Oklahoma City
UNIVERSITY

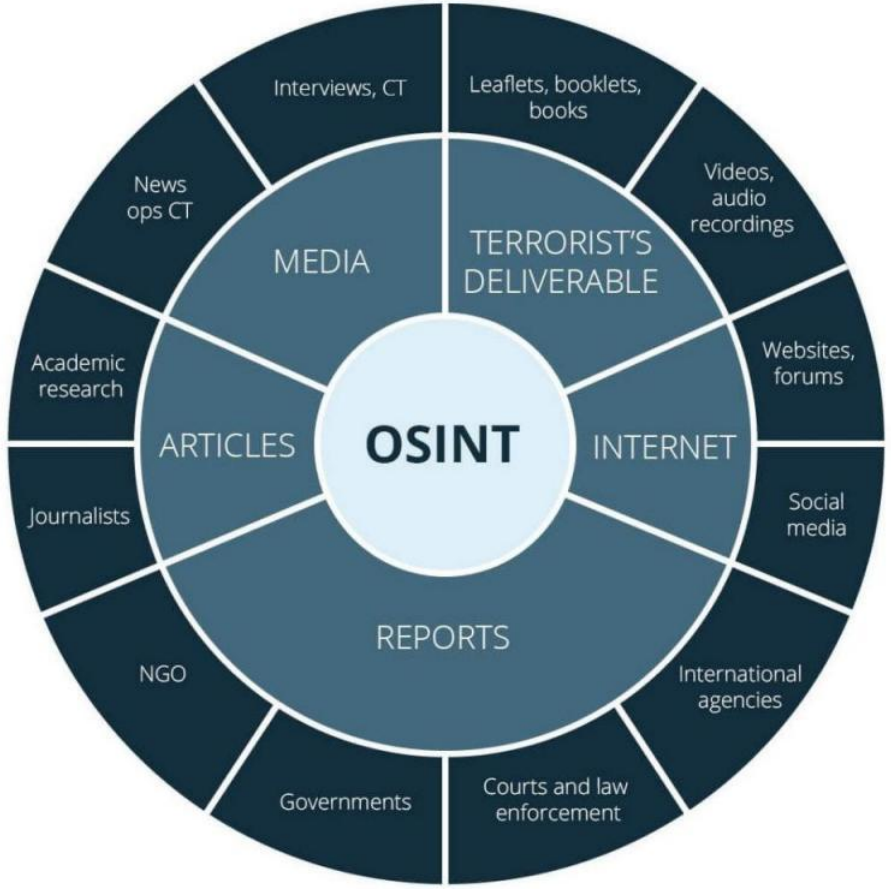
Cybersecurity
CSCI 2413

Mid-Term Review

OSINT (Open-Source Intelligence)

Oklahoma City UNIVERSITY

Open-Source Intelligence (OSINT) – collecting and analyzing **publicly** available information to gather insight and information on a target



OSINT Workflow/Steps

- **Planning and Direction**: Establish clear objectives by defining what information is needed and why.
- **Collection**: Data gathering from public sources, social media, public records…. Manual and automated methods are used to gather the data.
- **Processing and Organization**: Filter the Raw data for only relevant information and remove duplicates this is mainly a manual process.

OSINT Workflow/Steps – cont.

- **Analysis and Correlation**: Identify patterns, relationships, and trends. Corroborate findings with multiple sources to ensure accuracy.
- **Dissemination**: Report the final findings in a structured way (Report, Briefing) to the relevant stakeholders.

OSINT Targets

- Individuals
- Organizations and Businesses
- Critical Infrastructure
- Cybersecurity and Threat Intelligence
- Governments and Nations
- Public Health

Sock Puppet

Sock Puppet is a covert account that is not related to your identity.

This will protect you from revealing your true identity when performing SOCMINT (Social Media Intelligence)

When doing this for an investigation/pentest you want to do this from a Virtual Machine (VM) using a VPN (Virtual Private Network)

We will be setting them up later in the semester.

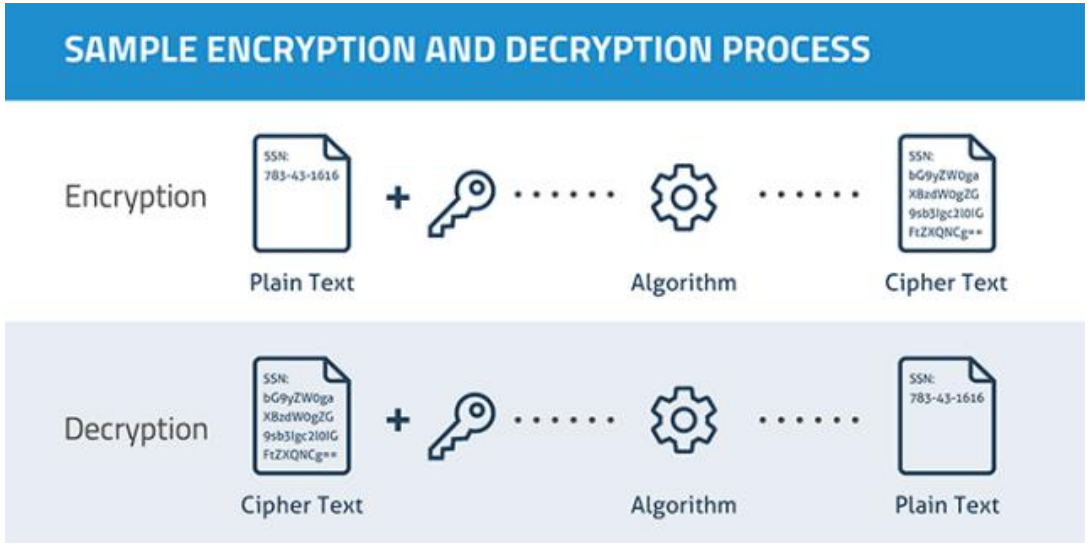
Cryptography Basics

Encryption

- Algorithm scrambles plain text
- Sender and receiver agree on algorithm
- Message difficult to re-create without protocol

Decryption

- Reversal of the scrambling protocol to make the message comprehensible



Cryptography Basics (cont.)

Oklahoma City University

Two basic types

- **Transposition**
  - Rearranging each letter with a different letter
- **Substitution**
  - Replaces each letter with a different letter
  - Two types of substitution
    - Single/symmetric key encryption
      - Stream
      - Block
    - Public/asymmetric key encryption

Transposition Cipher

Oklahoma City UNIVERSITY

Rail Fence

Message: **“Defend the east wall”** with a key of 3

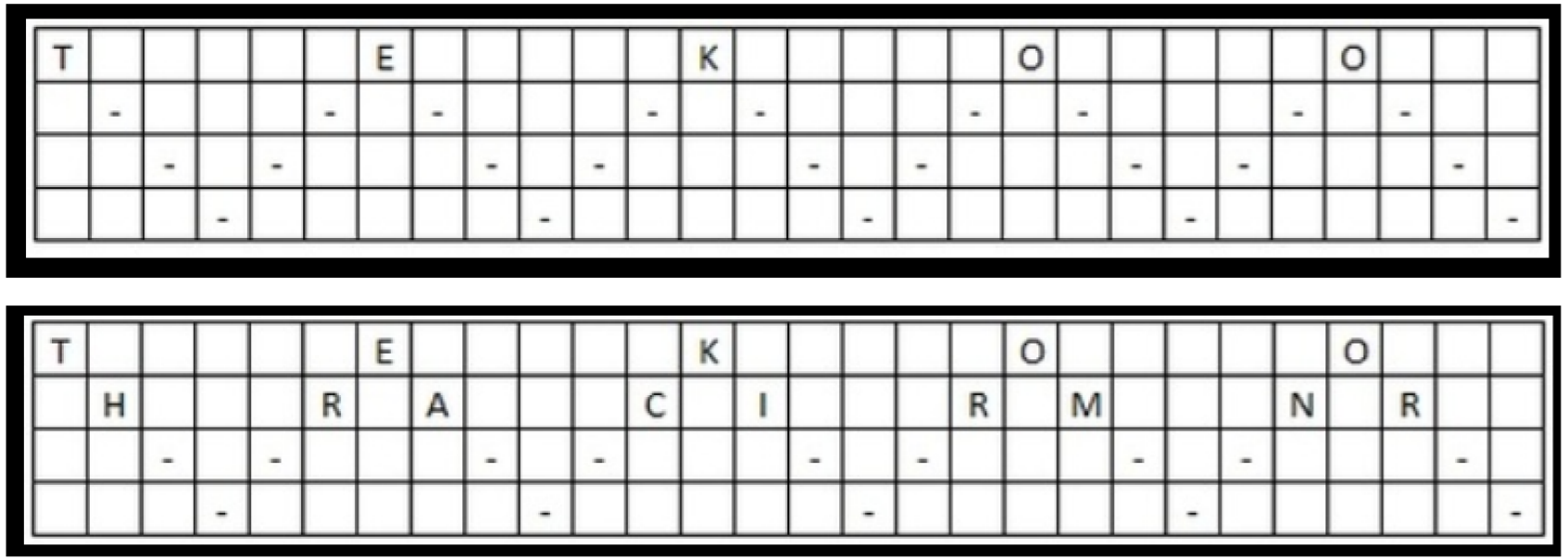
D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

The cipher text is read off row by row to get:
DNETLEEDHESWLXFTAAX

Transposition Cipher

Decrypt:

TEKOOHRACIRMNREATANFTETYTGHH
Encrypted with a key of 4

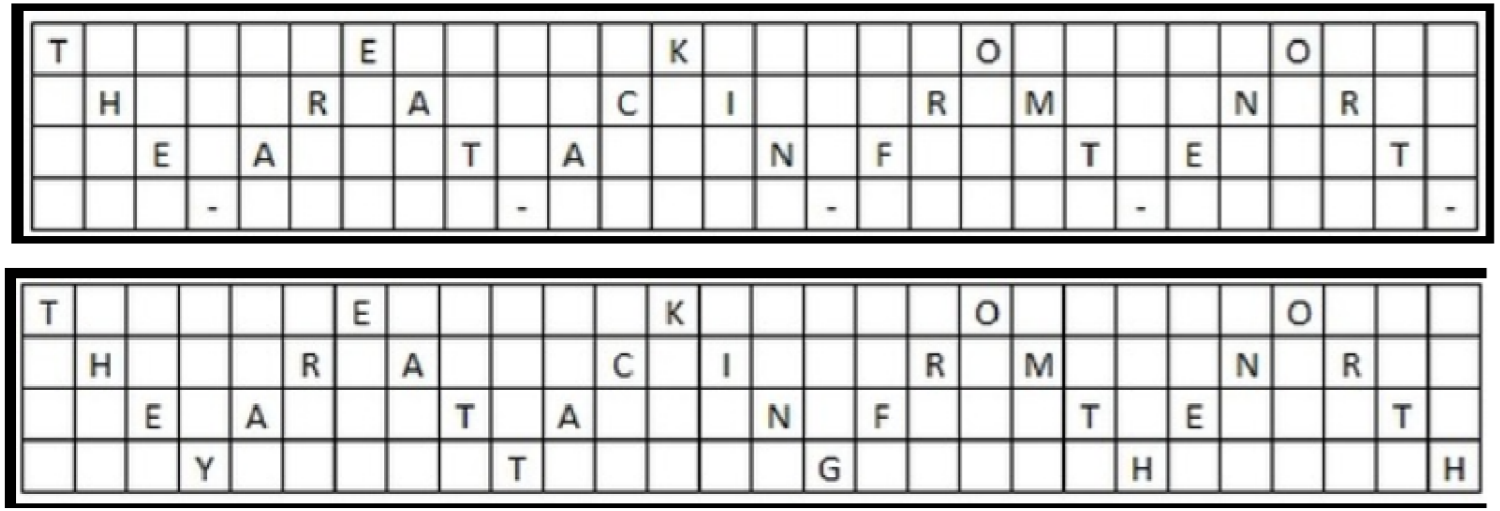


Transposition Cipher

Received:

TEKOOHRACIRMNREATANFTETYTGHH

Encrypted with a key of 4



“They are attacking from the north”

