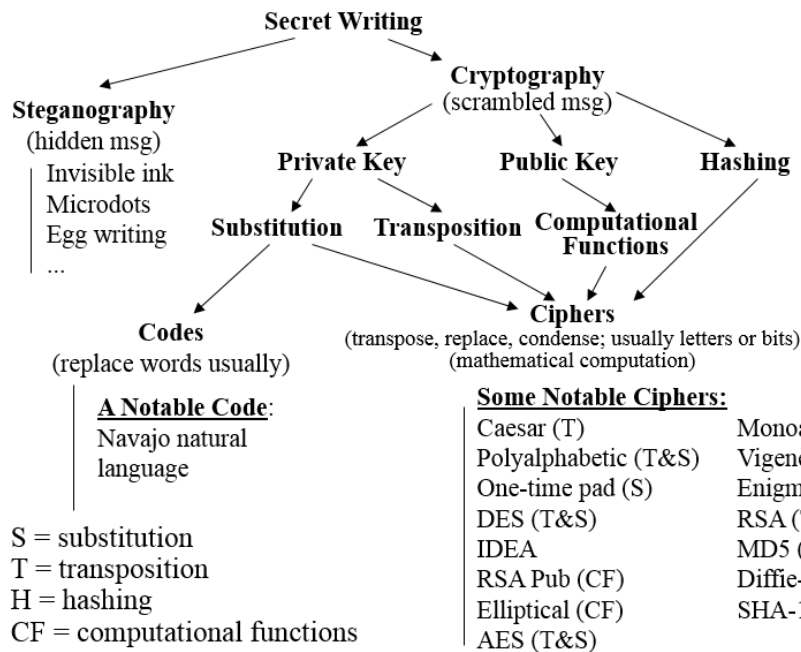


Week 9–Crypto



Cryptography and Ciphers usually refer to the same things, with Cryptography being the science and Ciphers being the encoded entities. The only exception is **Codes**. Private key ciphers usually use S and T. Public key systems use CF.

•Know the terms on the “Terminology” slides

- Secret Writing**: The science of hiding *messages* or their *meaning* from outsiders.
- Steganography**: Science of hiding messages so that the *existence* of the message is *unknown* to outsiders.
- Cryptography**: Science of hiding the *meaning* of messages that are *known* to exist.
 - Writing and reading scrambled (often incorrectly referred to as "coded") messages.
 - Today *cryptography* subsumes *coding*, *transposing*, *hashing*, and some forms of authentication.
- Coding (Substituting)**: The process of substituting one part of a message with something that is external to the message so as to hide its meaning from outsiders. Parts can be letters, words, phrases, bits...
- Transposing**: The process of moving parts of a message from one place to another within the message so as to hide its meaning from outsiders. Parts can be letters, words, phrases, bits...
- Hashing**: Creating a fixed-size value called a “hash” using a message as the source to create the hash, and doing it in a way that distributes the possible messages evenly among the possible hash values.
- Cryptanalyst**: A person or persons that try to decipher encrypted messages. Often synonymous with "attacker" or "threat".
- Encryption**: The science of scrambling the contents of the message in such a way that hides its meaning from outsiders.

- **Plaintext or Cleartext**: Unencrypted message (not necessarily text).
- **Ciphertext**: Encrypted plaintext.
- **Entropy**: Measure of uncertainty associated with a random variable

- ☐ Substitution (S-box) (substitution)
- ☐ Permutation (P-box) (transposition)

• **Confusion**

- ☐ Make relationship between the **ciphertext** and the **key** as complex as possible

• **Diffusion**

- ☐ Dissipate the statistical structure of **plaintext** over the entire **ciphertext**

• **Know the four goals of cryptographic ciphers**

• **Confidentiality**

- ☐ Ensures that the meaning of the message is hidden for outsiders.

• **Authentication**

- ☐ Establishes the identity of the sender of the message.

• **Integrity**

- ☐ Ensures that the message & its authentication have not been changed.

• **Non repudiation**

- ☐ The sender cannot deny that she or he sent the message.

O Closely related to Authentication.

- ☐ Non-repudiation is sometimes not listed as goal because it is achieved via authentication methods

• **Note**: There is no attempt to hide the fact that a cipher exists.

