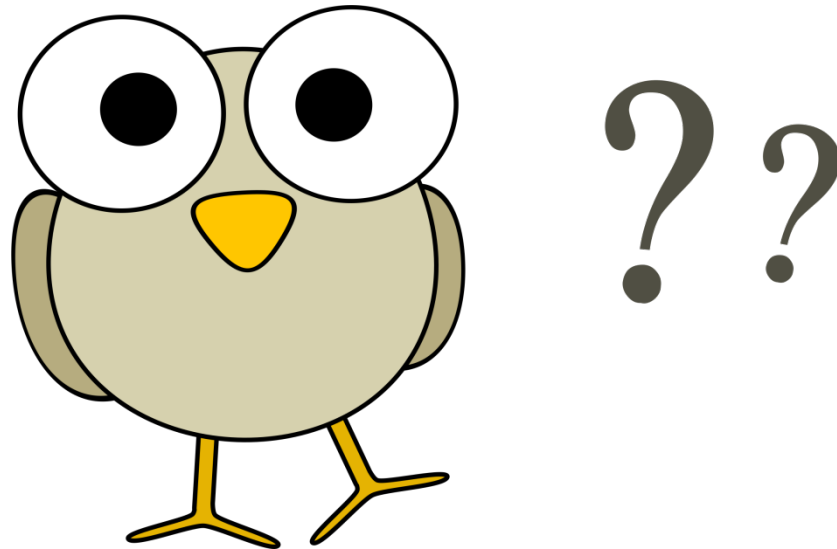
- The most secure protocol for wireless networks today
- Implemented counter mode CBC-MAC protocol
 - a technique for constructing a message authentication code from a block cipher



WPA2

- Based on AES
 - Not using RC4
- Allows for authenticated encryption
 - Data is confidential and authenticated
 - Authenticate and encrypt

- Questions?



COMPUTER SECURITY QUIZ

What is a computer network?

- A. A super computer owned only by the government
- B. A web of connected computers or devices
- C. A computer vulnerability
- D. An Internet service provider
- E. All of the above

What is a computer network?

- A. A super computer owned only by the government
- ✓ • B. A web of connected computers or devices
- C. A computer vulnerability
- D. An Internet service provider
- E. All of the above

Why are cyber vulnerabilities unlikely to ever go away?

- A. Criminals need them to steal identities.
- B. They are side effects of the freedom and ease of communicating online.
- C. They're protected in a secret base on the moon.
- D. The government won't allow people to fix them.


Why are cyber vulnerabilities unlikely to ever go away?

- A. Criminals need them to steal identities.
- ✓ B. They are side effects of the freedom and ease of communicating online.
- C. They're protected in a secret base on the moon.
- D. The government won't allow people to fix them.

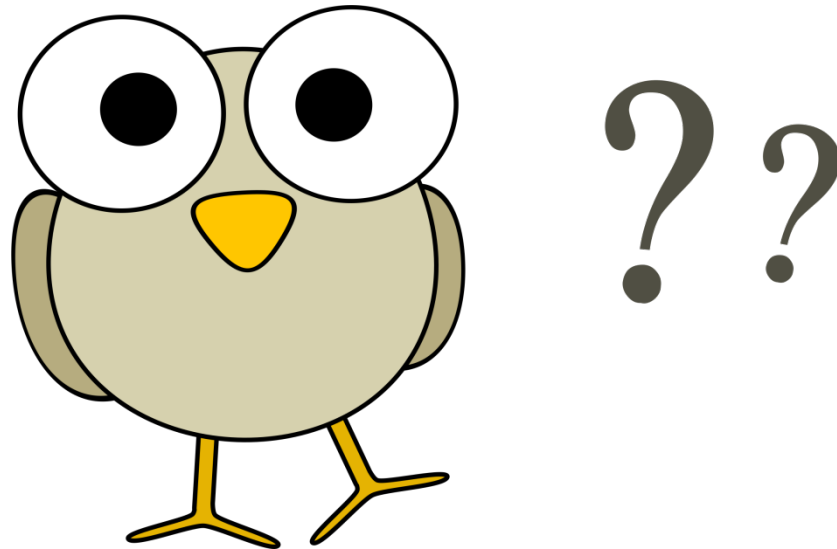
The size and complexity of networks grew enormously when:

- A. Only governments and universities owned computers.
- B. Spamware caused some computers to break down
- C. The number of personal computers greatly increased.
- D. The hacktivists started using the internet

The size and complexity of networks grew enormously when:

- A. Only governments and universities owned computers.
- B. Spamware caused some computers to break down
-  C. The number of personal computers greatly increased.
- D. The hacktivists started using the internet

- Questions?