Substitution Ciphers

Old as written communication and war

Caesar Cipher

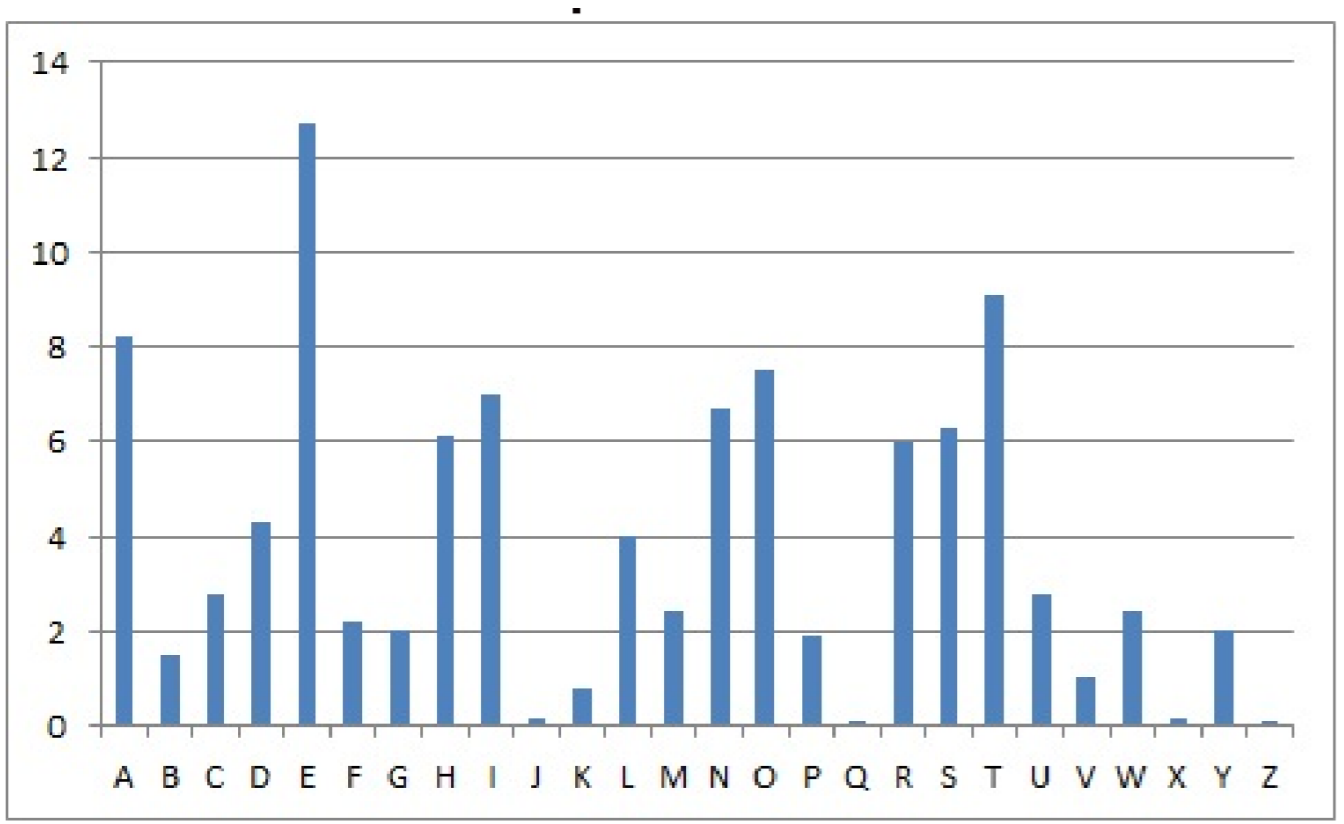
- Shift cipher
- Example Key +2
- Cleartext = HELLO WORLD

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CDEFGHIJKLMNOPQRSTUVWXYZAB

Cipher Text = JGNNQ YQTNF

Substitution Ciphers



Frequency distribution will crack the simple Caesar cipher.

Source: http://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

Vigenere Cipher

- Plaintext:

  ATTACKATDAWN

- Key:

  LEMON

- Keystream:

  LEMONLEMONLE

- Ciphertext:

  LXFOPVEFRNHR

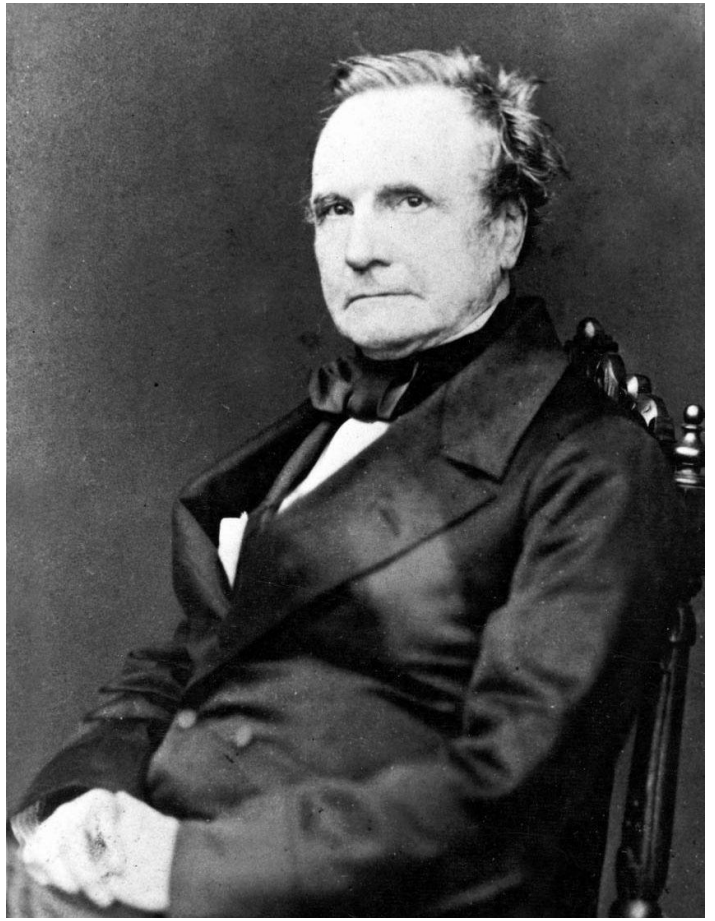
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Charles Babbage

In 1854 Babbage broke Vigenere Cipher

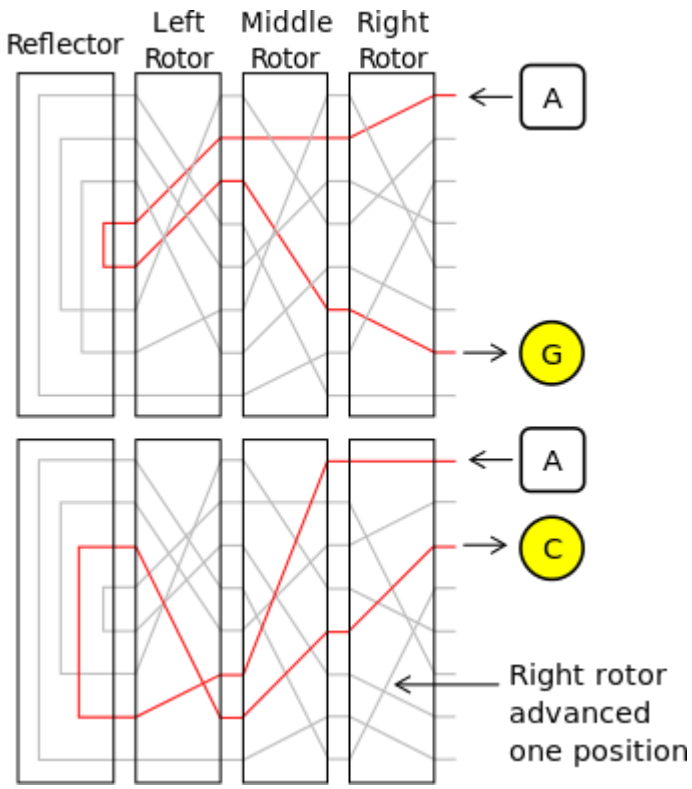
The 1st 100 Most Common English Words

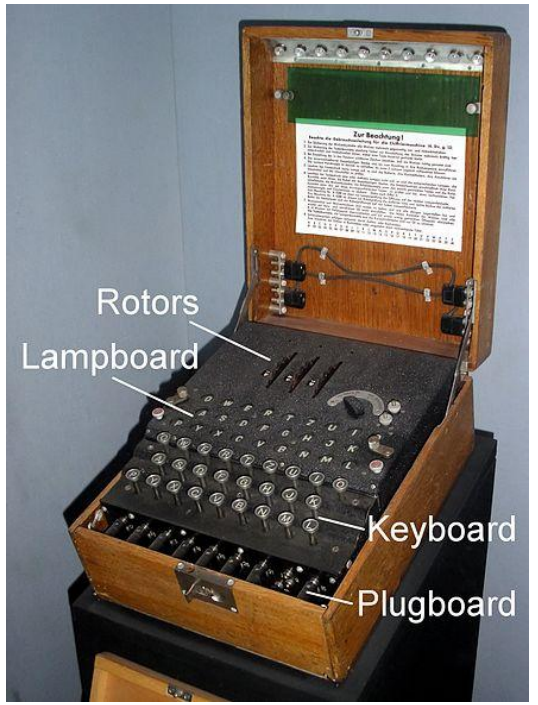
the	or	will	number
of	one	up	no
and	had	other	way
a	by	about	could
to	word	out	people
in	but	many	my
is	not	then	than
you	what	them	first
that	all	these	water
it	were	so	been
he	we	some	call
was	when	her	who
for	your	would	oil
on	can	make	now
are	said	like	find
as	there	him	long
with	use	into	down
his	an	time	day
they	each	has	did
I	which	look	get
at	she	two	come
be	do	more	made
this	how	write	may
have	their	go	part
from	if	see	over



Enigma

Arthur Scherbius – created in 1918



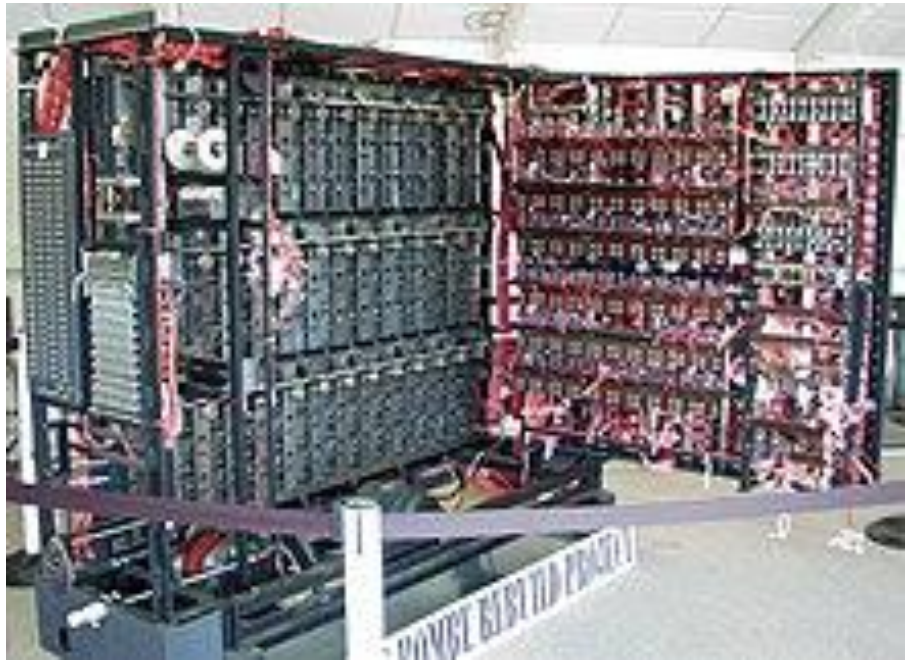


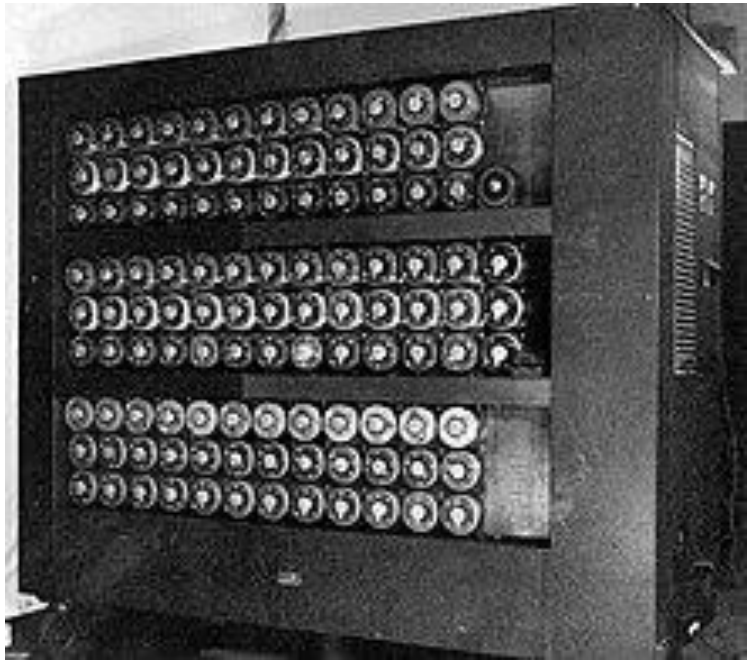
https://www.youtube.com/watch?v=ybkkiGtJmkM

