Network Security Workshop

APNIC48 - Chiang Mai, Thailand
5-9 September 2019

Outline

- Security Overview
- Security in Layers
- Crypto Basics

SECURITY OVERVIEW

Why Security?

- The Internet was initially designed for connectivity
  - Trust assumed
  - Security protocols are added on top of the TCP/IP
- The Internet has become fundamental to our activities (business, work, personal)
- Certain aspects of information must be protected
  - Confidential data
  - Employee information
  - Business models
  - Protect identity and resources

Internet Evolution

LAN connectivity

Application-specific
More online content

Application/data
hosted in the “cloud”

Different ways to handle security as the Internet evolves

Threat Landscape

Figure 1 Security Professionals’ Biggest Sources of Concern Related to Cyber Attacks

Mobile Devices	Data in Public Cloud	Cloud Infrastructure	User Behavior (For Example, Clicking Malicious Links in Email or Websites)
58%	57%	57%	57%

Percentage of Security Professionals Who Find the Categories Very or Extremely Challenging

Source: Cisco 2017 Security Capabilities Benchmark Study

Incident: Mirai Botnet

- **Mirai botnet (Sep/Oct 2016)**
- Exploited IoT devices and CCTV cameras (“IoT botnet”)
- Scanned the Internet for open Telnet ports, then attempted login with default password
- Affected:
  - OVH with 799Gbps using 145,607 hacked IP cameras
  - Akamai / Krebs on Security with 665Gbps traffic
  - Dyn with almost 1Tbps traffic from 100k malicious endpoints

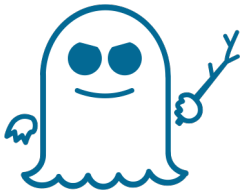
Incident: Ransomware

- **WannaCry Ransomware (May 2017)**
  - As of 12 May, 45K attacks across 74 countries
  - Remote code execution in SMBv1 using EternalBlue exploit
    - TCP 445, or via NetBIOS (UDP/TCP 135-139)
  - Patch released on 14 March 2017 (MS17-010), exploit released on 14 April 2017

Incident: Meltdown / Spectre

- **Meltdown/Spectre (Jan 2018)**
- Exploits processor vulnerabilities!
  - Intel, AMD, ARM

- Meltdown (CVE-2017-5754):
  - Breaks the isolation between programs & OS
  - An application could read kernel memory locations
  - "If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information"

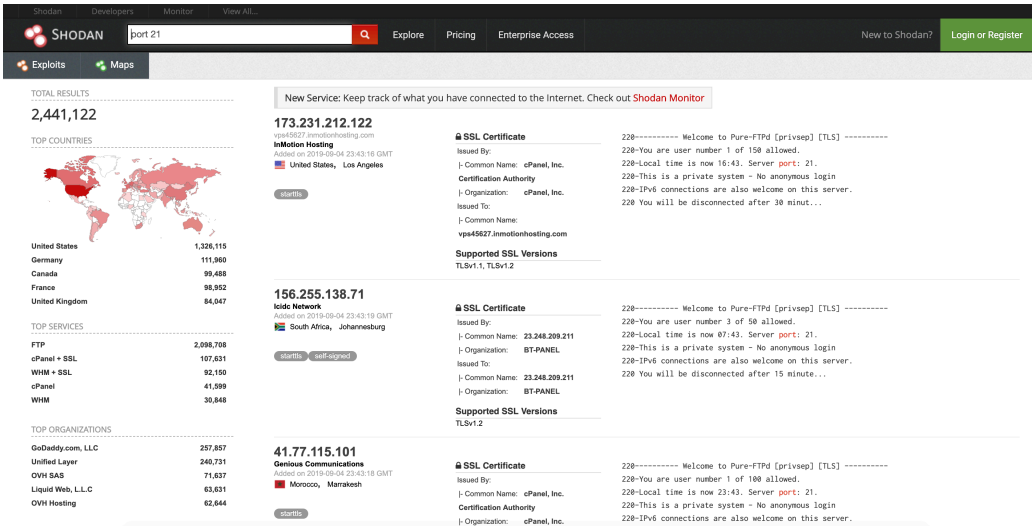


- Spectre (CVE-2017-5753/CVE-2017-5715)
  - Breaks isolation between applications
  - An application could read other application memory

https://meltdownattack.com/

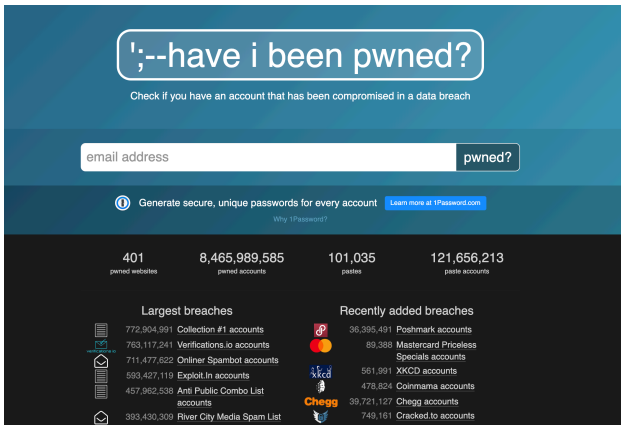
Find any device

- Shodan.io

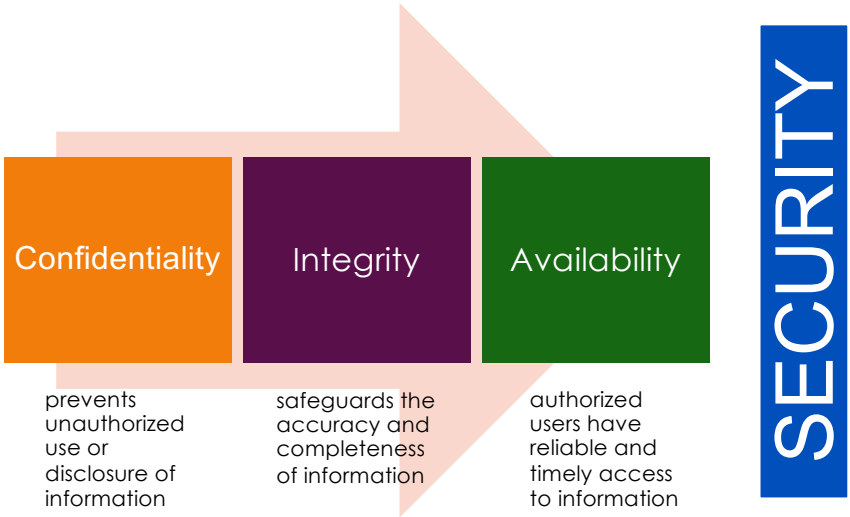


Compromised?

- Haveibeenpwned.com
- Tracks compromised accounts released into the wild



Goals of Information Security



Access Control

- The ability to permit or deny the use of an object by a subject.