• **Know the difference between symmetric and asymmetric key crypto**

- ☐ Private key encryption

O Also called *symmetric* or *secret*

- ☐ Public key encryption

O Also called *asymmetric*

- ☐ Hashing

O Also called *message digest*

Symmetric Key Cryptography: a single key is used to encrypt as well as decrypt

Asymmetric Key Cryptography: Two keys, one public (Kpu) and one private (Kpr)

•Know the common stream and block ciphers

•Stream ciphers process messages a bit or byte at a time when encrypting or decrypting

•Block ciphers divide messages into blocks, each of which is then en/decrypted

□Sort of like a substitution on very big characters

O 64-bits or more

□Many current ciphers are block ciphers

Stream ciphers:

1.MonoalphabeticCiphers:

- Uses substitution
- Fixed alphabet during encryption process
- Example: Caesar Cipher

2.Polyalphabetic Ciphers:

- Uses substitution
- Alphabet changes during encryption process
- Example: Vigenère Cipher, Enigma Machine

3.One-Time Pad (OTP)

- Uses substitution
- If used correctly, provides “Perfect Secrecy” and cannot be broken by cryptanalysis
- Key is completely random and provides no information about the content of the plaintext
- Key is also as long as the plaintext and is kept secret and is not ever reused

Block ciphers:

• Most symmetric block ciphers are based on a **Feistel Cipher Structure** (Horst Feistel)

Claude Shannon and Substitution-Permutation Ciphers

1.DES (Data Encryption Standard)

•Message is a binary bit string

- Message is broken into 64-bit blocks
- Each block encrypted using 56-bit secret key
 - Arranged as eight 7-bit pieces
- Process is symmetric: almost same process for encoding and decoding

2.3DES (Triple Data Encryption Standard)

- Uses the same algorithm as DES
- Applies the algorithm three times
- Uses a different key each time
- $C = Ek_1[Dk_2[Ek_3[P]]]$
- Pros & Cons
 - Uses same software as DES
 - Block size is smallish (64 bits), resulting in insecurities
 - Three times as slow as DES

3. AES (Advanced Encryption Standard)

- 128-bit block size
- Keys can be 128, 192, or 256 bits
- Approved by NIST in November 2001
- AES-128 and its variants have been shown to be vulnerable
 - Side Information Attack
 - If software runs on same system as AES code, gets key in a few seconds
 - Others
- AES-192 & 256 Vulnerability
 - Related Keys Attack
 - Monitor ciphertext created by several different but mathematically related keys

4. IDEA (International Data Encryption Algorithm)

- First 128-bit key widely used
 - Used by browsers and PGP
- Developed by Swiss
- Uses 64-bit block size

- Can use 4 different block chaining methods
- Used in several public encryption schemes those are applied to email

□Modes of Operation –ECB, CBC, CFB, OFB, CTR

- ECB: Electronic Code Book
 - Each block of plaintext is encoded independently
- CBC: Cipher Block Chaining
 - Blocks are linked together in the encryption operation
- CFB: Cipher FeedBack
 - Combination of stream and block-chaining encryption
- OFB: Output FeedBack
 - Combination of stream and block-chain encryption but plaintext is XORed to the output of the block cipher in order to get the cipher text block.
- CTR: CounTeR
 - Similar to OFB but encrypts counter value rather than any feedback value
 - Used for high-speed network encryptions

•Understand broadly how CrypTool was used to crack ciphers

- 64 bit kit
 - 5 bytes (40 bits) can crack in around 20 seconds
 - 6 bytes (48 bits) can crack almost instantly

•Understand how to manually decrypt cipher text with the Caesar and Vigenere ciphers

•Caesar:

- Encrypt using Caesar cipher with shift of 2 (letter C)
- Check out histogram before and after
- Use Auto-Decryption option under Analysis