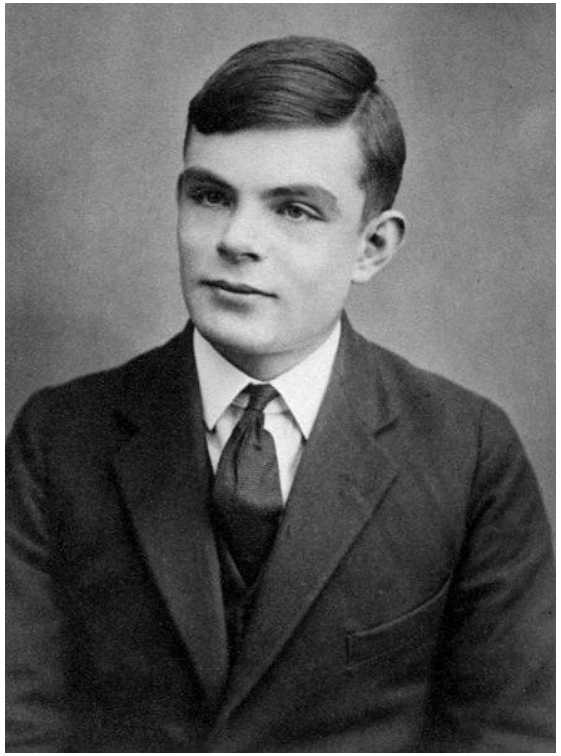
Alan Turing

Created first “Bombe” in 1940s

This helped crack the Enigma codes

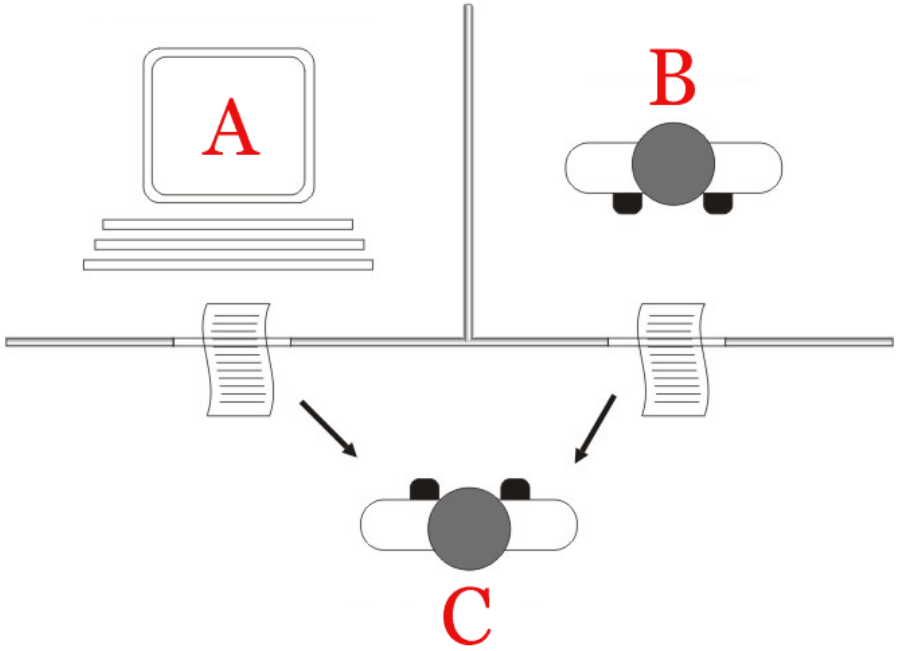


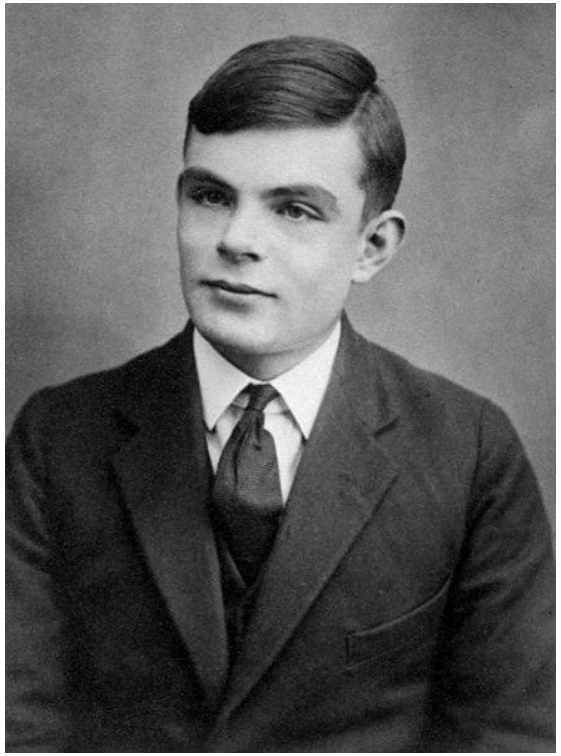




Alan Turing – "Turning Test"

The interviewer asks the same question of a computer and a human to determine if you talking to a computer or human.





Alan Turing – 6 Primitives

Wrote about the 6 basic operations (primitives) to be considered a software language.

- **Right**: Move the Machine's head to the right of the current square

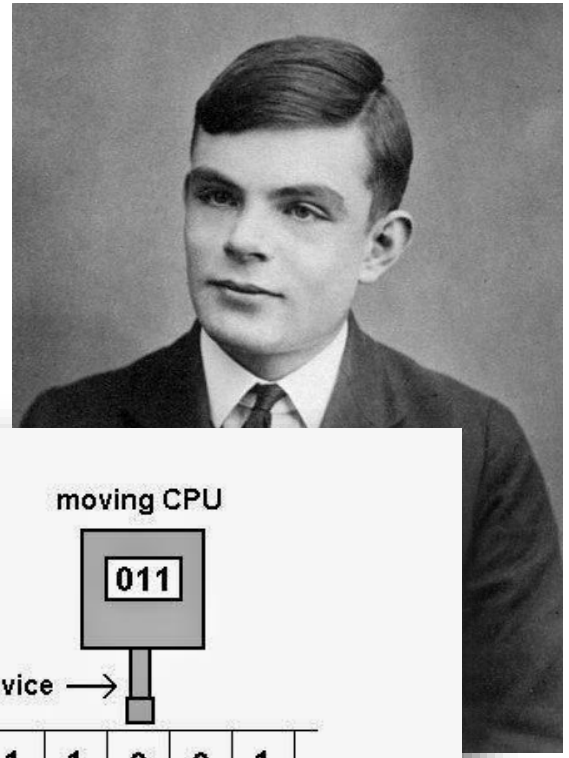
- **Left**: Move the Machine's head to the left of the current square

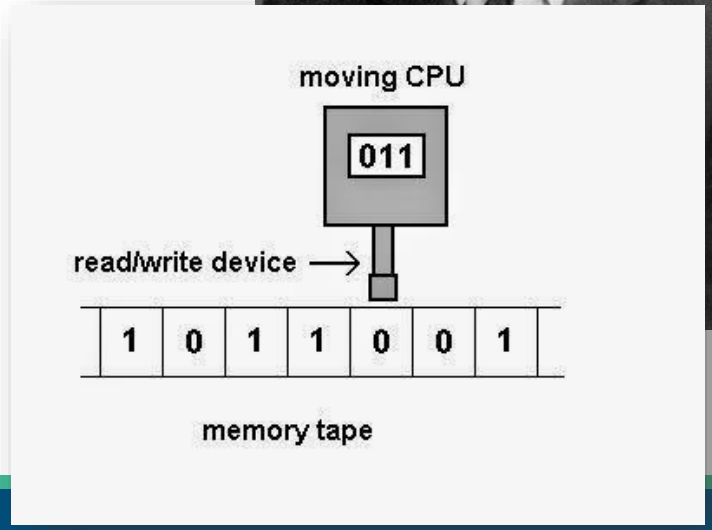
- **Print**: Print a symbol on the current square

- **Scan**: Identify any symbols on the current square

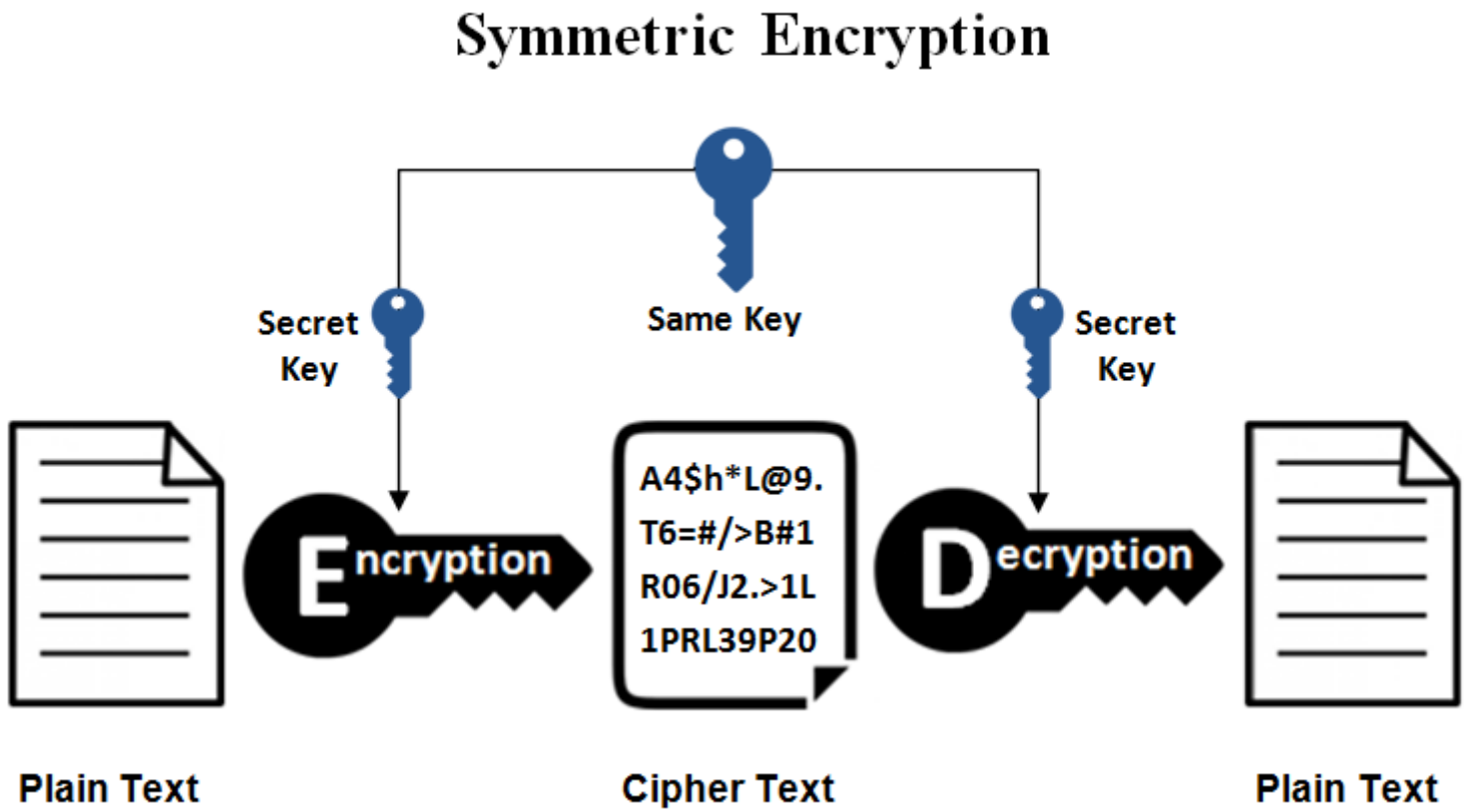
- **Erase**: Erase any symbols presented on the current square