- provides 3 essential services:
  - Authentication (identification of a user)
  - Authorization (who is allowed to use a service)
  - Accountability (what did a user do)

Authentication

- a means to verify or prove a user's identity
- The term "user" may refer to:
  - Person
  - Application or process
  - Machine or device
- Identification comes before authentication
  - Provide username to establish user's identity
- To prove identity, a user must present either of the following:
  - What you know (passwords, passphrase, PIN)
  - What you have (token, smart cards, passcodes, RFID)
  - Who you are (biometrics such as fingerprints and iris scan, signature or voice)

Strong Authentication

- An absolute requirement
- Two-factor authentication
  - Passwords (something you know)
  - Tokens (something you have)
- Examples:
  - Passwords
  - Tokens
  - Tickets
  - Restricted access
  - PINs
  - Biometrics
  - Certificates

Two-factor Authentication

- Requires a user to provide at least two authentication 'factors' to prove his identity
  - something you know
    Username/userID and password
  - something you have
    Token using a one-time password (OTP)
- The OTP is generated using a small electronic device in physical possession of the user
  - Different OTP generated each time and expires after some time
  - An alternative way is through applications installed on your mobile device
- Multi-factor authentication is also common

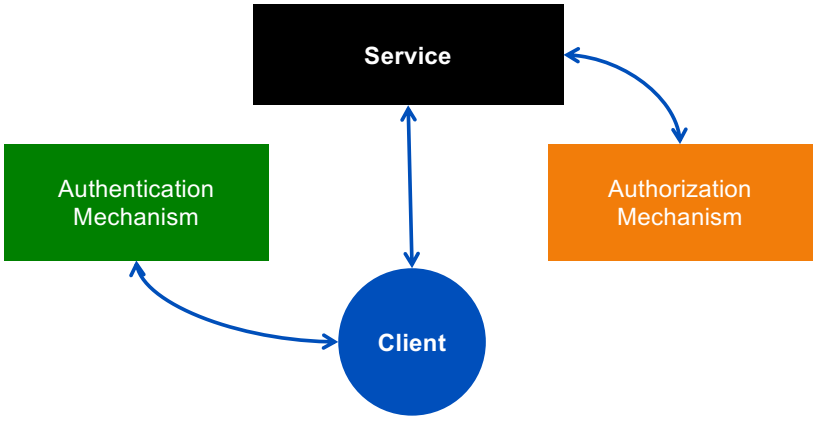
Authorization

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Authorization

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Authentication vs. Authorization



"Authentication simply identifies a party, authorization defines whether they can perform certain action" – RFC 3552

Authorization Concepts

- Authorization Creep
  - When users may possess unnecessarily high access privileges within an organization
- Default to Zero
  - Start with zero access and build on top of that
- Need to Know Principle
  - Least privilege; give access only to information that the user absolutely need
- Access Control Lists
  - List of users allowed to perform particular access to an object (read, write, execute, modify)

Single Sign On

- Property of access control where a user logs in only once and gains access to all authorized resources within a system.
- Benefits:
  - Ease of use
  - Reduces logon cycle (time spent re-entering passwords for the same identity)
- Common SSO technologies:
  - Kerberos, RADIUS
  - Smart card based
  - OTP Token
- Disadvantage: Single point of attack

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action

Source: NIST Risk Management Guide for Information Technology Systems

Integrity

- Security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity
- Data integrity
  - The property that data has when it has not been altered in an unauthorized manner
- System integrity
  - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation

Source: NIST Risk Management Guide for Information Technology Systems

Threat, Vulnerability, Risk

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
- Vulnerability
  - A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
- Risk
  - The possibility that a particular vulnerability will be exploited

Threat

- “a motivated, capable adversary”
- Examples:
  - Human Threats
    - Intentional or unintentional
    - Malicious or benign
  - Natural Threats
    - Earthquakes, tornadoes, floods, landslides
  - Environmental Threats
    - Long-term power failure, pollution, liquid leakage

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Where to check for vulnerabilities?
- Exploit
  - Taking advantage of a vulnerability

Risk

- Likelihood that a vulnerability will be exploited
- Some questions:
  - How likely is it to happen?
  - What is the level of risk if we decide to do nothing?
  - Will it result in data loss?
  - What is the impact on the reputation of the company?
- Categories:
  - High, medium or low risk

Risk = Threat * Vulnerability (* Impact)

What Are You Protecting?

- Identify Critical Assets
  - Hardware, software, data, people, documentation
- Place a Value on the Asset
  - Intangible asset – importance or criticality
  - Tangible asset – replacement value, training costs and/or immediate impact of the loss
- Determine Likelihood of Security Breaches
  - What are threats and vulnerabilities ?

Attack Motivation

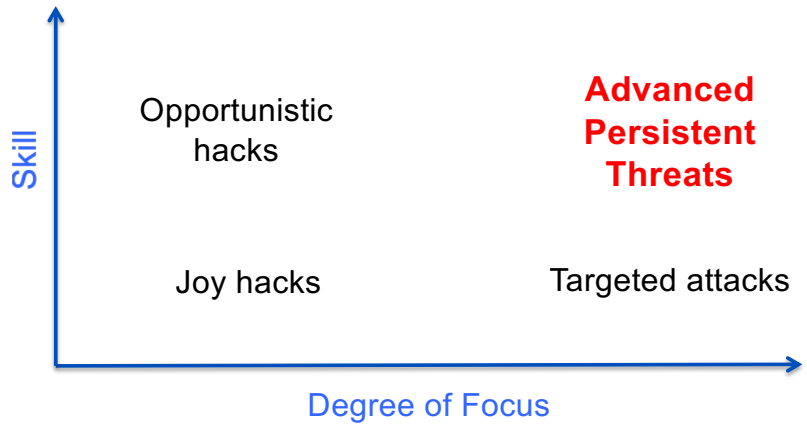
- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

Attack Motivation

- Nation States want SECRETS
- Organized criminals want MONEY
- Protesters or activists want ATTENTION
- Hackers and researchers want KNOWLEDGE

Source: NANOG60 keynote presentation by Jeff Moss, Feb 2014

The Threat Matrix



Joy Hacks

- For fun
  – with little skill using known exploits
- Minimal damage
  – especially unpatched machines
- Random targets
  – anyone they can hit
- Most hackers start this way – learning curve

Opportunistic Hacks

- Skilled (often very skilled) - also don't care whom they hit
  – Know many different vulnerabilities and techniques
- Profiting is the goal - bank account thefts, botnets, ransomwares....
  – WannaCry? Petya?
- Most phishers, virus writers, etc.

Targeted Attacks

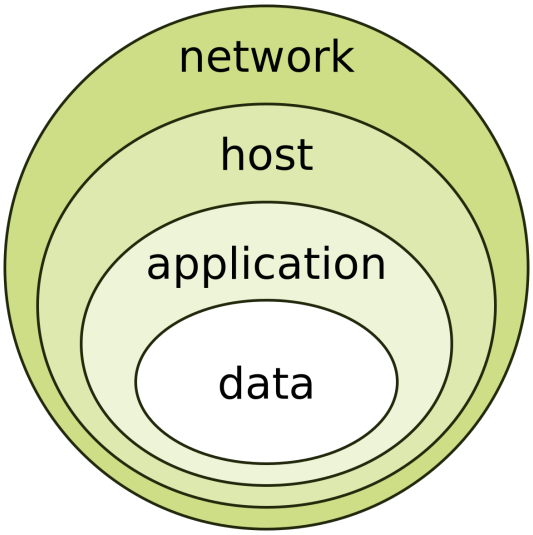
- Have a specific target!
- Research the target and tailor attacks
  - physical reconnaissance
- At worst, an insider (behind all your defenses)
  - Disgruntled employee
- Watch for tools like “spear-phishing”
- May use 0-days

Advance Persistent Threats

- Highly skilled (well funded) - specific targets
  - Mostly 0-days
- Sometimes (not always) working for a nation-state
  - Think Stuxnet (up to four 0-days were used)
- May use non-cyber means:
  - burglary, bribery, and blackmail
- ***Note:*** many lesser attacks blamed on APTs