NETWORK ATTACKS

DOMAIN NAME SERVER (DNS)

- A DNS server is used to resolve a particular domain **to its IP equivalent**
 - Takes time since once a new website request is made,
 - Client asks the resolver
 - Resolver asks the root server for information.
 - Client must wait to receive a response.

DOMAIN NAME SERVER (DNS) Cache

- To save time, DNS cache is created
 - Temporary storage of information about previous DNS lookups on a machine's OS or web browser
 - Keeping a local copy of a DNS lookup allows OS or browser to quickly retrieve it
 - thus a website's URL can be resolved to its corresponding IP much more efficiently

Domain Name Service (DNS) Cache

- A temporary database, maintained by a computer's operating system
- contains records of all the recent visits to websites and other internet domains.
 - A DNS cache is just a memory of recent DNS lookups
 - computer uses when trying to figure out how to load a website

DNS Cache

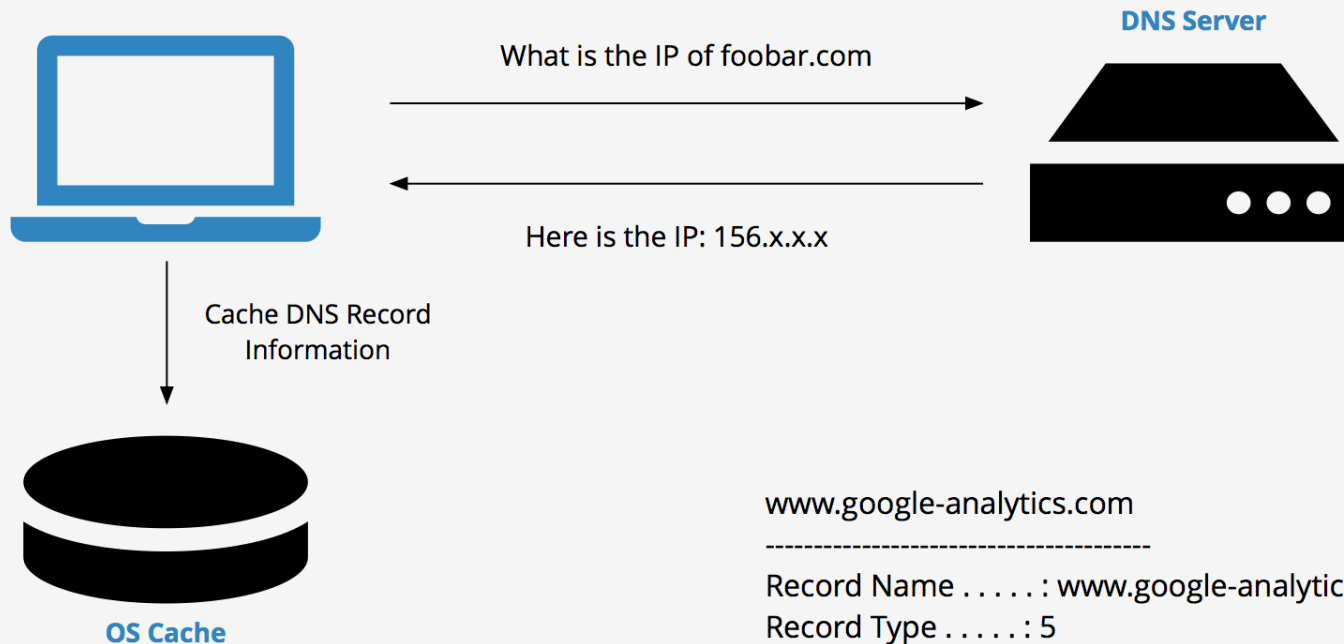
- DNS maintains an index of all public websites and their corresponding IP addresses
 - Analogous to a phone book
 - With a phone book, we can find everyone's phone number
 - Phones need number to communicate
 - Similarly, DNS is used to find website's IP address
 - Needed so network equipment can communicate with websites
 - Occurs when you ask your web browser to load a website.

DNS Cache Example

- You type in a URL like google.com
- your web browser asks your router for the IP address
- The router has a DNS server address stored
 - it asks the DNS server for the IP address of that hostname
- The DNS server finds the IP address that belongs to google.com
 - Enables your browser to load the appropriate page

DNS Cache Example

- Occurs every time user asks to view a website
 - the web browser initiates a request out to the internet
 - site's name is converted into an IP address
 - Only then request can be completed