- **Nothing/Halt**: Do nothing





Symmetric Encryption



Diffie Hellman

Martin Hellman

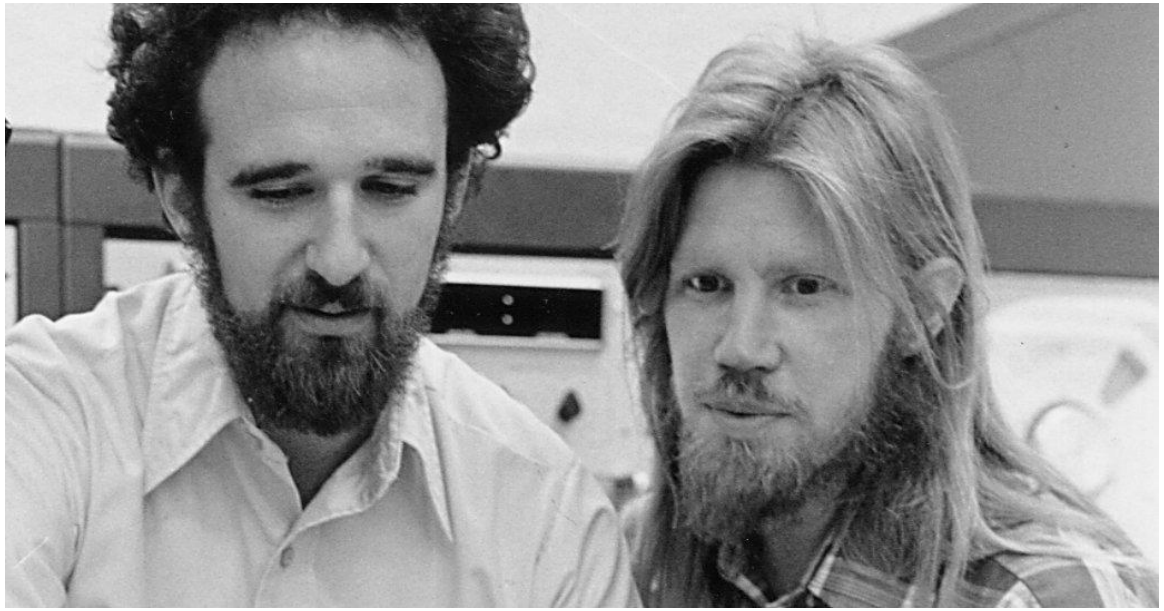
IBM Watson Research Center

1968 - 1969

Whitfield Diffie

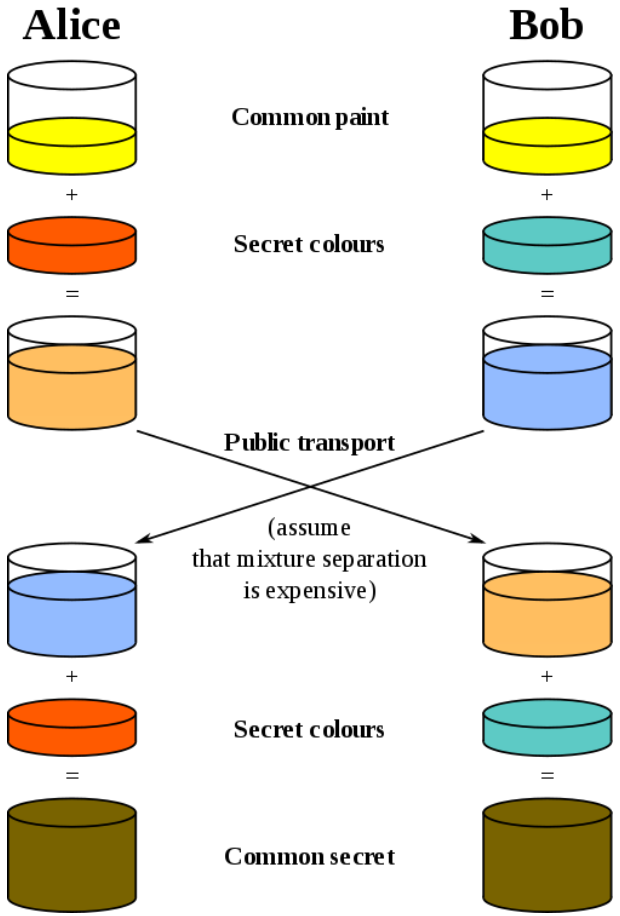
Stanford AI Lab

1974



Diffie Hellman Example (Colors)

Oklahoma City UNIVERSITY

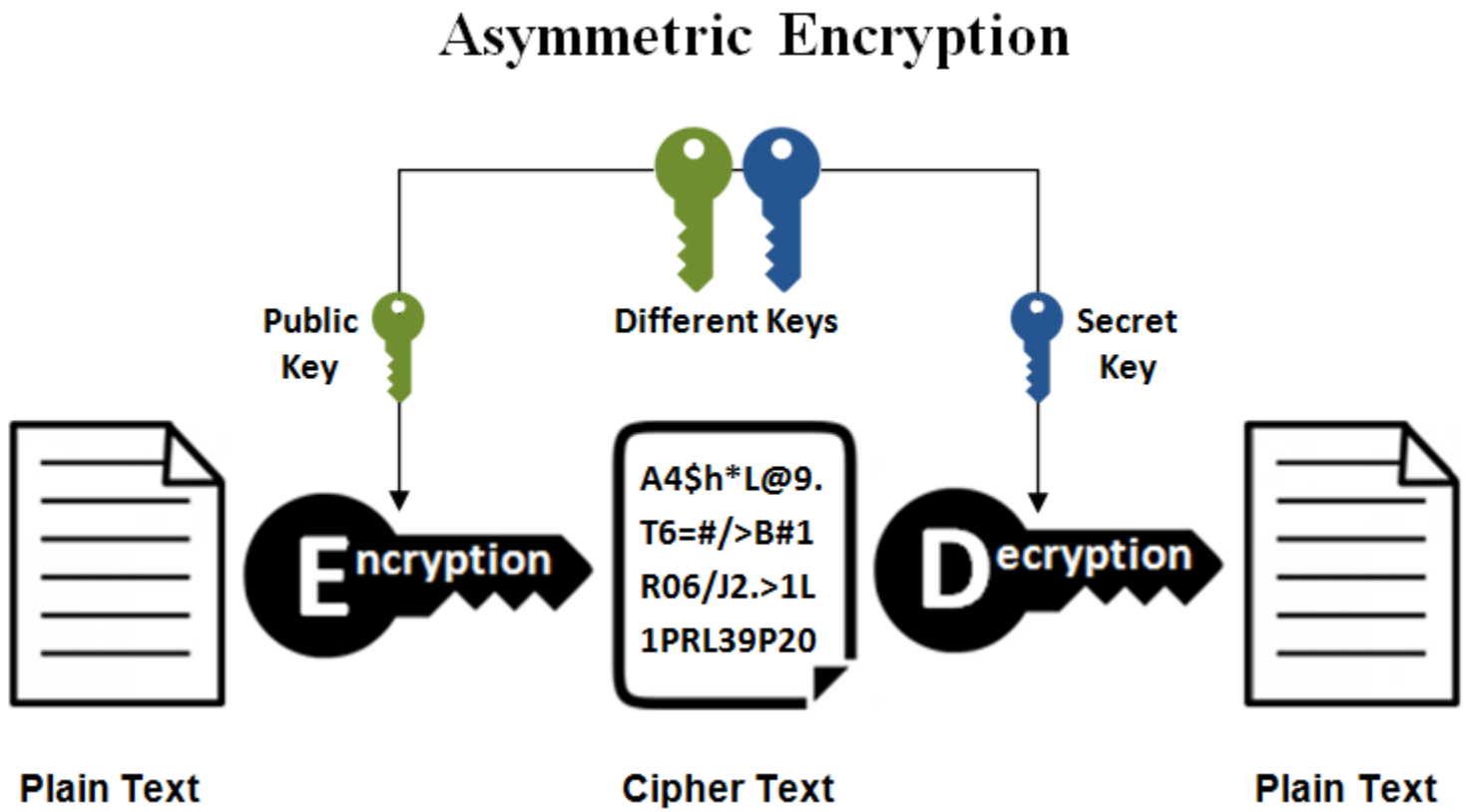


Diffie Hellman Example (Numbers)

Alice		Bob		Eve	
Known	**UN**	**Known**	**UN**	**Known**	**UN**
p=23		p=23		p=23	
g=5		g=5		g=5	
a=6	b	b=15	a		a,b
$A=5^a \bmod 23$		$B = 5^b \bmod 23$			
$A=5^6 \bmod 23 = 8$		$B=5^{15} \bmod 23 = 19$			
B=19		A=8		A=8, B=19	
$S=B^a \bmod 23$		$S=A^b \bmod 23$			
$S=19^6 \bmod 23 = 2$		$S=8^{15} \bmod 23 = 2$			S

Asymmetric Encryption

Oklahoma City University



Certificate Authorities (CA)

Oklahoma City University

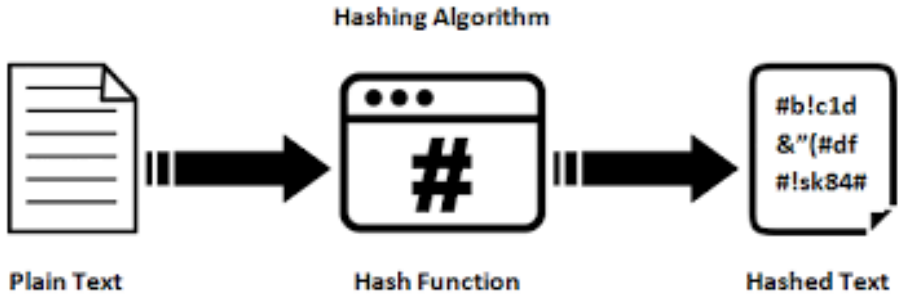
Primary role is to digitally sign and public the public key of a given user

Registration Authority (RA) is often used to handle verification prior to certificates being issued

Public Key Infrastructure (PKI)

- An arrangement that binds public keys with respective user identities by means of a CA
- A network of trusted CA servers

Hashing



Oklahoma City UNIVERSITY

Takes a variable-size input and returns a fixed-size string

The value returned is called the hash value

Hashing is **one-way**; you cannot un-hash something

Hashing is how Windows stores passwords

Salt refers to random bits that are used as one of the inputs to the hash

- Complicates dictionary and rainbow table attacks

Salting

Salting uses a randomly generated string used with the has so each hashed password will be unique even if the passwords are the same.

				
Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Hashing Methods

Secure Hash Algorithm (SHA)

- Most widely used
- SHA-1, SHA-2, SHA-3, SHA-256, SHA-512

MD5

- Not collision resistant

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

Steganography

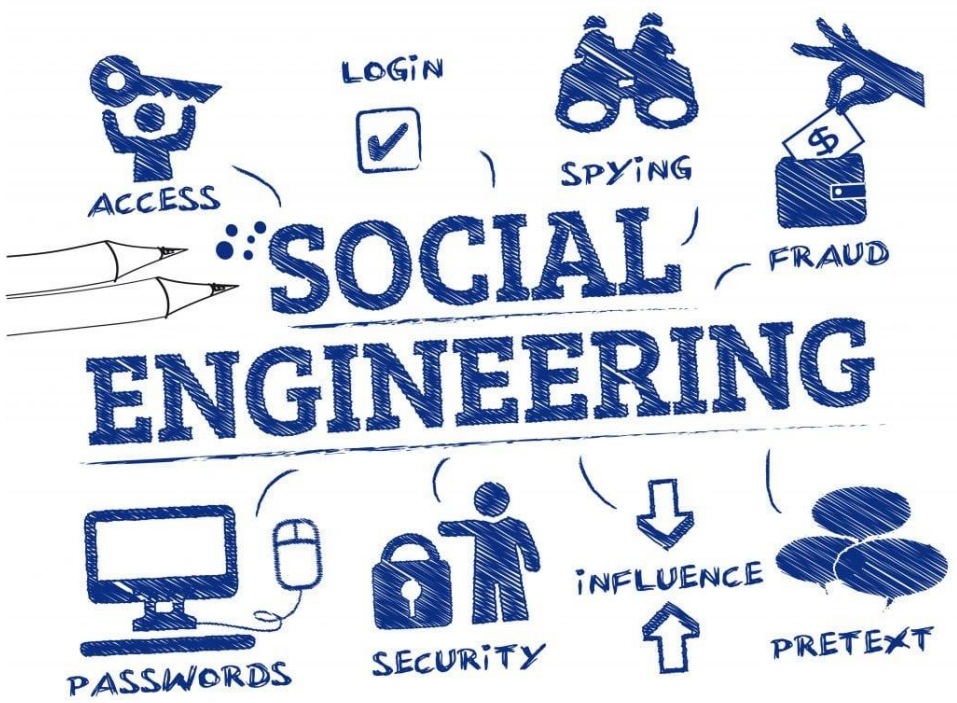
Steganography is the art and science of writing hidden messages in such a way that nobody other than the sender and intended recipient suspects the existence of the message

Message is often hidden in some other file such as a digital picture or audio file

Messages do not attract attention to themselves

Introduction

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.



Attacks - Techniques

Commitment

Authority

Reciprocation

Reverse Engineering

Likening

Scarcity

Commitment

Commitment attacks occur when the attacker tricks the victim into making a promise which he or she will then feel obligated to keep

Victim do not want to be untrustworthy

- Car Deals and Furniture stores use these tactics

Conformity is a special type of commitment leveraging an implied commitment made by society rather than by the individual

- Waiter provides poor service then collects the tip in person

Authority

Authority is the process of an attacker assuming a role of authority which he does not possess.

3 Types

- **Impersonation** – pretending to be some they are not
- **Diffusion of Responsibility** – involves an attacker manipulating the decision-making process from one that is normally individual to one that is collective
- **Reciprocation** – occur when an attacker gives the victim a gift and the victim feels a strong social pressure to return some type of favor.

Reverse Social Engineering

Reverse Social Engineering is an attack where the aggressor tricks the victim into asking him for assistance in solving a problem.

1) **Sabotage** – Attacker creates a problem compelling the victim to action
2) **Advertise** – Attacker advertises his/her willingness and ability to solve the problem
3) **Assist** – Attacker requests assistance from the victim to solve the problem. Typically requesting passwords or access to the users system.