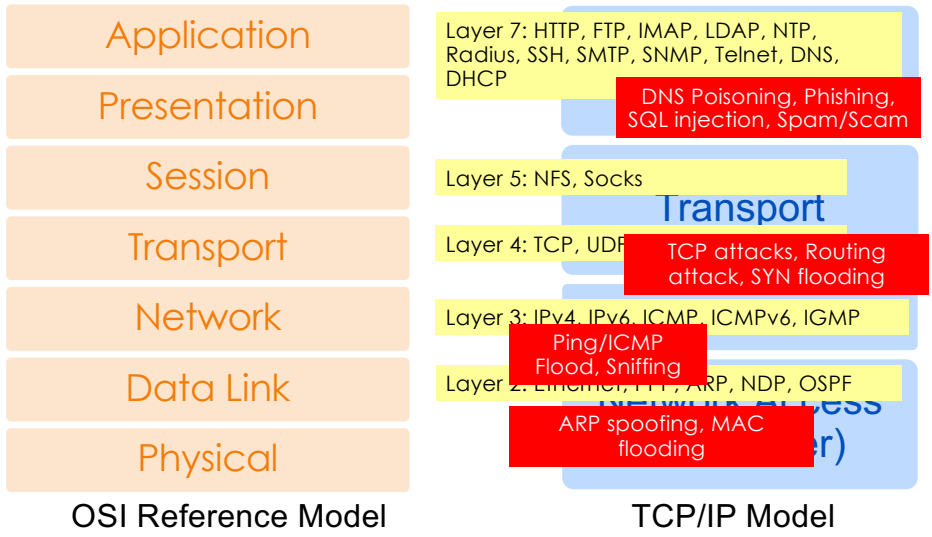
Defense in Depth

- Using multiple layers of security controls
- Explained using the **Onion Architecture**
  - Outer layer with firewalls
  - Middle layer with various controls
  - Center is data/service to be protected



SECURITY IN LAYERS

Attacks on Different Layers



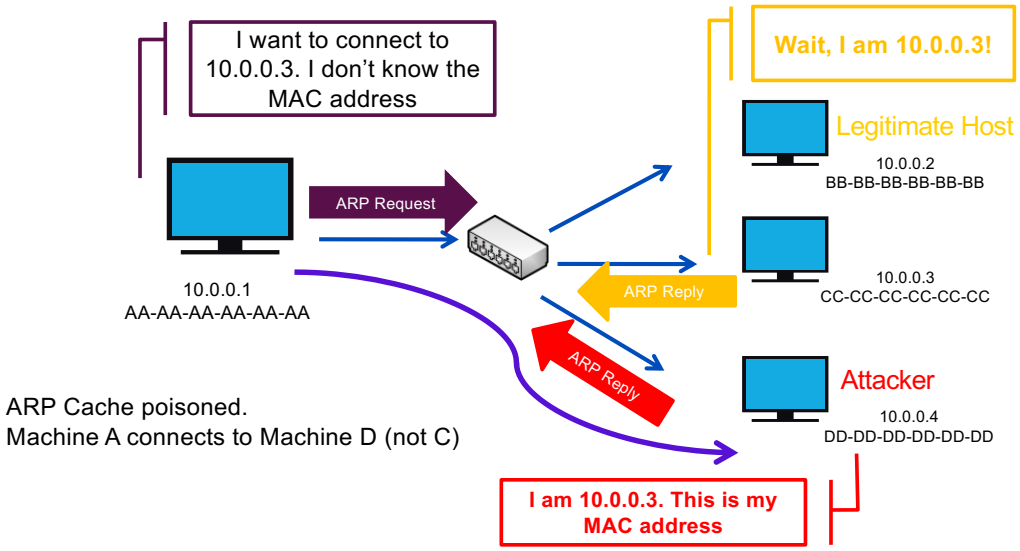
Application
Presentation
Session
Transport
Network
Data Link
Physical

L2 Attacks

ARP spoofing
MAC flooding
DHCP attacks
VLAN hopping

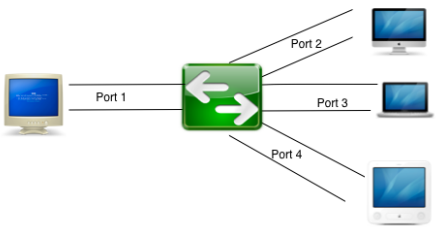
Layer 2: Ethernet, PPP, ARP, NDP, OSPF

ARP Spoofing



MAC Flooding

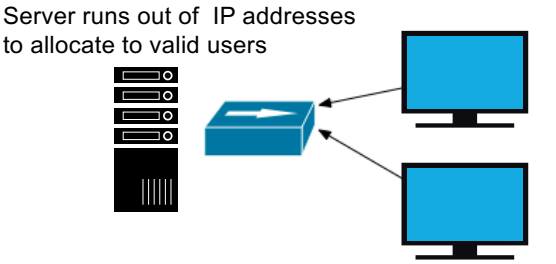
- Exploits the limitation of all switches – fixed CAM table size
- CAM = Content Addressable memory = stores info on the mapping of individual MAC addresses to physical ports on the switch.



	Port 1	Port 2	Port 3	Port 4
00:01:23:45:67:A1	x			
00:01:23:45:67:B2		x		
00:01:23:45:67:C3			x	
00:01:23:45:67:D4				x

DHCP Attacks

- DHCP Starvation Attack
  - Broadcasting vast number of DHCP requests with spoofed MAC address simultaneously



Attacker sends many different DHCP requests with many spoofed addresses.

- DHCP Spoofing
  - Rogue DHCP Server Attacks

Wireless Attacks - MITM

- Creates a fake access point and have clients authenticate to it instead of a legitimate one.
- Capture traffic (usernames, passwords)

Link Layer Defense

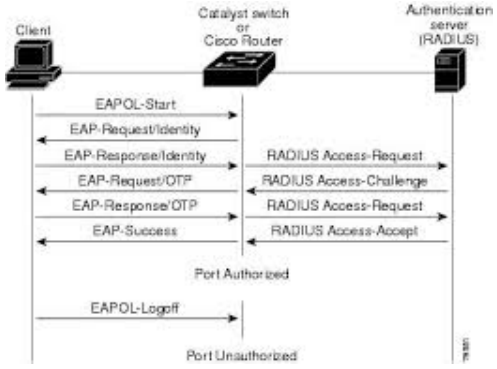
- Dynamic ARP inspection
  - Protect against ARP spoofing
  - Uses DHCP snooping
  - Forward ARP packets on Trusted interfaces without checks
  - Intercept all ARP packets on untrusted ports and check against IP-to-MAC binding
    - Drop and log if no valid binding

Link Layer Defense

- Port Security
  - Protects the MAC table
  - Limit the number of MACs per port (static or sticky learning)
    - Forwards valid frames (valid source MACs), and drops invalid frames
  - Violation could trigger:
    - Dropping of invalid frames and port shutdown, or
    - Drop frames with/without notification

Link Layer Defense

- 802.1X
  - Identity based network access control
  - Protection against rogue devices (DHCP or AP) attaching to a LAN



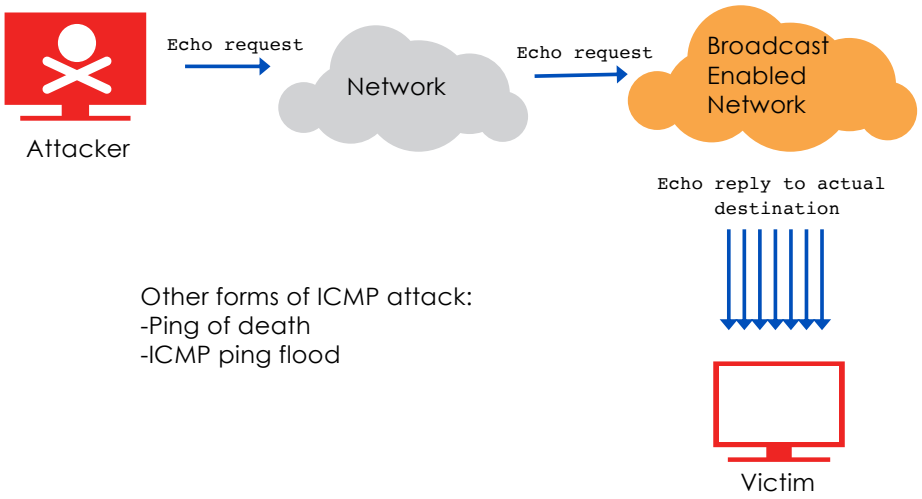
Application
Presentation
Session
Transport
Network
Data Link
Physical