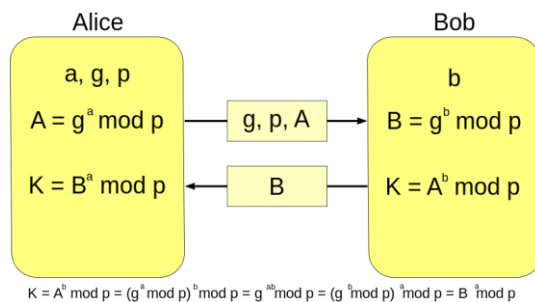
•Vigenere每个单词有不同的顺序排列进行解密

- Align **A** with **W**: Then **S**→**O** to encrypt 1st letter
 - 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
 - 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
- Align **A** with **H**: Then **T**→**A** to encrypt 2nd letter
 - 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
 - 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

- ❑ Encrypt
- ❑ Set key as BRIA
- ❑ Put portion of encrypted text into new file
- ❑ Show how key detection doesn't always find the correct number of characters in the key
- May take trial and error

• Understand the broad concept that Whitfield Diffie came up with

公钥加密是一种干扰信息的方法，使用该方法的双方拥有一对密钥，其中一个可以公开分享，而另一个只有预定的目标接收方才知晓。任何人都可能使用私人的公开密钥对信息进行加密。但是，只要预定接收方的解密密钥被安全地保护起来，信息就无法被解码。



mod: 模。意思就是求余数。

1. 爱丽丝与鲍伯协定使用 $p=23$ 以及 base $g=5$.
2. 爱丽丝选择一个秘密整数 $a=6$, 计算 $A = g^a \mod p$ 并发送给鲍伯.
 - $A = 5^6 \mod 23 = 8$.
3. 鲍伯选择一个秘密整数 $b=15$, 计算 $B = g^b \mod p$ 并发送给爱丽丝.
 - $B = 5^{15} \mod 23 = 19$.
4. 爱丽丝计算 $s = B^a \mod p$
 - $19^6 \mod 23 = 2$.
5. 鲍伯计算 $s = A^b \mod p$
 - $8^{15} \mod 23 = 2$.

• Understand how the key pairs work for Confidentiality and Authentication

One Lock & Two Keys

- Matched pair (Public & Private keys)
 - ❑ Public keys are shared and not secret
 - ❑ Private keys are never shared and are kept secret

- Confidentiality

- ☐Public Key encrypts data

- O Then private key decrypts that data

- Authentication

- ☐Private Key encrypts data

- O Then public key decrypts that data

- Understand how message integrity and authentication, and non-repudiation is achieved

1. Alice sends information about herself and her public key to the CA
2. The CA issues her a digital certificate
3. Alice runs plaintext message through hash function to create the hash
4. Alice encrypts message to Bob with Bob's public key
5. Alice encrypts hash with her private key to create digital signature
6. Alice sends encrypted message, digital signature, and her digital certificate to Bob
7. Bob decrypts message with his secret key
8. Bob decrypts Alice's digital certificate to obtain Alice's public key
9. Bob hashes decrypted plaintext message to obtain his own hash of it
10. Bob uses Alice's public key to decrypt digital signature to view the hash Alice created
11. Bob verifies that the hash he took matches Alice's hash

- We now know that:

- ☐The message has not been changed since being signed

- ☐Whoever signed the message used Alice's private key

- ☐Bob obtained Alice's public key from a trusted digital certificate that bound the public Key to Alice's identity

- ☐Alice can't deny she signed the message because her secret key was used to create the digital signature

- What uses hashing to guarantee message integrity and somewhat provides authentication???

- ☐Digital Signatures!

- How do we trust that the person who created the digital signature is really Alice and not an imposter??? Also, how do we enforce non-repudiation so the sender cannot deny they sent the message??? ☐Use Digital Certificates!

•Be familiar with Digital Signatures, CAs, Digital Certificates, Etc.