DNS Cache

www.google-analytics.com

Record Name: www.google-analytics.com

Record Type: 5

Time To Live: 104

Data Length: 4

Section: Answer

CNAME Record: www-google-analytics.l.google.com

DNS Cache Poisoning Attack

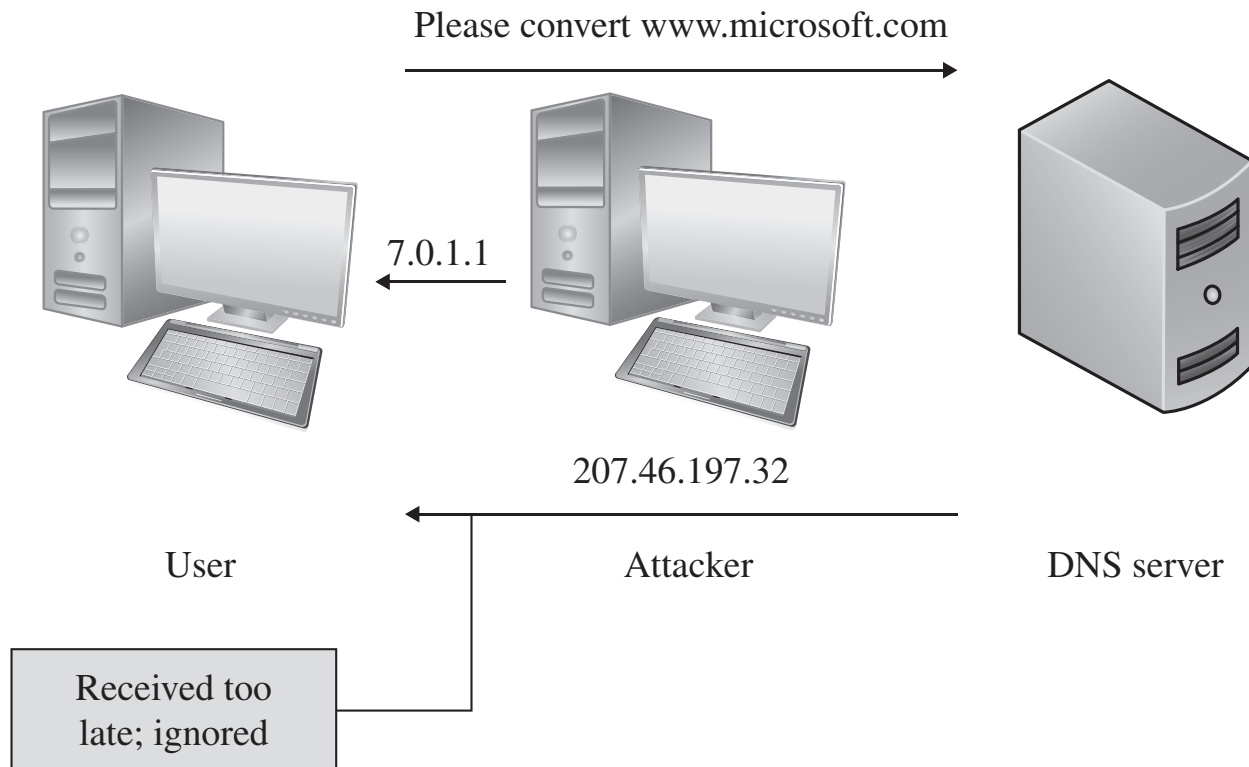
- DNS works by getting information about IP's and names
- **DNS cache poisoning:** a pharming attack directed at changing a host's DNS cache
 - to create a falsified domain-name/IP-address association
 - Feeds you fake DNS addresses when you try to access a legitimate website

DNS Cache Poisoning Attack

- Can spread to other networks:
 - If other servers can get their information from a compromised server
 - Serve this information to other hosts

DoS Attack: DNS Spoofing

- The attacker acts as the DNS server in order to redirect the user to malicious sites



DNS Cache poisoning attacks

- DNS cache poisoning attacks

DNS Cache Poisoning Attack

- Occurred in Brazil, 2018
- Attackers installed fake DNS addresses for popular websites
 - Google, Hotmail, etc.
- Victims were sent to a server that the attacker controlled
 - Installed a malicious applet on their system
 - Banking trojan designed to steal banking information

How Hackers Hijacked a Bank's Entire Online Operation



<https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/>

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

IoT Hackers Trick Brazilian Bank Customers into Providing Sensitive Information

August 10, 2018 — by [Pascal Geenens](#) —  85

Radware Threat Research Center has identified a hijacking campaign aimed at Brazilian Bank customers through their IoT devices, attempting to gain their bank credentials.

The research center has been tracking malicious activity targeting DLink DSL modem routers in Brazil since June 8th. Through known old exploits dating from 2015, a malicious agent is attempting to modify the DNS server settings in the routers of Brazilian residents, redirecting all their DNS requests through a malicious DNS server. The malicious DNS server is hijacking requests for the hostname of Banco de Brasil (www.bb.com.br) and redirecting to a **fake, cloned** website hosted on the same malicious DNS server, which has no connection whatsoever to the legitimate Banco de Brasil website.

<https://blog.radware.com/security/2018/08/iot-hackers-trick-brazilian-bank-customers/>

- Questions?