L3 Attacks

ICMP Ping Flood
ICMP Smurf
Ping of Death
MITM Attack (Rogue Router)

Layer 3: IPv4, IPv6, ICMP, ICMPv6, IGMP

Ping Flood



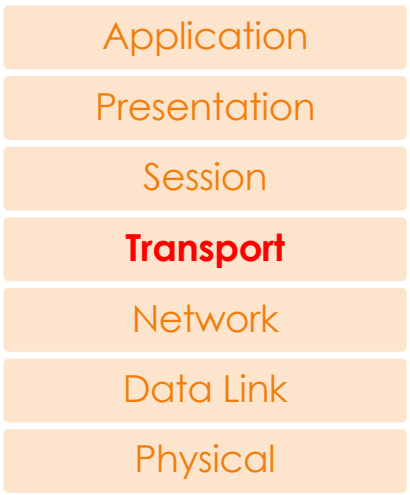
Other forms of ICMP attack:
-Ping of death
-ICMP ping flood

Routing Attacks

- Malicious route inspection
  - Poison routing table
  - To divert traffic and eavesdrop
- BGP attacks
  - ASes can announce arbitrary prefix
  - ASes can alter path

Defense - Routing Attacks

- Authenticate source of routing updates
  - Peer authentication
- Origin Validation
  - Rolled out today as RPKI
  - ROA (resource certificate) signed by the owner
    - Verifies the origin AS (signed route announcement)
- Path Validation
  - Sign the full path (ASNs traversed)
    - In IETF process as BGPsec



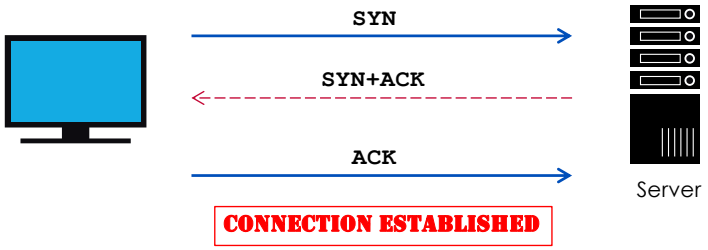
L4 Attacks

Layer 4: TCP, UDP, SCTP

TCP attacks
SYN flooding

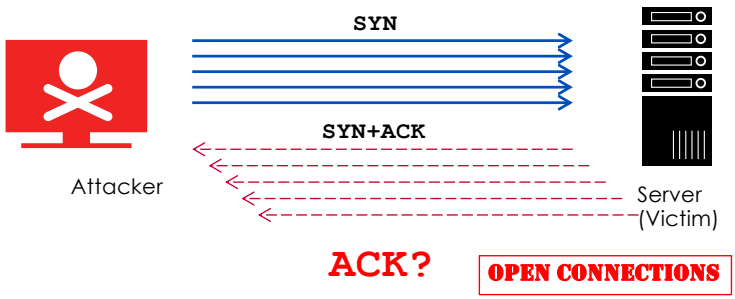
TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



Defense – SYN Flood

- SYN Cookies
  - MD5 hash (src IP, src port, dst IP, dst port, and ISN in SYN)
    - Sent back as ISN in its SYN-ACK
  - no states for half-open connections in memory
    - until valid ACK: SEQ = ISN+1
    - Store state after valid ACK

```
Enable:
vi /etc/sysctl.conf
Þ net.ipv4.tcp_syncookies = 1
```

```
Verify:
cat /proc/sys/net/ipv4_tcpsyncookies
sysctl –n net ipv4.tcp_syncookies
```


Layer 7: HTTP, FTP, IMAP, LDAP, NTP, Radius, SSH, SMTP, SNMP, Telnet, DNS, DHCP

Application-layer DDoS
DNS Poisoning
Amplification Attacks
Brute-force attacks
Command injection Attacks
Social Engineering
Phishing/Scamming/Ransomware

Application Layer Attacks

Application Layer Attacks

- Scripting vulnerabilities
- Cookie poisoning
- Buffer overflow
- Hidden field manipulation
- Parameter tampering
- Cross-site scripting
- SQL injection

Command Injection Attacks

- SQL injection
  - Insert an SQL query as a user input data
- Cross-site Scripting (XSS)
  - Malicious script inserted into trusted website
- Cross-site Request Forgery (CSRF)
  - Exploits website's trust in a user's browser

Read: Why I am anxious about clickjacking (link)

Layer 7 DDoS Attack

- Traditional DoS attacks focus on Layer 3 and Layer 4
- On Layer 7, a DoS attack is targeted towards the applications disguised as legitimate packets
  - aim is to exhaust application resources (bandwidth, ports, protocol weakness) rendering it unusable
- Includes:
  - Slowloris
  - LOIC / HOIC
  - RUDY (R-U-Dead Yet)

Application Layer Attacks

- Target applications or services at Layer 7
  - Increasingly common in recent years
- Sophisticated, stealthy and difficult to detect and mitigate
  - "slow and low"

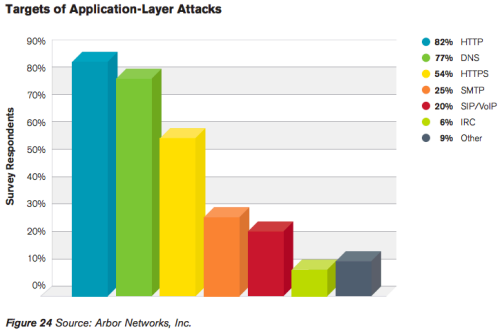


Figure 24 Source: Arbor Networks, Inc.

Source: Arbor Networks WISR 2014

Layer 7 DDoS – Slowloris

- Incomplete HTTP requests
- Properties
  - Low bandwidth
  - Keep sockets alive
  - Only affects certain web servers
  - Doesn't work through load balancers

Application Layer Attacks

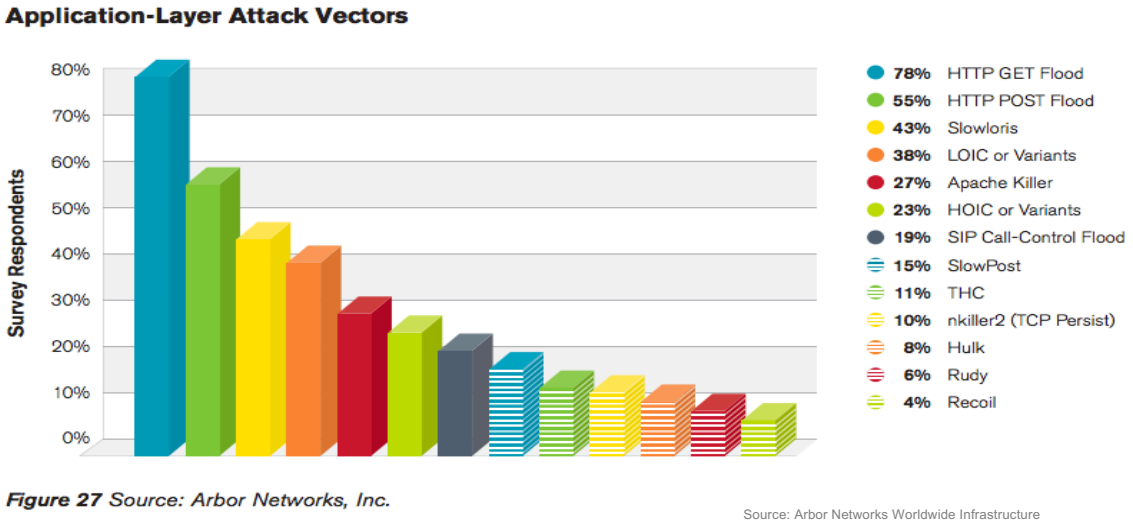


Figure 27 Source: Arbor Networks, Inc.