Digital Signature

- Allows recipient to verify:
 - ☐ Message has not changed (Integrity)
 - ☐ Who the message came from (Authentication) ***

工作原理:

- Run plaintext message through hash function to form the hash
- Encrypt hash with sender's private key to create the digital signature
- Send plaintext message and digital signature to recipient

Digital Certificates

- Helps recipients determine if the digital signature and public key belong to the sender
- Allows exchange of public keys
- Digital Certificate consists of:
 - ☐ Serial Number
 - ☐ Issuer
 - ☐ Dates Valid
 - ☐ Sender's Public Key
 - ☐ Identity information for the sender
 - Name, User ID, etc.
 - ☐ Other users' digital signatures that have vouched that the identify information is bound to the public key
 - Creates trust

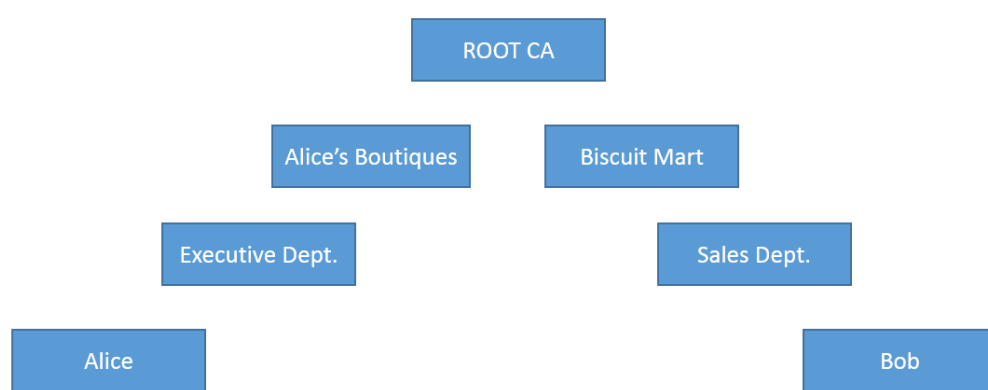
工作原理:

- Certificate Server
 - ☐ Database that allows users to submit their certificates as well as retrieve other individual's certificates
- Public Key Infrastructure (PKI)
 - Allows trust between parties that might not know each other previously
 - X.509 Standard which describes:
 - ☐ Ability to issue, revoke, store, retrieve, and trust certificates

Certificate Authority (CA)

- Uses PKI
- CA binds parts of certificate (user's public key, information about them) by using its secret certification key to encrypt them
- Individuals can decrypt the certificate by using the CA's public verification key

Certificate Hierarchies



- Root CA issues certificate to Alice's Boutiques and Biscuit Mart
- Alice's Boutiques issues certificate to their Executive Dept.
- Biscuit Mart issues certificate to their Sales Dept.
- Executive Dept. issues certificate to Alice
- Sales Dept. issues certificate to Bob

Certificate Hierarchy

▲ VeriSign Class 3 Public Primary Certification Authority - G5
▲ Symantec Class 3 EV SSL CA - G3
www.chase.com

Uses of CA Digital Certificates

- Website certificates
 - Software Code signing
 - Software Update signing
- ☐ MS, Mac OS X, Linux all use CAs

- Be familiar with the email and web standards that offer all four goals of cryptographic ciphers

PGP (Pretty Good Privacy) / GPG

- Hybrid Cryptosystem

- ☐Uses RSA for asymmetric encryption to share key and IDEA for symmetric encryption of data

- ☐Requires PKI to distribute and manage digital certificates

- Often used for sending and receiving secure emails

- Allows for:

- ☐Full disk encryption

- ☐File share encryption

- ☐Secure email

S/MIME

- Secure/Multipurpose Internet Mail Extensions

- Hybrid Cryptosystem

- ☐Uses RSA for asymmetric encryption to share key and AES for symmetric encryption of data

- ☐Requires PKI to distribute and manage digital certificates

- Often used for sending and receiving secure emails

HTTPS with SSL/TLS

- Uses TLS/SSL for encryption

- ☐Uses asymmetric encryption to share keys and symmetric encryption for data (various ciphers and algorithms used)

- ☐PKI with X.509 Digital Certificates

Difference between TLS and SSL:

- Transport Layer Security (TLS) is basically a newer version of Secure Sockets Layer (SSL)