Likening

Likening is the process of an attacker behaving in a way to appear similar to a member of a trusted group.

Political groups

Religious groups

Hobbies

Gain confidence getting to know you and the group

Scarcity

Scarcity attacks occur when the attacker is able to introduce the perception of scarcity of an item that is a high perceived value.

Rushing – involves then attacker putting severe time constraints on a decision

Defenses

The simplest and most effective defense against social engineering attacks is **EDUCATION**.

Training – Repeat Often

Reaction – recognize the attack and moving to more alert state.

Inoculation – making attack resistance a normal part of the work experience.

Physical Security Attacks

Tailgating – seeking entry to a restricted area secured by walking in after someone else has opened the door

Shoulder Surfing – Looking over someone's shoulder to see them type their password or read a confidential document

Leaving Computer Unlocked – Never leave your computer unlocked (**TRUST NO ONE**)

What do the attackers want?

Personally Identifiable Information (PII)

- **Name** – Full Name, maiden name, mother's maiden name
- **Personal identification numbers** – Social Security Number (SSN), Passport Number, Drivers License Number, Taxpayer ID
- **Personal Address** – Street address, city, state, zip
- **Personal Phone #/Email**
- **Personal Characteristics** – Photograph, fingerprints, handwriting
- **Biometric data** – retina scans, voice signatures or facial geometry
- **Financial Data** – Bank accounts, Credit cards, Tax records

Other Shared PII

Date of Birth

Place of Birth

Business Phone, Email, Address

Race

Religion

Employment Information

Medical Information

Education Information

Financial Information

Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, bank account info….

Spear Phishing – directed at specific individuals or companies

Whaling – Targets a specific individual usually a senior executive (Jeff Bezos)

Vishing – Voice call

Smishing – SMS/Text Message

HIPAA

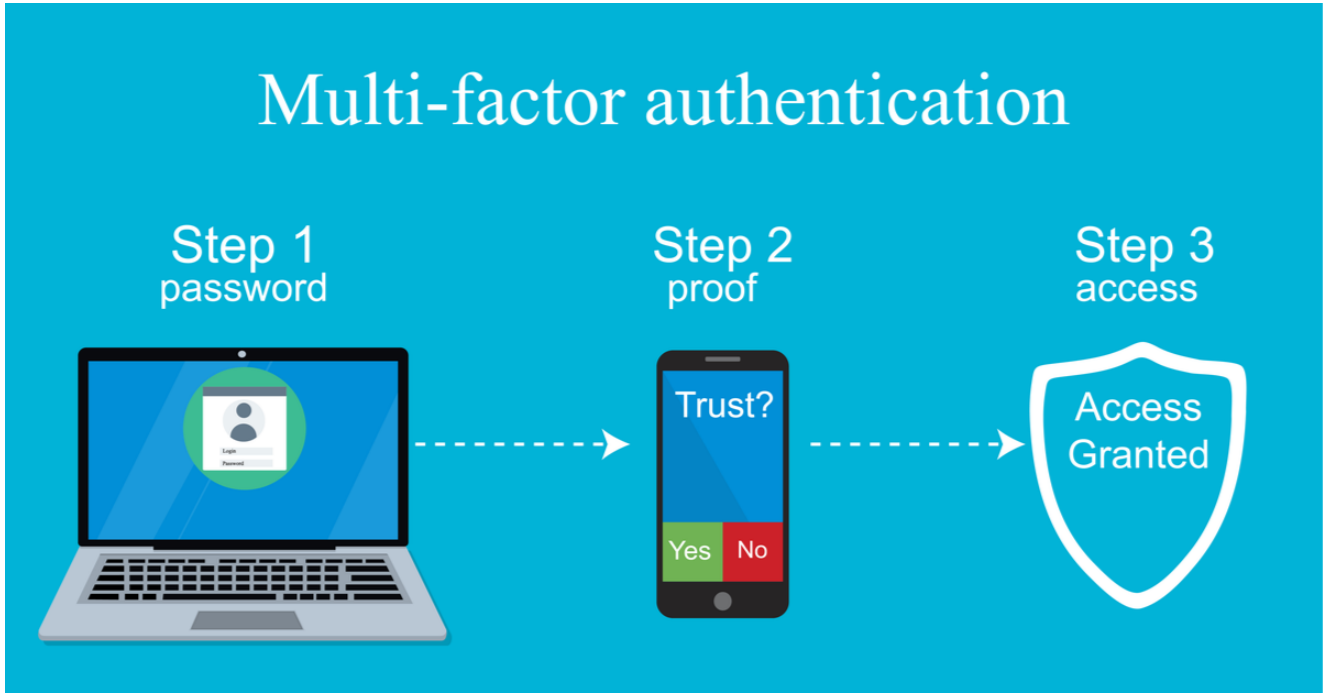
Health Insurance Portability and Accountability Act (HIPAA) of 1996

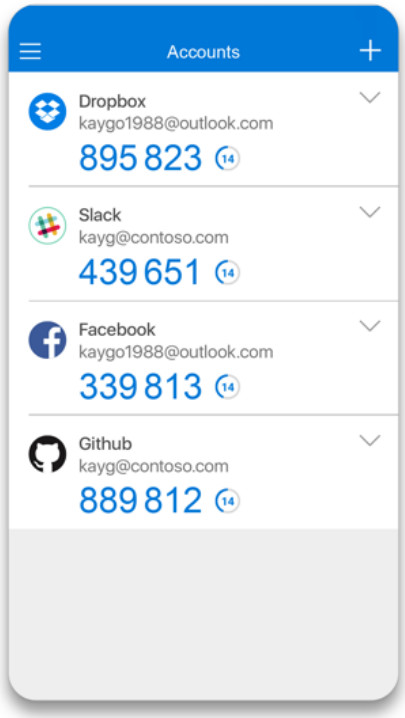
Designed to protect the privacy and security of certain health information.

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Multi-factor Authentication (MFA)

Oklahoma City University





Dictionary Attack

Dictionary Attack is a type of brute-force cyberattack where an attacker uses pre-compiled lists of common passwords, keyboard patterns, common words, and previously leaked credentials to try to break into a user account.

Attack Types

Rule-based attack makes modifications to the words from a dictionary file, replacing common characters like “a” and “@” that follow password patterns

Mask attack is an optimized brute-force that reduces the search by exploiting known information about the passwords format or length.

The Open Systems Interconnect (OSI) Model

Layer	Description	Protocols
Application	This layer interfaces directly to applications and performs common application services for the application processes.	POP, SMTP, DNS, FTP, Telnet
Presentation	The presentation layer relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems.	Telnet, Network Data Representation (NDR), Lightweight Presentation Protocol (LPP)
Session	The session layer provides the mechanism for managing the dialogue between end-user application processes.	NetBIOS
Transport	This layer provides end-to-end communication control.	TCP, UDP
Network	This layer routes the information in the network.	IP, ARP, ICMP
Data link	This layer describes the logical organization of data bits transmitted on a particular medium. The data link layer is divided into two sublayers: the Media Access Control layer (MAC) and the Logical Link Control layer (LLC).	SLIP, PPP
Physical	This layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. In other words, the physical layer is the actual NIC, Ethernet cable, and so forth.	IEEE 1394, DSL, ISDN

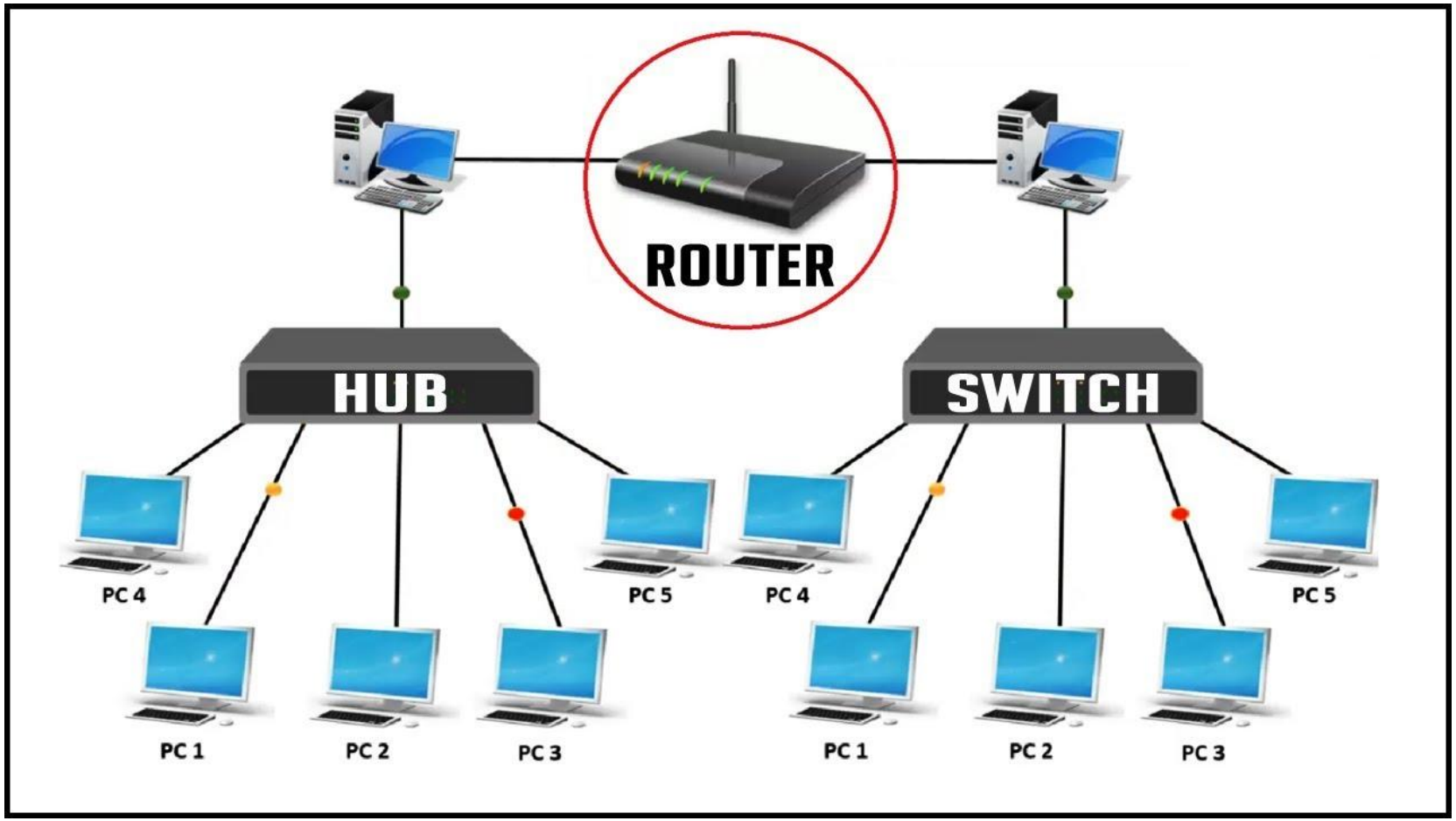
Router, Switch and Hub

Router – forwards data packets along networks. It is connected to at least two networks, commonly two LANs or WANs.