Source: Arbor Networks Worldwide Infrastructure Security Report Volume 2014

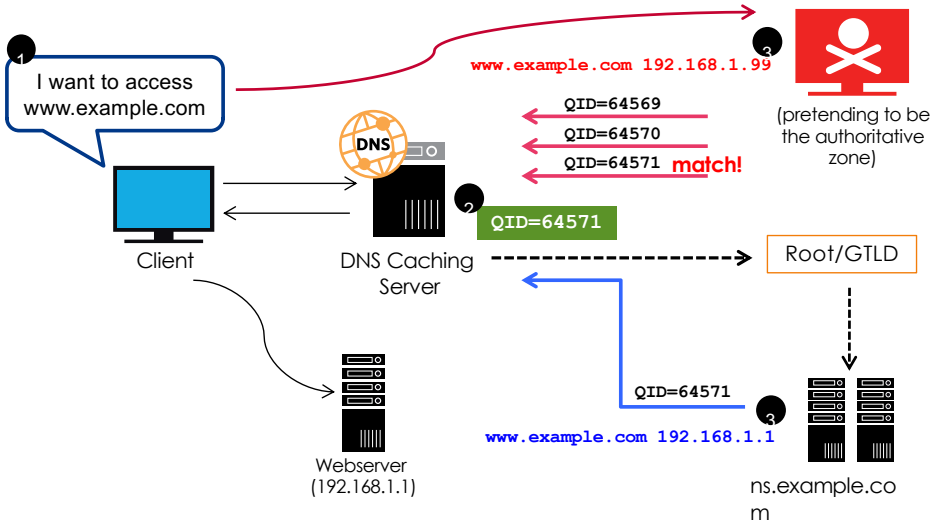
Layer 7 DDoS – Defense

- Load balancers
  - Delayed binding
  - Perform HTTP Request header completeness check
    - Request not sent to server until the final \r\n (CRLF) received from client
- Non-threaded webservers
  - not vulnerable to slow header attacks
- ModSecurity
  - Open source WAF plugin for Apache
  - embedded or reverse proxy mode
    - In front of the web server

DNS Cache Poisoning

- Caching incorrect resource record that did not originate from authoritative DNS sources.
- Result:
  - connection (web, email, network) is redirected to another target (controlled by the attacker)

DNS Cache Poisoning



Cache Poisoning – Defense

- DNSSEC – DNS security extensions
  - Uses public-key crypto
  - Operates as follows:
    - Records (RRset) signed with private key (authenticity and integrity)
    - Signatures (RRSIG) published in DNS responses
    - Public key published (DNSKEY) to verify signatures
    - Child zones sign their records with their private key
    - Parent sings the hash of child's public key - DS (chain-of-trust)

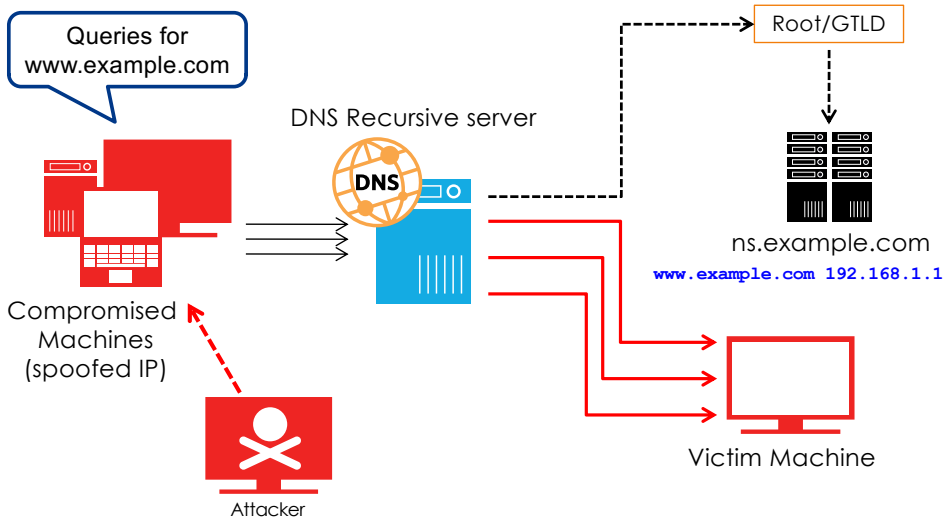
Amplification Attacks

- Exploiting UDP protocol to return large amplified amounts of traffic / data
- Small request, large reply
- Examples:
  - DNS
  - NTP
  - SMTP
  - SSDP

DNS Amplification Attack

- A type of reflection attack combined with amplification
  - Source of attack is reflected off another machine
  - Traffic received is bigger (amplified) than the traffic sent by the attacker
- UDP packet's source address is spoofed
- Several incidents in 2013

DNS Amplification



Source IP Spoofing – Defense

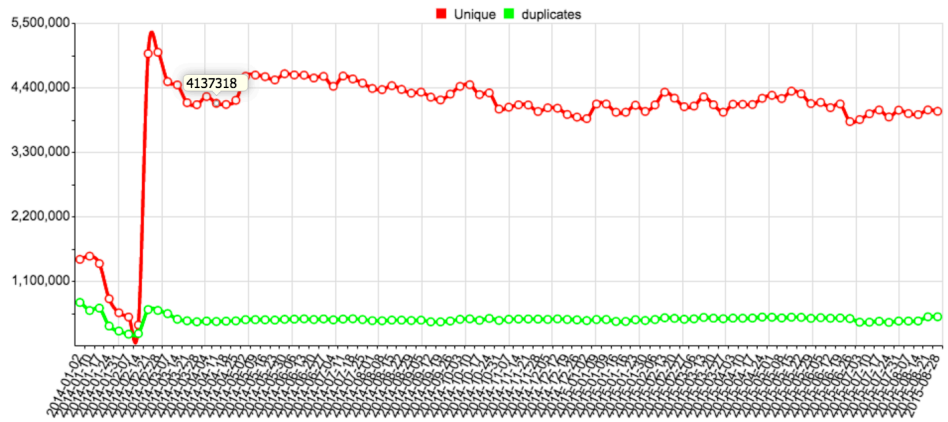
- BCP38 (RFC2827)
  - Since 1998!
  - https://tools.ietf.org/html/bcp38
- Only allow traffic with valid source addresses to
  - Leave your network
    - Only from your own address space
  - To enter/transit your network
    - Only from downstream customer address space

NTP Amplification

- Network Time Protocol (NTP)
- Port 123/UDP
- Exploits NTP versions older than v4.2.7
  - Vulnerable to “monlist” attack (CVE-2013-5211)
- Several incidents in 2014

Open NTP Servers

OpenNTPProject trends



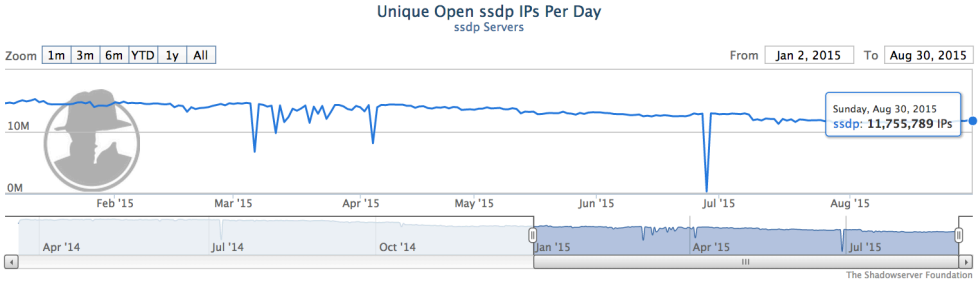
http://openntpproject.org/

NTP Amplification – Defense

- BCP38
- Upgrade NTP (ntpd) server
  - to v4.2.7p26 or later
  - Removes/disables “monlist” command; replaced with “mrulist”
    - Requires proof that the command came from the address in the NTP packet
- In older versions:
  - disable ntp monitor and do not answer ntpq/ntpdc queries