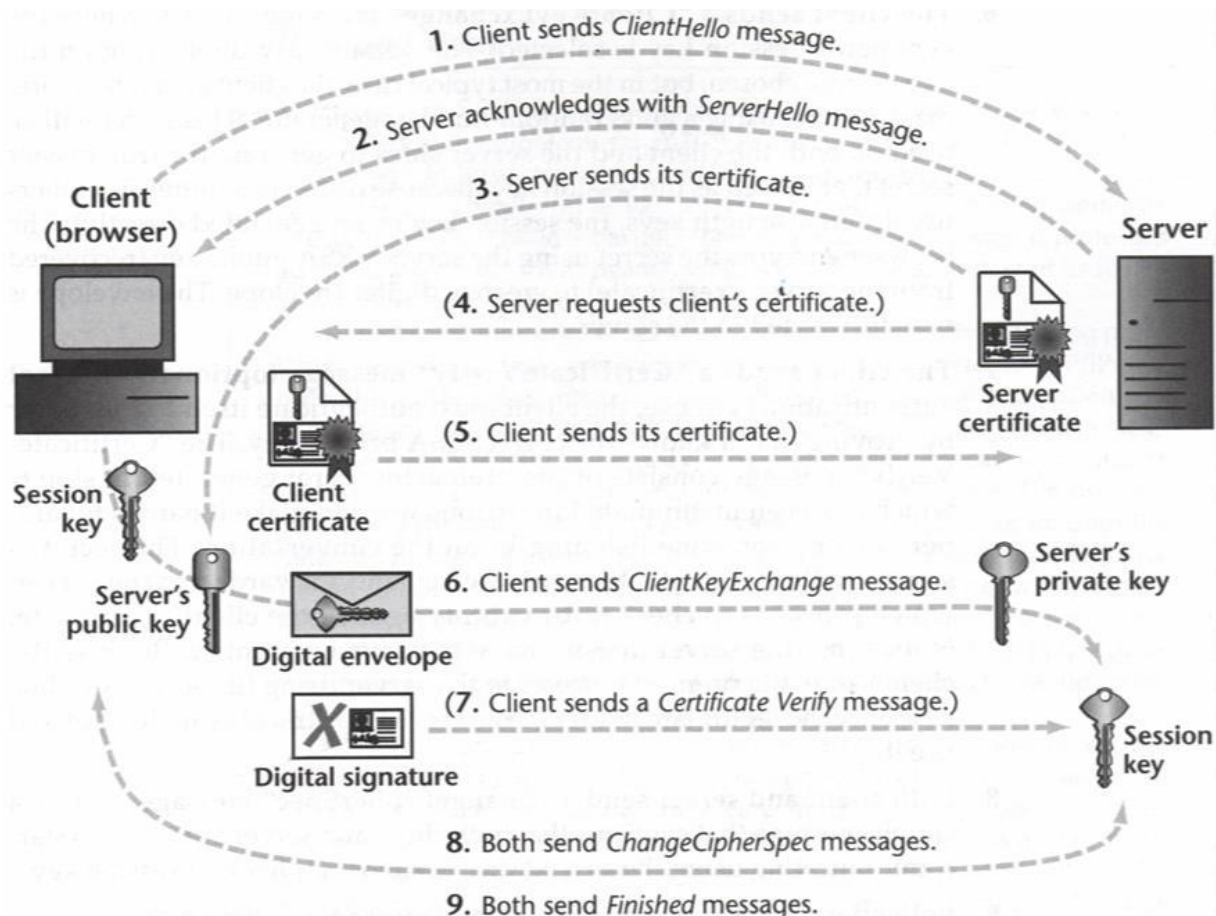
- Most browsers use TLS today

- Ensures you are communicating with intended web server

- Ensures messages aren't changed in transit

- Ensures data is confidential

- Ensures non-repudiation



•Be familiar with the tools used in the in-class SSH lab

- Secure Shell (SSH) provides an encrypted tunnel to remotely administer a system, move files.
- Secure replacement for telnet, ftp, rlogin, rcp, and rsh

Pageant lets you import your private key and only asks for your passphrase once. Then, as long as pageant is running, you won't have to type in your passphrase.

Command:

- `apt-get install openssh-server` `service ssh start`
- `service ssh status` `ssh-keygen-t rsa`

Command used to decrypt: `openssl des3 -d -a -in plans`

des3 = cipher used to encrypt

-d = decrypt

-a = base64 decode

-in = input file to be decrypted

Week 11 – Stego/ Firewalls

•Know details about overt and covert files

- ☐ A carrier or overt file

- ☐ A covert file to be hidden

- Any type of covert data file can be hidden inside a carrier file

- ☐ A covert executable file hidden inside a carrier Word file

- ☐ A covert image file hidden inside a carrier audio file

- ☐ Etc.