Switch – device that filters and forwards packets between LAN segments. (Data Link Layer)

Hub – connect point for devices in a network connecting segments of a LAN. (Physical Layer)

Router, Switch, and Hub



IP Addresses

IPv4 is a series of four three-digit numbers separated by periods:
107.22.98.129

Each set of digits range between 0 and 255

0.0.0.0 to 255.255.255.255

Certain ranges are private, for use within networks

IPv6 uses a 128-bit address and hex numbering. Example:
3FFE:B000:800:2:C

IP Ranges (First Byte)

- **Class A (0 - 126)** - Extremely large networks (All Class A IPs have been assigned)
- **Class B (128 - 191)** - Large corporate and government networks (All Class B Ips have been assigned)
- **Class C (192 - 223)** – Most common IP ranges (Used by ISP)
- **Class D (224 – 247)** – Reserved for multicasting (transmitting different data on the same channel)
- **Class E (248 – 255)** – Reserved for experimental use

IP Addresses

Private Networks

- 10.0.0.10 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Local Host (localhost)

- 127.0.0.1

Uniform Resource Locators

URLs are text-based web addresses, such as www.okcu.edu that translate into Internet IP addresses 165.227.49.159

Translation is performed by Domain Name Service (DNS) servers

MAC Addresses

MAC addresses are unique hardware addresses

Every NIC in the world has a unique MAC address

Six-byte hexadecimal numbers

Address Resolution Protocol (ARP) converts IP addresses to MAC addresses

Protocols/Ports

Protocol	Port
FTP	20, 21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
LDAP	389
HTTPS	443
RDP	3389

Basic Network Utilities

ipconfig

ping

tracert

netstat

Basic Network Utilities

ipconfig (PC)

Or

ifconfig (Mac/Unix)

```
Command Prompt

C:\Users\Jeff Maxwell>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::eca7:a813:773c:6b87%67
   IPv4 Address. . . . . . . . . . . : 172.26.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cf9:3d00:263f:ec5a%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1073:cf75:9f6c:8075%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.19
```

```
Command Prompt
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::eca7:a813:773c:6b87%67
   IPv4 Address. . . . . . . . . . . : 172.26.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cf9:3d00:263f:ec5a%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1073:cf75:9f6c:8075%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.19
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Basic Network Utilities

ping

```
Command Prompt

C:\Users\Jeff Maxwell>ping google.com

Pinging google.com [142.251.32.174] with 32 bytes of data:
Reply from 142.251.32.174: bytes=32 time=23ms TTL=58
Reply from 142.251.32.174: bytes=32 time=24ms TTL=58
Reply from 142.251.32.174: bytes=32 time=17ms TTL=58
Reply from 142.251.32.174: bytes=32 time=14ms TTL=58

Ping statistics for 142.251.32.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 24ms, Average = 19ms

C:\Users\Jeff Maxwell>
```

Basic Network Utilities

tracert

```
Select Command Prompt

C:\Users\Jeff Maxwell>tracert google.com

Tracing route to google.com [142.251.32.174]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  10.0.0.1
  2     2 ms     2 ms     1 ms  192.168.0.1
  3    10 ms    15 ms    11 ms  10.3.160.1
  4    10 ms     9 ms    10 ms  100.126.0.220
  5    21 ms    13 ms    15 ms  100.126.5.120
  6    43 ms    17 ms    15 ms  dalsbprj02-ae1.0.rd.dl.cox.net [68.1.5.140]
  7    16 ms    26 ms    15 ms  74.125.52.228
  8    17 ms    16 ms    17 ms  209.85.243.95
  9    25 ms    16 ms    21 ms  142.251.60.47
 10    16 ms    15 ms    17 ms  dfw28s30-in-f14.1e100.net [142.251.32.174]

Trace complete.