SSDP Reflection Attack

- Simple Service Discovery Protocol (SSDP)
- Part of Universal Plug and Play (UPnP) protocol standard
- Port 1900/UDP
- Several incidents in 2015



https://ssdpscan.shadowserver.org/

Using DNS for Other Attacks

- Fast flux
  - Domain name resolves to many different IP addresses over a short period

```
hello.com       IN          A           203.176.188.25
hello.com       IN          A           203.176.188.26
```

- Double IP Flux
  - Both hostname and IP address mapping and also the authoritative nameserver rapidly change

```
hello.com                   IN      A       203.176.188.25
hello.com                   IN      NS      203.176.188.111

hello.com                   IN      NS      61.101.155.3
hello.com                   IN      A       203.176.188.26
```

- Domain Generation Algorithms (DGAs)
  - Randomise the domain name, resolves to the same IP

```
qwekhh4562313erreq4.hello.com       IN      A       203.176.188.25
90j653gdfmrrn589sq.hello.com        IN      A       203.176.188.25
```


Application
Presentation
Session
Transport
Network
Data Link
Physical

Beyond Layer 7 ☺

People, Social Engineering

Botnets
Passwords
Spear Phishing

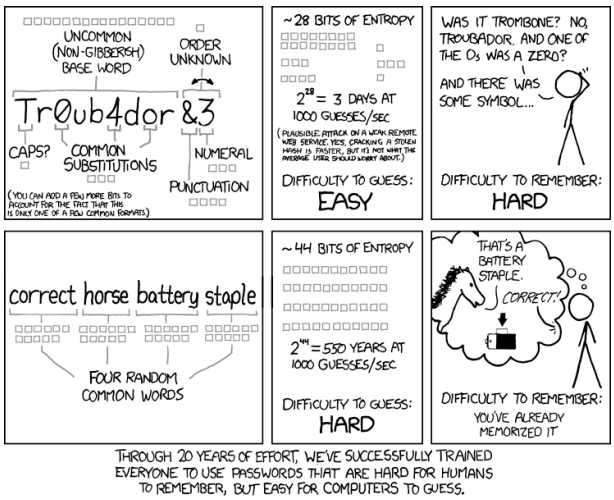
Botnet

- Collection of compromised computers (or 'bot')
- Computers are targeted by malware (malicious software)
- Once controlled, an attacker can use the compromised computer via standards-based network protocol such as IRC and HTTP
- How to become a bot:
  - Drive-by downloads (malware)
  - Go to malicious websites (exploits web browser vulnerabilities)
  - Run malicious programs (Trojan) from websites or as email attachment

Password Cracking

- Network sniffing
  - Listen or capture packet
- Dictionary attacks
  - Guessing passwords using a file of 1M possible password values
  - Offline dictionary attack when the entire password file has been attacked
- Brute-force attacks
  - Checking all possible values until it has been found
  - The resource needed to perform this attack grows exponentially while increasing the key size
  - Some tools: Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa
- Social engineering
  - Manipulate or trick a person to provide the password

Password Strength



https://xkcd.com/936/

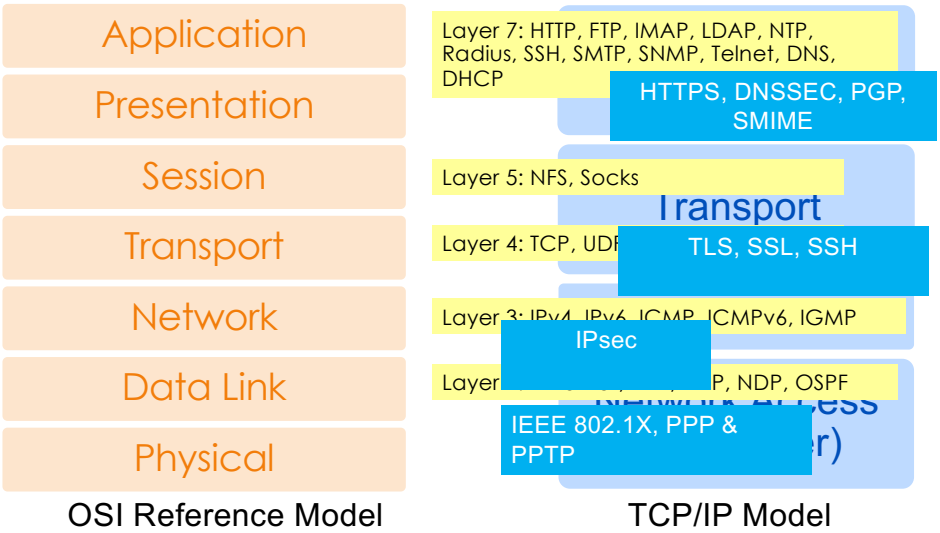
Pharming and Phishing

- Phishing – victims are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site
  - Typically uses fraud emails with clickable links to fake websites
- Pharming – redirect a website's traffic to another fake site by changing the victim's DNS settings or hosts file
- Spear phishing – a highly targeted phishing attack, customized to a specific person
  - Whaling attack – targets a "bigger fish"

Other forms of Social Engineering

- Pretexting - creating a fake identity to obtain private information
  - Ex: tricking helpdesk
- Baiting – exploits human curiousity
  - Ex: leaving USB sticks on the parking lot
- Tailgating – or “piggybacking” allows entry to restricted area

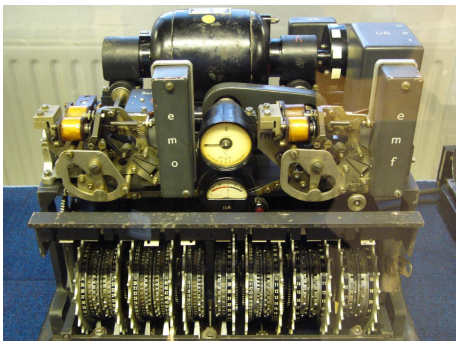
Attacks on Different Layers



CRYPTO BASICS

Cryptography

- Cryptography is everywhere



German Lorenz cipher machine

Cryptography

- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Other terms closely associated
  - Cryptanalysis = code breaking
  - Cryptology
    - Kryptos (hidden or secret) and Logos (description) = secret speech / communication
    - combination of cryptography and cryptanalysis
- Cryptography is a function of plaintext and a cryptographic key

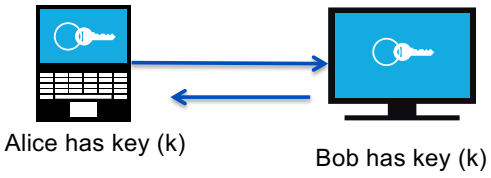
$$C = F(P,k)$$

Typical Scenario

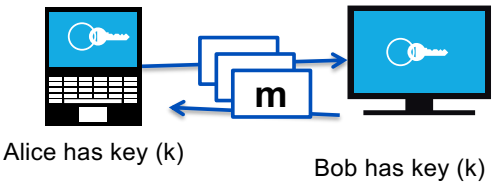
- Alice wants to send a “secret” message to Bob
- What are the possible problems?
  - Data can be intercepted
- What are the ways to intercept this message?
- How to conceal the message?
  - Encryption

Crypto Core

- Secure key establishment



- Secure communication



Confidentiality and integrity

Source: Dan Boneh, Stanford

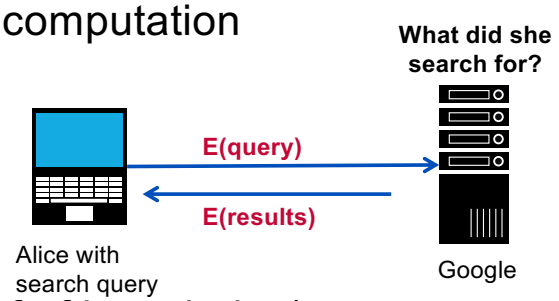
It can do much more

- Anonymous communication
- Anonymous digital cash
  - Spending a digital coin without anyone knowing my identity
  - Buy online anonymously?
  - Cryptocurrency / Bitcoin?
- Elections and private auctions
  - Finding the winner without actually knowing individual votes (privacy)