- However, some carrier file types are better than others for holding covert data

- ☐ Each Stego tool only works with specific types of carrier files

•Understand the common stego schemes (Image and Audio file carriers)

Popular Overt / Carrier Files

- Carrier files can be of many different types

- ☐ Document files (e.g., text, spreadsheet, word processor)

- ☐ Image files (e.g., jpeg, bmp, gif, tiff)

- ☐ Video files (e.g., avi, flv, H120, H261 through H265, mpeg1, mpeg4)

- ☐ Audio files (e.g., mp3, wav, G711, G729)

- ☐ Web page files

- Most of the above are in the public domain

- There are many more that are proprietary

- ☐ e.g., realAudio, realVideo...

Other Possible Carrier Schemes

- Video files

- Document files such as those of MSWORD

- ☐ e.g., Put covert info in slack space

- Web pages

- ☐ e.g., HTML non-visible text and images

- Simple text files

Hidden / Covert Files

- The file(s) to be hidden can usually be any bit stream
- So the nature of the file actually is irrelevant
 - ☐ Don't matter if the file is text, doc, xls, bmp, avi, mp3...
 - ☐ Don't matter if the file is compressed, encrypted or both
 - ☐ Don't matter what encryption or compression algorithm is used
 - ☐ They're all just bits as far as the stego hiding software is concerned

• Understands the differences between and how data is hidden in each method:

• Insertion

- Where data is hidden
 - ☐ Locations in the overt file that the application ignores
 - Header of File
 - Slack Space (•A Windows NTFS cluster is 4KB)
 - Ignored space in the file proper
- How data is hidden
 - ☐ Data is added to file and the application ignores it
- The file size increases when covert data is added
- Insertion is the most basic stego method and is often easy to detect since:
 - ☐ The file size increases
 - ☐ The covert data is often stored in one part of the file

• Substitution

- Where data is hidden
 - ☐ In place of part of carrier file content
 - ☐ Modified carrier content
- How data is hidden
 - ☐ Overwrite carrier data in such a way that
 - It is not noticeable
 - Keeps the overt file usable by the application
- The file size generally does not increase when covert data is added

- **Generation**

- Where data is hidden

- ☐ In the overt file as part of the overt file

- How data is hidden

- ☐ Algorithmic scheme is used to hide data in the overt file

- ☐ Covert file algorithm and values create the overt file

- The file size does not increase when covert data is added since the covert data is designed to be a part of the file

- Know the general steganalysis detection techniques**

- Statistical detection of changes in patterns of the carrier file (LSB, etc.)

- Could be visible or audible differences

- ☐ Could use histogram to look for patterns

- Take a hash of original known good file and compare it against the potential stego file

- Size differences in file

- Look for signature that stego program uses

- ☐ Hiderman places “CDN” at end of file (footer)

- Understand the commands for hiding and unhiding alternate data streams**

Alternate Data Streams (ADS)

- ☐ echo “This is a normal file” > file1.txt

- ☐ echo “This is a secret file” > file1.txt:hidden.txt

- ☐ more file1.txt

- ☐ more < file1.txt:hidden.txt

- ☐ notepad file1.txt

- ☐ notepad file1.txt:hidden.txt

- Understand the capabilities a Firewall needs to have

- Defines a single choke point
- Creates logs for monitoring security events
- Often hosts other useful functions:
 - NAT
 - Web usage auditing
 - IPS/IDS
- Can often be used to implement virtual private networks (VPN)

- Understand the difference between the two types of Firewalls (as well as the four sub-types)

Contrast Packet Filters and Proxy Servers

- Client/Server Connections
 - Packet filters allow direct connections
 - Proxy servers prevent direct connections
 - TCP: Instead the Proxy Server splices two TCP connections together
 - UDP: Proxy Server investigates the payload
- Application
 - Packet filters do not understand the application or service
- oOr mostly do not
 - Proxy servers do understand the application or service