C:\Users\Jeff Maxwell>
```

Basic Network Utilities

netstat

```
Select Command Prompt

C:\Users\Jeff Maxwell>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.0.19:1024         162.159.133.234:https  ESTABLISHED
  TCP    10.0.0.19:1033         52.114.132.127:https   ESTABLISHED
  TCP    10.0.0.19:1061         52.114.128.204:https   ESTABLISHED
  TCP    10.0.0.19:1067         ec2-52-86-118-144:8884  ESTABLISHED
  TCP    10.0.0.19:2165         52.109.20.39:https     ESTABLISHED
  TCP    10.0.0.19:2294         40.83.240.146:https    ESTABLISHED
  TCP    10.0.0.19:2296         40.83.240.146:https    ESTABLISHED
  TCP    10.0.0.19:2297         40.83.240.146:https    ESTABLISHED
  TCP    10.0.0.19:2300         ne-in-f109:imaps       ESTABLISHED
  TCP    10.0.0.19:2318         209.54.180.48:https    ESTABLISHED
  TCP    10.0.0.19:2319         209.54.180.48:https    ESTABLISHED
  TCP    10.0.0.19:2401         52.111.239.4:https     ESTABLISHED
  TCP    10.0.0.19:2477         52.111.239.17:https    ESTABLISHED
  TCP    10.0.0.19:2523         209.87.209.216:https   ESTABLISHED
  TCP    10.0.0.19:2567         40.97.212.18:https     ESTABLISHED
  TCP    10.0.0.19:2568         40.97.212.18:https     ESTABLISHED
  TCP    10.0.0.19:2570         40.97.212.18:https     ESTABLISHED
  TCP    10.0.0.19:2587         40.97.212.18:https     ESTABLISHED
  TCP    10.0.0.19:2593         40.97.212.18:https     ESTABLISHED
  TCP    10.0.0.19:2600         13.107.136.9:https     ESTABLISHED
  TCP    10.0.0.19:2621         ec2-44-197-9-56:https  CLOSE_WAIT
  TCP    10.0.0.19:2630         20.69.137.228:https    TIME_WAIT
^C
C:\Users\Jeff Maxwell>
```

UDP vs. TCP

Oklahoma City University

UDP – User Datagram Protocol

- Connection-less
- Packets are sent in chucks
- faster

TCP – Transmission Control Protocol

- Establishes a connection
- Bidirectional communication
- More reliable

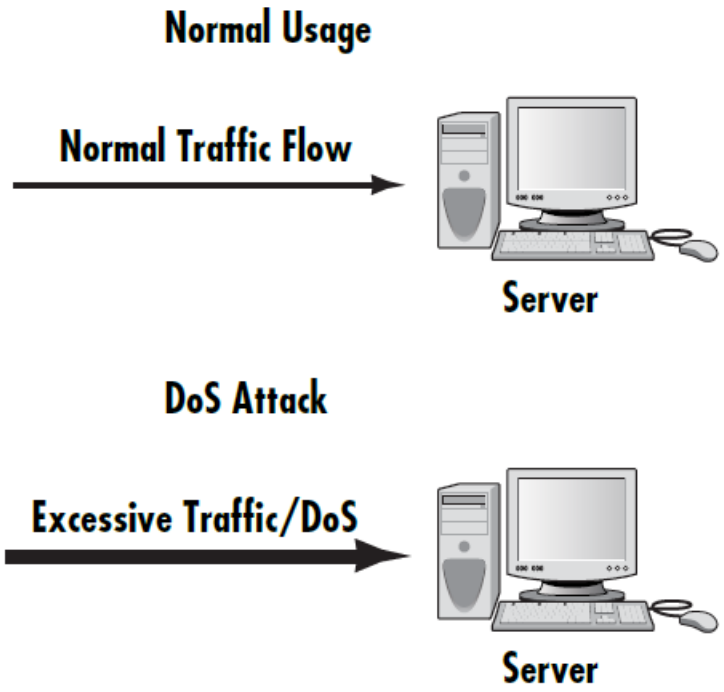
Denial of Service Attack

Oklahoma City University

Based on the premise that all computers have operational limitations

Utilizes the ping utility to execute the attack

You can use the /h or /? Switch with ping to find out what options are available



Example:

ping [target] -1 65000 –w 0 -t

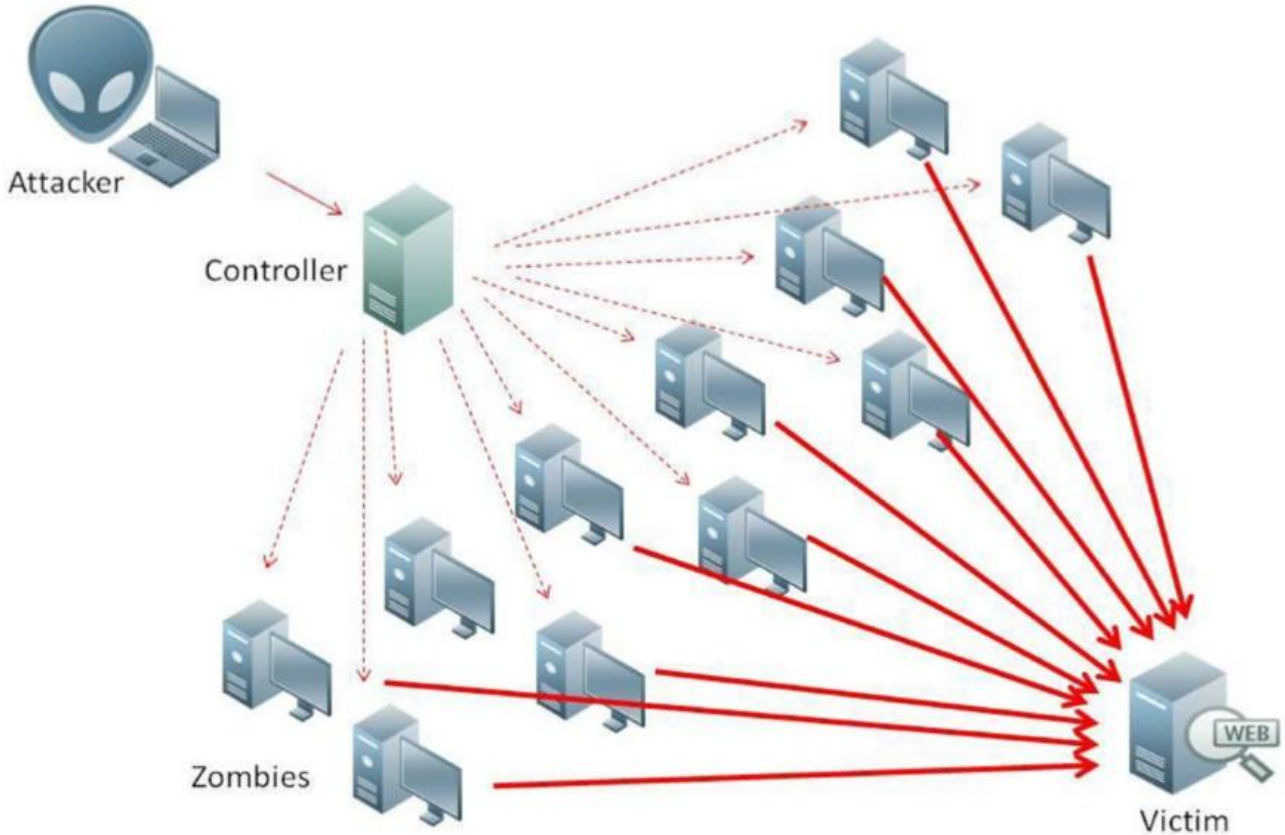
Oklahoma City UNIVERSITY

Distributed Denial of Service (DDoS) Attack

Variation of a Denial of Service

Launched from multiple clients

More difficult to track due to the use of zombie machines



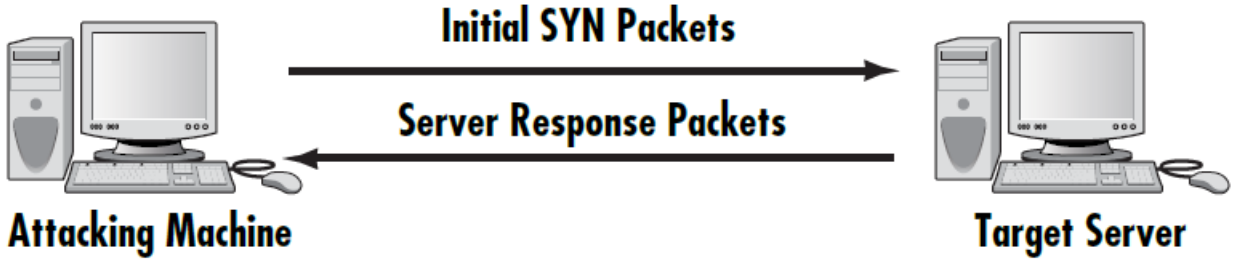
SYN Flood

Oklahoma City University

Takes advantage of the TCP handshake process

Can be addressed in the following manners:

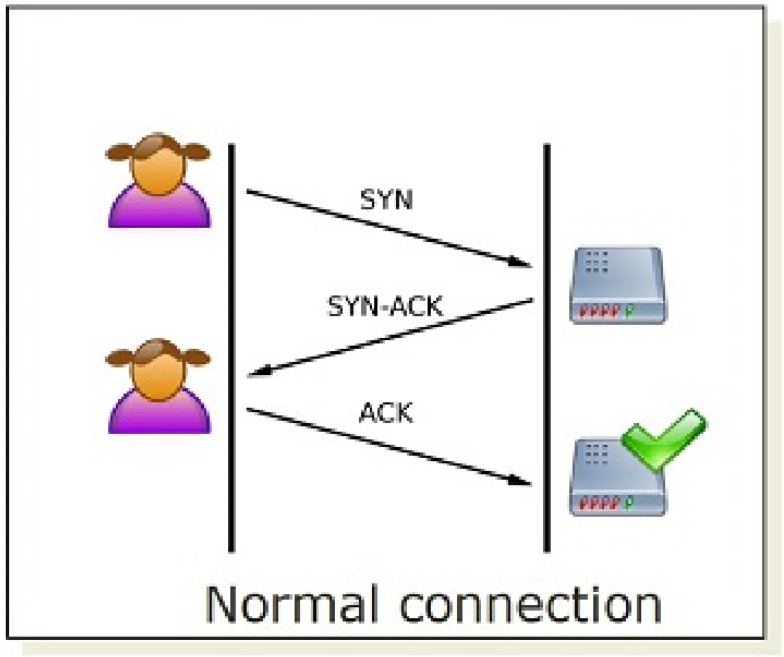
- Micro Blocks
- Bandwidth Throttling
- SYN Cookies
- RST Cookies
- Stack Tweaking

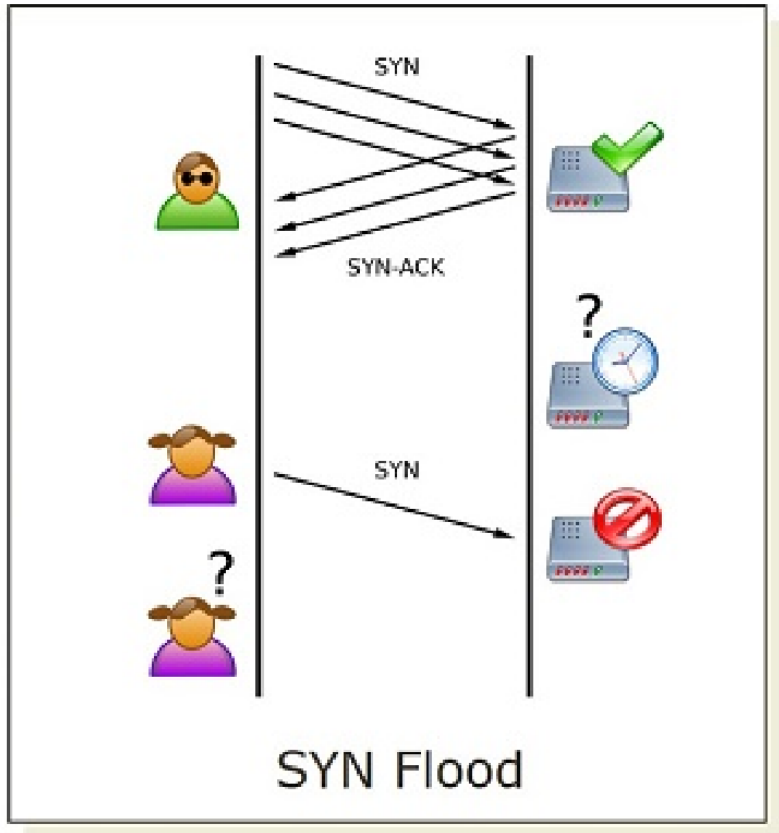


SYN Flood

Oklahoma City UNIVERSITY

Takes advantage of the TCP handshake process



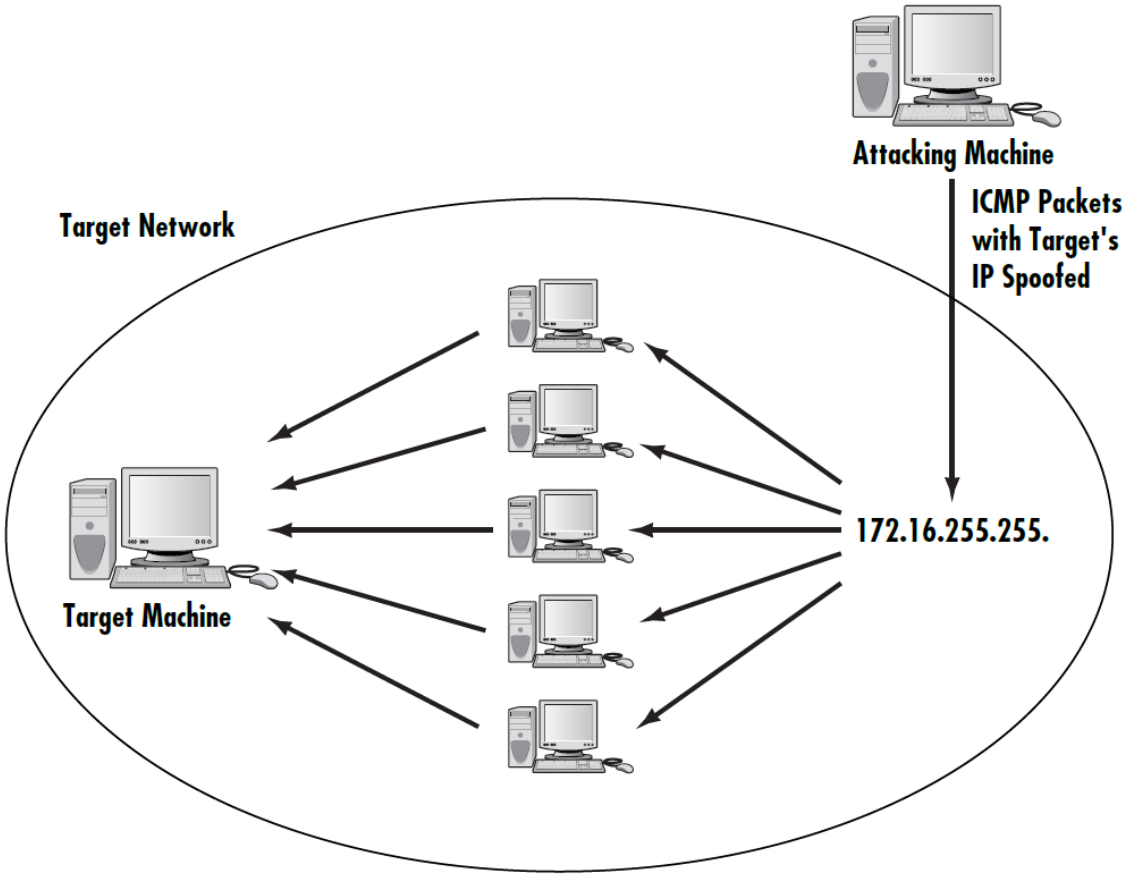


Smurf Attack

Oklahoma City UNIVERSITY

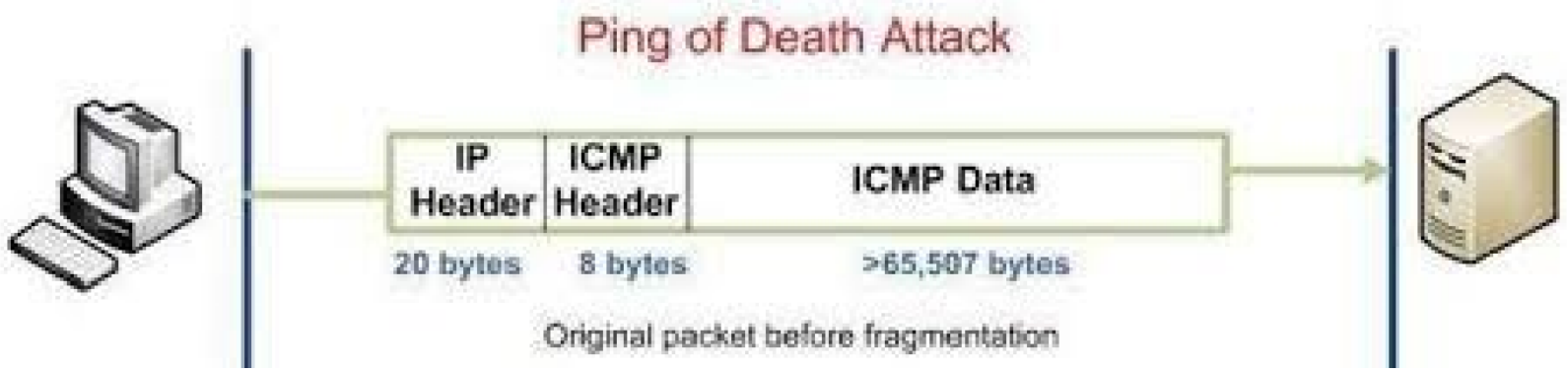
Very popular attack

Utilizes the ICMP packet to execute the attack



Ping of Death (PoD)

Attacks machines that cannot handle oversized packets (> 65,535 bytes)



Ensure that systems are patched and up to date

Most current operating systems automatically drop oversized packets

UDP Flood and ICMP Flood

UDP Flood

- Variation to the PoD that targets open ports
- Faster due to no acknowledgments required
- Sends packets to random ports
- If enough are sent, the target computer shuts down

ICMP Flood

- Another name for the ping flood

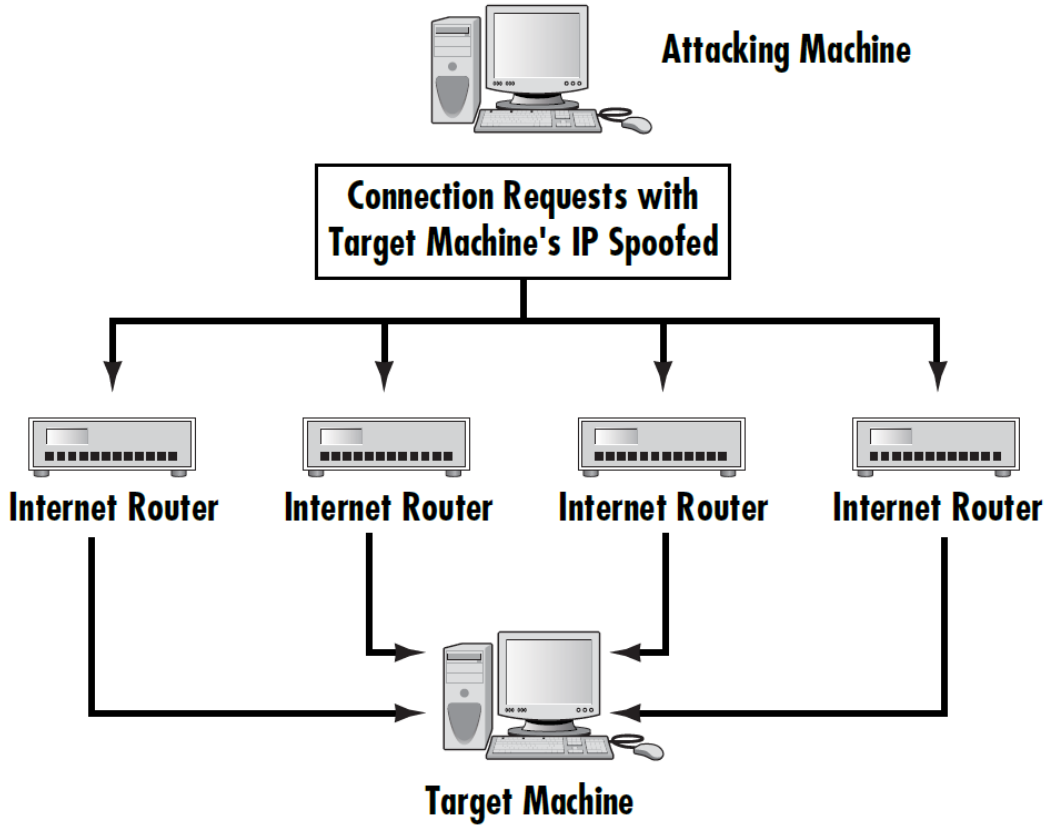
Distributed Reflection DoS (DRDoS)

Uses routers to execute the DoS attack

Routers do not have to be compromised in order to execute the attack

Configure routers to not forward broadcast packets

Distributed Reflection DoS (DRDoS)

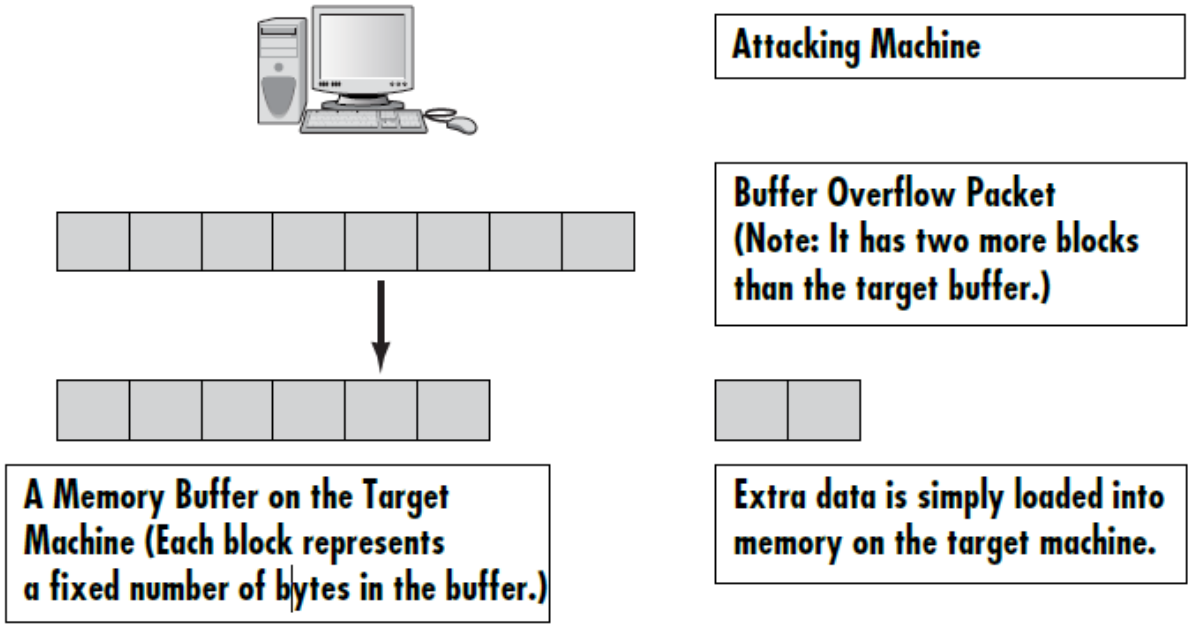


Defending Against Buffer Overflow Attacks

Oklahoma City UNIVERSITY

How do buffer overflow attacks occur?

What do script viruses have to do with buffer overflows?



Oklahoma City UNIVERSITY

Viruses, Logic Bombs, Backdoors

Virus – malware that replicates when executed

Logic Bomb – a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out

Backdoor – covert method of bypassing normal authentication or encryption

Virus vs. Worm

Viruses and Worms both do malicious things

Viruses require human interaction to spread

Worms can spread without human interaction

Trojan Horse Attacks

Program that looks benign but has malicious intent

They might:

- Download harmful software
- Install a key logger or other spyware
- Delete files
- Open a backdoor for hacker to use

How Do Viruses Spread?

Reads your e-mail address book and e-mails itself to everyone in it

Usually attaches itself to the victim's existing e-mail software

Some viruses have their own e-mail engines

How Do Worms Spread?

Scans your computer for connections to a network

Copies itself to other machines in the network to which you have write access

Ransomware

A virus or other malware payload

Locks down the user's files until they pay a ransom

WannaCry ransomware started in health care systems in the UK in 2017

Unpatched systems are most vulnerable

Trojan Horses

Typical actions Trojan horses take:

- Delete files from a computer
- Spread other malware
- Use the computer to launch a DDoS
- Search for personal information
- Install “back door” to the computer

Symptoms of a Trojan Horse

Home page for your browser changes

Any change to passwords, usernames, accounts, and so on

Any change to screen savers

Changes to mouse settings, backgrounds, and such

Any device seeming to work on its own, such as a CD door

What Ports are OPEN?

Windows

netstat –an

Mac

netstat –pant | grep ESTABLISHED

Unix/Bash

netstat –an | grep LISTEN

Single Loss Expectancy (SLE)

Oklahoma City University

Calculates the impact a single loss will cause:

- Asset value (AV)
- Exposure value (EF)
- Exposure factor is a percentage of the asset's value that will be lost
- SLE = AV x EF
- $800 laptop, one year old, depreciation of 10% a year, 800 (AV) x 0.9 (EF) = $720

Annualized Loss Expectancy (ALE)

Oklahoma City University

How much loss you can expect from a particular issue in a year

ARO = annual rate of occurrence

ALE = SLE x ARO

Example: if you estimate you will lose 6 laptops a year:

- 720 (SLE) x 6 (ARO) = $4320

Evaluating the Security Risk

Oklahoma City University

How do you calculate Risk?

- Attractiveness to attackers
- Nature of information
- Level of security

Each system receives a 1 to 10 score for each category

Evaluating the Security Risk

Attractiveness (A) to hackers

Information (I) content

Security (S)

Formula: (A + I) – S = Rating (R)

The lower the rating, the more secure the system

Evaluating the Security Risk

Oklahoma City UNIVERSITY

TABLE 12-1 Value of Data

Value Assigned Description	Impact	Description
1	Negligible, at most some personal embarrassment	Non-sensitive data: video rental records, book sales records
2–3	Slight loss of competitive advantage	Low-level business data: basic process and procedure documents, customer contact lists, employee lists