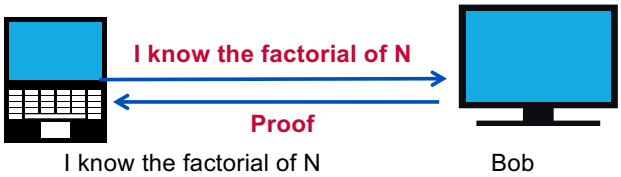
Source: Dan Boneh, Stanford

Other uses are also theoretically possible (Crypto magic)

- Privately outsourcing computation



- Zero knowledge (proof of knowledge)



Source: Dan Boneh, Stanford

History: Ciphers

- Substitution cipher
  - involves replacing an alphabet with another character of the same alphabet set
  - Can be mono-alphabetic (single set for substitution) or poly-alphabetic system (multiple alphabetic sets)
- Example:
  - Caesar cipher, a mono-alphabetic system in which each character is replaced by the third character in succession
  - Vigenere cipher, a poly-alphabetic cipher that uses a 26x26 table of characters

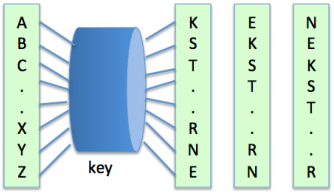
Transposition Cipher

- No letters are replaced, they are just rearranged.
- Rail Fence Cipher – another kind of transposition cipher in which the words are spelled out as if they were a rail fence.

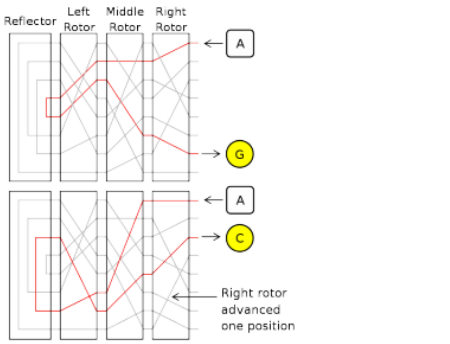
```
T...U...B...N...J...E...E...E...Y..
.H.Q.I.K.R.W.F.X.U.P.D.V.R.H.L.Z.D.G.
..E...C...O...O...M...O...T...A...O
```

History: Rotor Machines (1870-1943)

- Hebern machine – single rotor



- Enigma - 3-5 rotors



Source: Wikipedia (image)

Modern Crypto Algorithms

- specifies the mathematical transformation that is performed on data to encrypt/decrypt
- Crypto algorithm is NOT proprietary
- Analyzed by public community to show that there are no serious weaknesses
- Explicitly designed for encryption

Kerckhoff's Law (1883)

- The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
- In other words, the security of the system must rest entirely on the secrecy of the key.

Properties of a Good Cryptosystem

- There should be no way short of enumerating all possible keys to find the key from any amount of ciphertext and plaintext, nor any way to produce plaintext from ciphertext without the key.
- Enumerating all possible keys must be infeasible.
- The ciphertext must be indistinguishable from true random values.

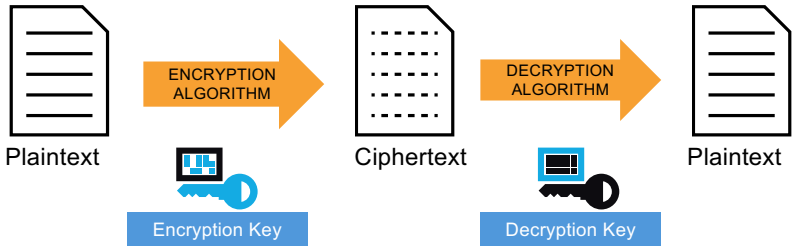
Encryption

- process of transforming plaintext to ciphertext using a cryptographic key
- Used all around us
  - In Application Layer – used in secure email, database sessions, and messaging
  - In session layer – using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
  - In the Network Layer – using protocols such as IPsec

Encryption – Benefits

- Resistant to cryptographic attack
- They support variable and long key lengths and scalability
- They create an avalanche effect
- No export or import restrictions

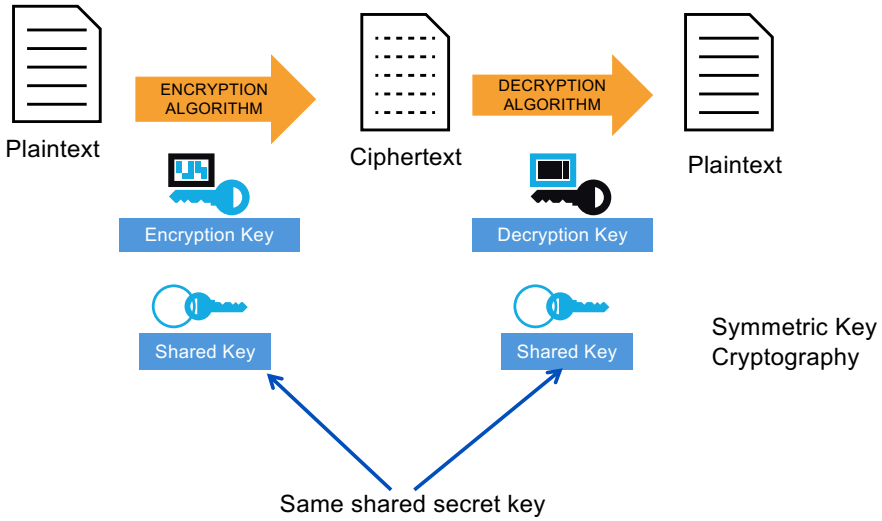
Encryption and Decryption



Symmetric Key Algorithm

- Uses a single key to both encrypt and decrypt information
- Also known as a secret-key algorithm
  - The key must be kept a “secret” to maintain security
  - This key is also known as a private key
- Follows the more traditional form of cryptography with key lengths ranging from 40 to 256 bits.
- Examples:
  - DES, 3DES, AES, RC4, RC6, Blowfish

Symmetric Encryption



Symmetric Key Algorithm

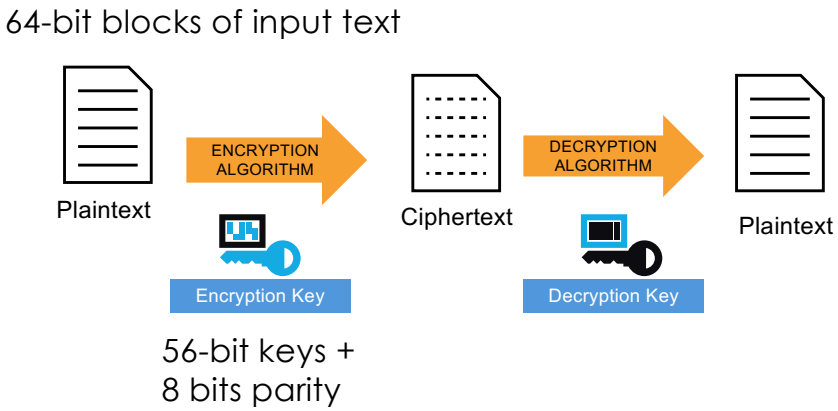
Symmetric Algorithm	Key Size
DES	56-bit keys
Triple DES (3DES)	112-bit and 168-bit keys
AES	128, 192, and 256-bit keys
IDEA	128-bit keys
RC2	40 and 64-bit keys
RC4	1 to 256-bit keys
RC5	0 to 2040-bit keys
RC6	128, 192, and 256-bit keys
Blowfish	32 to 448-bit keys

Note:
Longer keys are more difficult to crack, but more computationally expensive.