1. Packet Filters:

- Stateless packet filtering firewall
- Stateful inspection firewall

Packet Filters –General Traits

- Can either:
 - Allow packets that meet defined criteria to pass through the firewall
 - Reject packets that meet defined criteria to be blocked from passing through the firewall
- May examine the following attributes of a packet:

- ☐ Protocol headers
- ☐ Payload
- ☐ Pattern generated by a sequence of packets

Stateless Packet Filtering Firewall

•Applies rules to each incoming and outgoing packet based on:

- ☐ IP Header
- ☐ TCP/UDP Headers
- ☐ Firewall Interface

Stateful Packet Filtering Firewall

•Applies rules to each incoming and outgoing packet based on:

- ☐ IP Header
- ☐ TCP/UDP Headers

O Evaluates Sequence and ACK #s

O Remembers connection state (TCP 3-Way Handshake)

- ☐ Firewall Interface

Stateless vs Stateful Packet Filters

•Stateless (Static):

- ☐ Evaluates contents of each packet but doesn't keep track of the connection state
- ☐ Similar to an Access Control List (ACL)
- ☐ Low overhead / High throughput
- ☐ Inexpensive

•Stateful (Dynamic):

- ☐ Keeps track of connection state in order to make decisions
- ☐ Higher overhead / Lower throughput
- ☐ More costly

2. Proxy Servers:

- ☐ Application proxy firewall
- ☐ Circuit-level proxy firewall

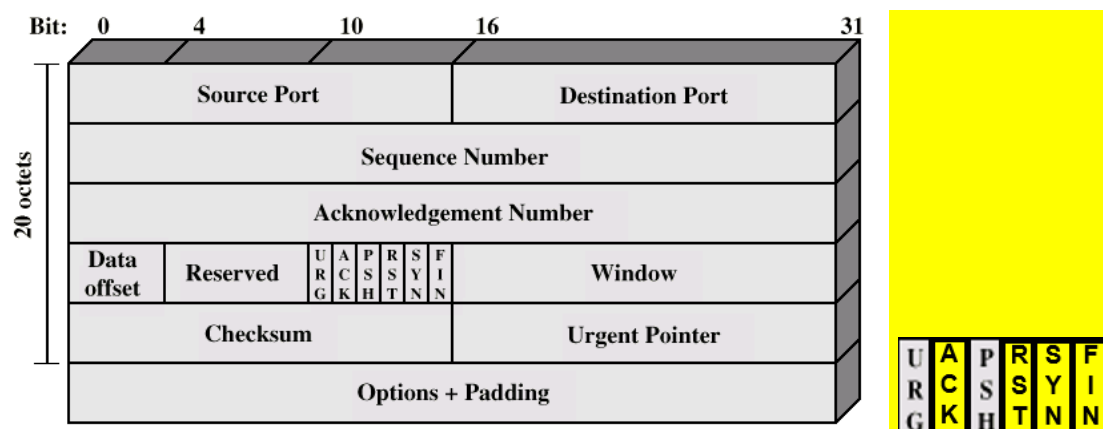
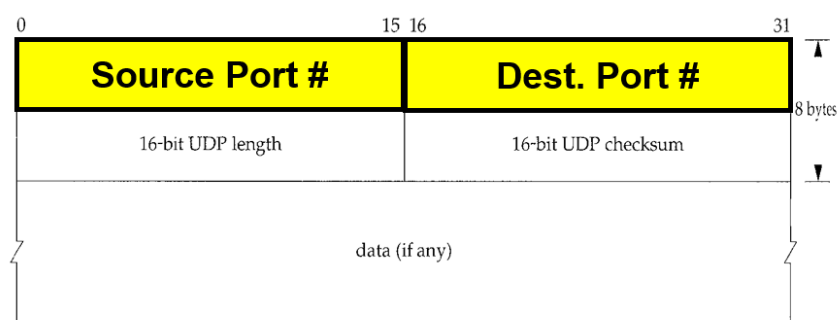
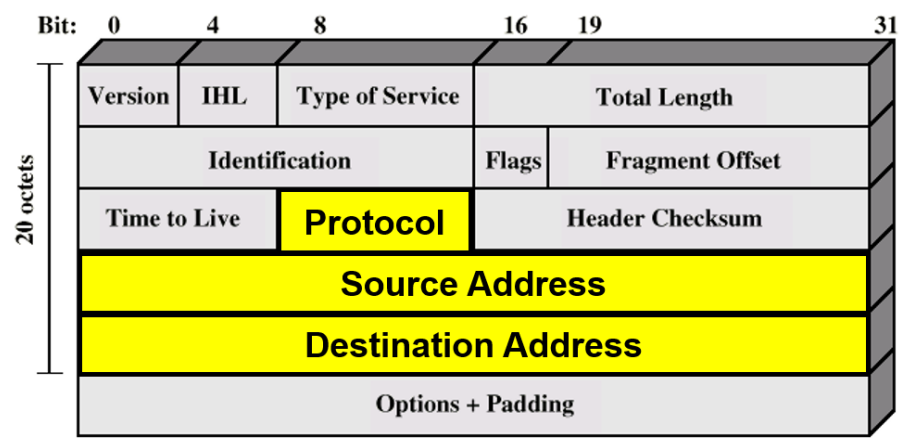
Proxy Server