4–5	Significant loss of competitive advantage (business or military)	More sensitive business data: business strategies, business research data, basic military logistical data
6–7	Significant financial loss, significant loss of reputation, possible negative impact on operations	Financial/personal data: Social Security numbers, credit card numbers, bank account numbers, detailed military logistical data, military personnel records, confidential health records
8–9	Significant business profit loss, significant negative military/ operational impact	Sensitive research data/patent product data, classified military information
10	Serious loss of life, danger to national security	Top secret data, weapons specifications, troop locations, lists of agent identities

Evaluating the Security Risk

Oklahoma City UNIVERSITY

TABLE 12-2 Security Measures Taken

Value Assigned	Security Measure Taken	Typical Implementer*
1	No security at all	Many home users
2	Basic antivirus software	Many home users
3	Antivirus, some security browser settings, basic filtering firewall	Small office/home office users (SOHO)
4	Level 3 plus routine patches and perhaps some additional security measures such as stronger browser security and anti-spyware	Small business/schools
5	Level 4 plus router hardening, strong password requirements, perhaps an IDS, basic policies about downloading, acceptable usage policies, sensitive servers hardened	Networks with a full-time network administrator
6–7	Level 5 with both IDS and anti-spyware, all unnecessary ports closed, subnets filtered, strong password policies, good physical security, encryption used for sensitive data, all servers hardened, back-up media destroyed appropriately, stateful packet inspection firewall on perimeter, web servers located in a DMZ, packet filtering on all subnet routers, very extensive policies on all aspects of computer security	Networks with a larger IT staff, possibly a full-time security professional
8–9	Level 6–7 with regular internal and external security audits, hard drive encryption (such as Windows EFS), possible use of biometrics in physical security (fingerprint scan), extensive logging, background checks on all IT personnel, all workstations/servers completely hardened, all personnel wear security ID badges, all data transmissions encrypted	Networks with a full-time security professional
10	Level 8–9 plus security clearance for all IT personnel, monthly updates/patching/auditing, routine penetration testing, Internet usage extremely restricted or blocked altogether, no portable media (optical disks, USB, etc.) on workstations, strong physical security including armed guards	Military/research installations

The Six P's of Assessment

(1) Patches

(2) Ports

(3) Protect

(4) Physical

(5) Probe

(6) Policies

(1) Patches

Patch policy

- Must be written and followed

Applying patches

- Must check all applications that require patches
- Should be first on list of assessing the system

(1) Patches

Automated patch systems

- Windows Update
- HFNetChkPro
- ZenWorks Patch Management
- McAfee ePolicy Orchestrator

(2) Ports

Common virus attacks come through specific ports

Close all unused ports to reduce vulnerability to specific virus attacks

(3) Protect

When assessing the protection of the network, ensure that the following are in place and functioning:

- Firewall
- Antivirus protection
- Antispyware
- IDS
- Proxy server or NAT
- Data transmission encryption

(4) Physical

Control access to:

- Server rooms
- Workstations
- Miscellaneous equipment
- Data backup media

Make sure physical equipment inventories are kept up-to-date

(4) Physical

Additional Physical Security Strategies

- Biometric locks
- All visitors to the building are logged in and escorted by an employee at all times
- All bags are inspected
- No portable devices that might record data are allowed on the premises
- All printing is logged
- All copying is logged similarly to printing

(5) Probing the Network

Port scanning

- Scan well-known ports to see which are open

Enumerating

- Try to determine what is on the target network (accounts, shares, printers)

Vulnerability assessment

- Use of a tool to seek out known vulnerabilities or manually assess vulnerabilities

Vulnerability Lists

Common Vulnerabilities and Exposures (CVE)

- Maintained by the Mitre Corporation

National Institute of Standards and Technology

- Uses the CVE format

Open Web Application Security Project (OWASP)

- The standard for web application security
- They publish a number of important documents, including a Top 10 List

(6) Policies - McCumber Cube

Oklahoma City University

Goals:

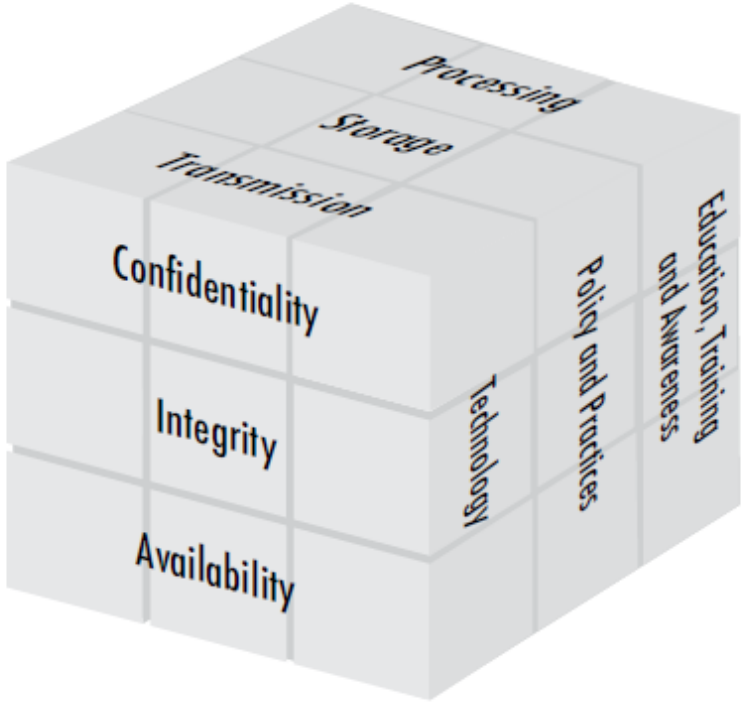
- Confidentiality, Integrity, Availability

Information States:

- Storage, Transmission, Processing

Safeguards:

- Policy and Practices, Human Factors, Technology



(6) Policies - Security Documentation

Physical security documentation

Policy and personnel documentation

Probe documents

Network protection documents

(6) Policies - Physical Security Documentation

Oklahoma City University

List physical security that is in place

Document location of every device

If device is in a locked room, a list of who has keys should be kept

If entry logs are kept, copies should be kept with physical documentation

(6) Policy and Personnel Documentation

Oklahoma City UNIVERSITY

All policies must be filed

Revisions must be documented and kept

Signed copies of agreements on awareness

List of personnel with their access rights

(6) Policies - Probe Documents

Internal audit results should be filed every time

External audit results should also be kept

Follow-up reports if flaws are found

If a security incident occurs, document what happened and how it was corrected

(6) Policies - Network Protection Documents

Oklahoma City University

These documents should detail the following:

- What firewall is used and how it is configured
- What IDS is in use and how it is configured
- What antivirus/antispyware is used
- Are honeypots in use
- Are individual machine security measures in use and what are they

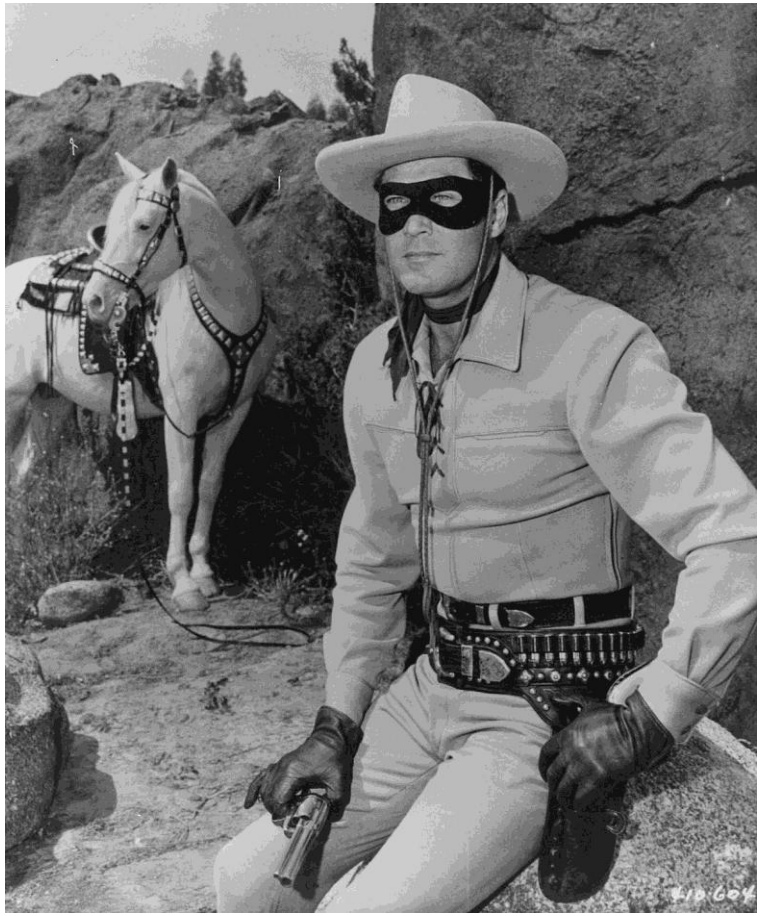
Oklahoma City UNIVERSITY

Types of Hackers

A ***white hat hacker*** is usually called a penetration tester today; It is someone who is hacking with permission of the owners of the target system

A ***black hat hacker*** is the person who gains access to a system in order to cause some type of harm; Black hat hackers are sometimes referred to as ***crackers***

A ***gray hat hacker*** is normally a law-abiding citizen, but in some cases will venture into illegal activities



Penetration Testing (PenTester)

Also know as Ethical Hacker is some one that is **AUTHORIZED** to simulate a cyber attack against a computer or server.

Pen Testers are usually a company or security firm that performs several attacks on a company and provides a report to the company of any vulnerabilities found and how to fix any issues found.

Evil Twin

Evil Twin is a fraudulent Wi-Fi access point that appears to be legitimate but is setup to eavesdrop on wireless communications.

The evil twin is the wireless LAN equivalent of a phishing scam