Data Encryption Standard (DES)

- Developed by IBM for the US government in 1973-1974, and approved in Nov 1976.
- Based on Horst Feistel's Lucifer cipher
- block cipher using shared key encryption, 56-bit key length
- Block size: 64 bits

DES: Illustration



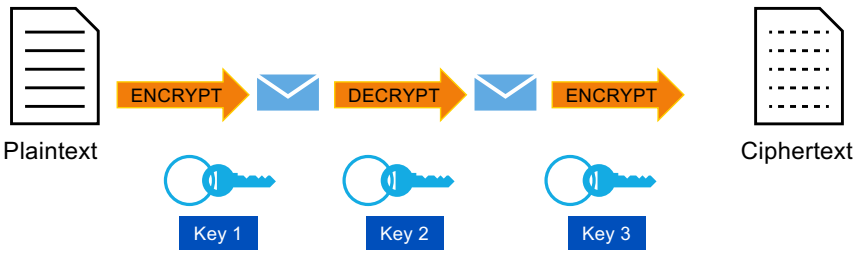
Triple DES

- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- Uses a key bundle comprising of three DES keys (K1, K2, K3), each with 56 bits excluding parity.
- DES encrypts with K1, decrypts with K2, then encrypts with K3

$$C_i = E_{K3}(D_{K2}(E_{K1}(P_i)))$$

- Disadvantage: very slow

3DES: Illustration



- Note:
  - If Key1 = Key2 = Key3, this is similar to DES
  - Usually, Key1 = Key3

Advanced Encryption Standard (AES)

- Published in November 2001
- Symmetric block cipher
- Has a fixed block size of 128 bits
- Has a key size of 128, 192, or 256 bits
- Based on Rijndael cipher which was developed by Joan Daemen and Vincent Rijmen
- Better suited for high-throughput, low latency environments

Rivest Cipher

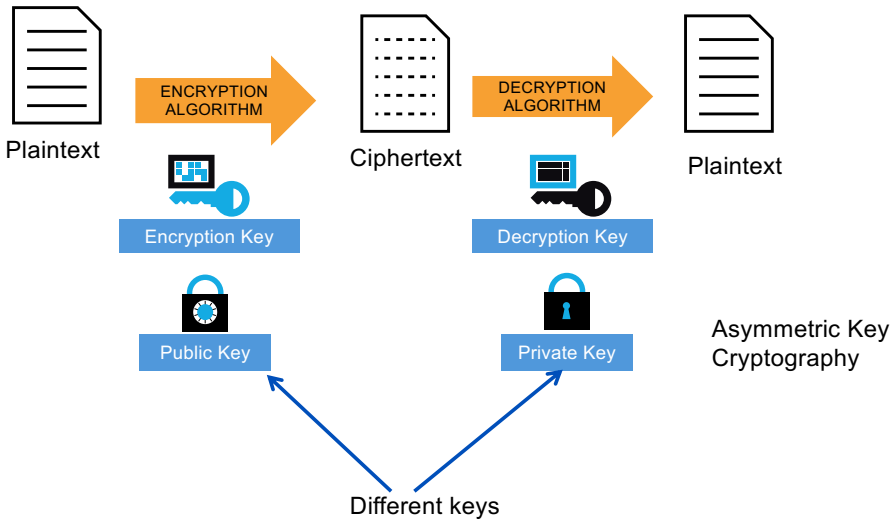
- Chosen for speed and variable-key length capabilities
- Designed mostly by Ronald Rivest
- Each of the algorithms have different uses

RC Algorithm	Description
RC2	Variable key-sized cipher used as a drop in replacement for DES
RC4	Variable key sized stream cipher; Often used in file encryption and secure communications (SSL)
RC5	Variable block size and variable key length; uses 64-bit block size; Fast, replacement for DES
RC6	Block cipher based on RC5, meets AES requirement

Asymmetric Key Algorithm

- Also called public-key cryptography
  - Keep private key private
  - Anyone can see public key
- separate keys for encryption and decryption (public and private key pairs)
- Examples:
  - RSA, DSA, Diffie-Hellman, ElGamal, PKCS

Asymmetric Encryption



Asymmetric Key Algorithm

- RSA – the first and still most common implementation
- DSA – specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for authentication of messages
- Diffie-Hellman – used for secret key exchange only, and not for authentication or digital signature
- ElGamal – similar to Diffie-Hellman and used for key exchange
- PKCS – set of interoperable standards and guidelines

Symmetric vs. Asymmetric Key

Symmetric	Asymmetric
generally fast Same key for both encryption and decryption	Can be 1000 times slower Uses two different keys (public and private) Decryption key cannot be calculated from the encryption key Key lengths: 512 to 4096 bits Used in low-volume

Hash Functions

- produces a condensed representation of a message
- takes an input message of arbitrary length and outputs fixed-length code
  - The fixed-length output is called the hash or message digest
- A form of signature that uniquely represents the data
- Uses:
  - Verifying file integrity
  - Digitally signing documents
  - Hashing passwords

Hash Functions

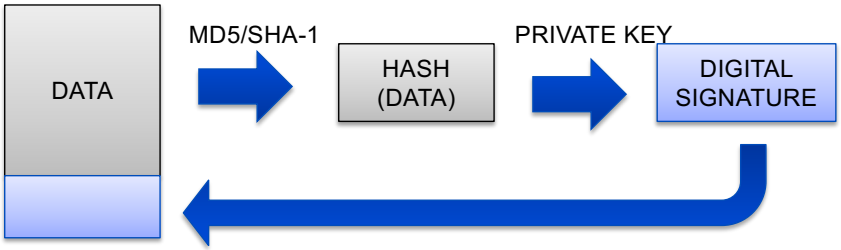
- Message Digest (MD) Algorithm
  - Outputs a 128-bit fingerprint of an arbitrary-length input
  - MD4 is obsolete, MD5 is still widely-used
- Secure Hash Algorithm (SHA)
  - SHA-1 produces a 160-bit message digest similar to MD5
  - Widely-used on security applications (TLS, SSL, PGP, SSH, S/MIME, IPsec)
  - SHA-256, SHA-384, SHA-512 can produce hash values that are 256, 384, and 512-bits respectively

Digital Signature

- A digital signature is a message appended to a packet
- The sender encrypts message with own private key instead of encrypting with intended receiver's public key
- The receiver of the packet uses the sender's public key to verify the signature.
- Used to prove the identity of the sender and the integrity of the packet

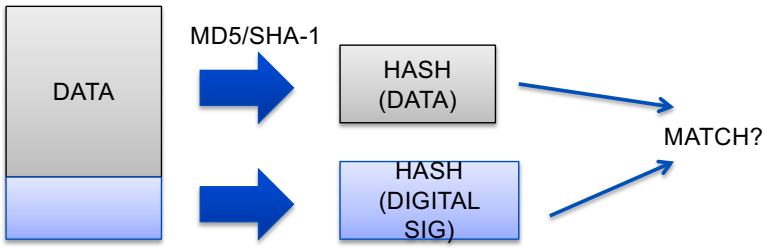
Digital Signature Process

- Hash the data using one of the supported hashing algorithms (MD5, SHA-1, SHA-256)
- Encrypt the hashed data using the sender's private key
- Append the signature (and a copy of the sender's public key) to the end of the data that was signed)



Signature Verification Process

- Hash the original data using the same hashing algorithm
- Decrypt the digital signature using the sender's public key. All digital signatures contain a copy of the signer's public key
- Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified.



Message Authentication Code

- Provides integrity and authenticity
- How it works:
  - In the sender side, the message is passed through a MAC algorithm to get a MAC (or Tag)
  - In the receiver side, the message is passed through the same algorithm
  - The output is compared with the received tag and should match
- Uses the same secret key
- Can also use hash function to generate the MAC, called Hash-based Message Authentication Code (HMAC)


Questions