•Proxy Server (or Application Gateway) acts as surrogates for the real servers at a network site

- Operates at the application layer of the reference model
- Terminates TCP connections both from internal hosts and external hosts, whether client or server
- ☐ Changes IP addresses, port numbers, etc.
- ☐ No direct connection between client and server

• Know what header fields are always considered by packet filters when performing filtering

Stateless Filters



- Understand the difference between the default policy choices

- Implicit Deny

- ☐ All traffic is implicitly blocked unless you explicitly allow it

- Implicit Allow

- ☐ All traffic is implicitly allowed unless you explicitly block it

- Understand how to read/explain as well as create a stateless packet filter rule

- It won't have to be with iptables for this question and will be more general as shown in slides 31 and 33
 - That means you should know the port numbers of the 10 most common services

Rule Creation

- Rules may be implicit or explicit:

- ☐ Implicit

- ☐ Firewall has this rule be default

- ☐ No logging occurs

- ☐ Explicit

- ☐ This rule must be created

- ☐ Logging occurs

Most Popular Default Choice

- Implicit Allow Policy to accept all traffic by default

- Add explicit rules allowing certain traffic to enter

- Add explicit deny at bottom of rule chain to reject all other traffic that isn't explicitly allowed in the prior rules

- If you accidentally flush (delete) all of your firewall rules, Implicit Allow will let you sshback into the firewall and fix your mistake

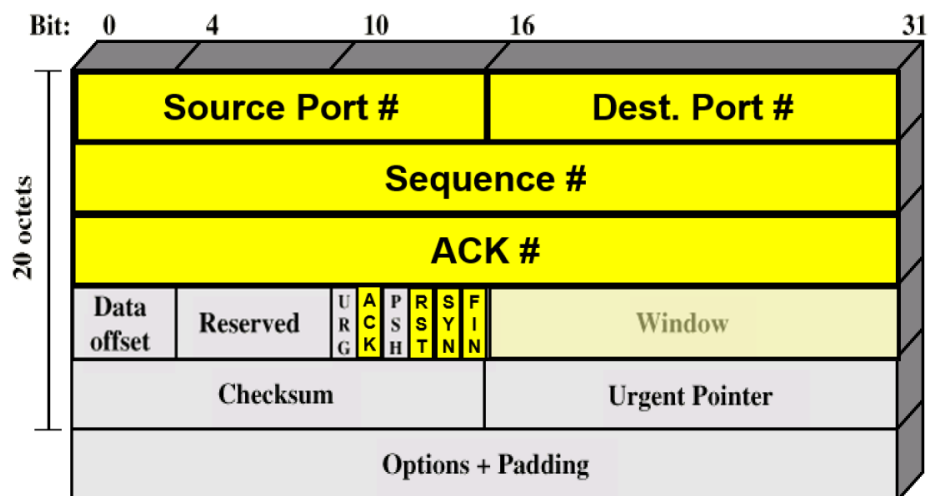
- If you have Implicit Deny set and accidentally flush all of your explicit allow rules, you will not be able to sshin and will have to drive to the site and logon to the firewall console via serial port

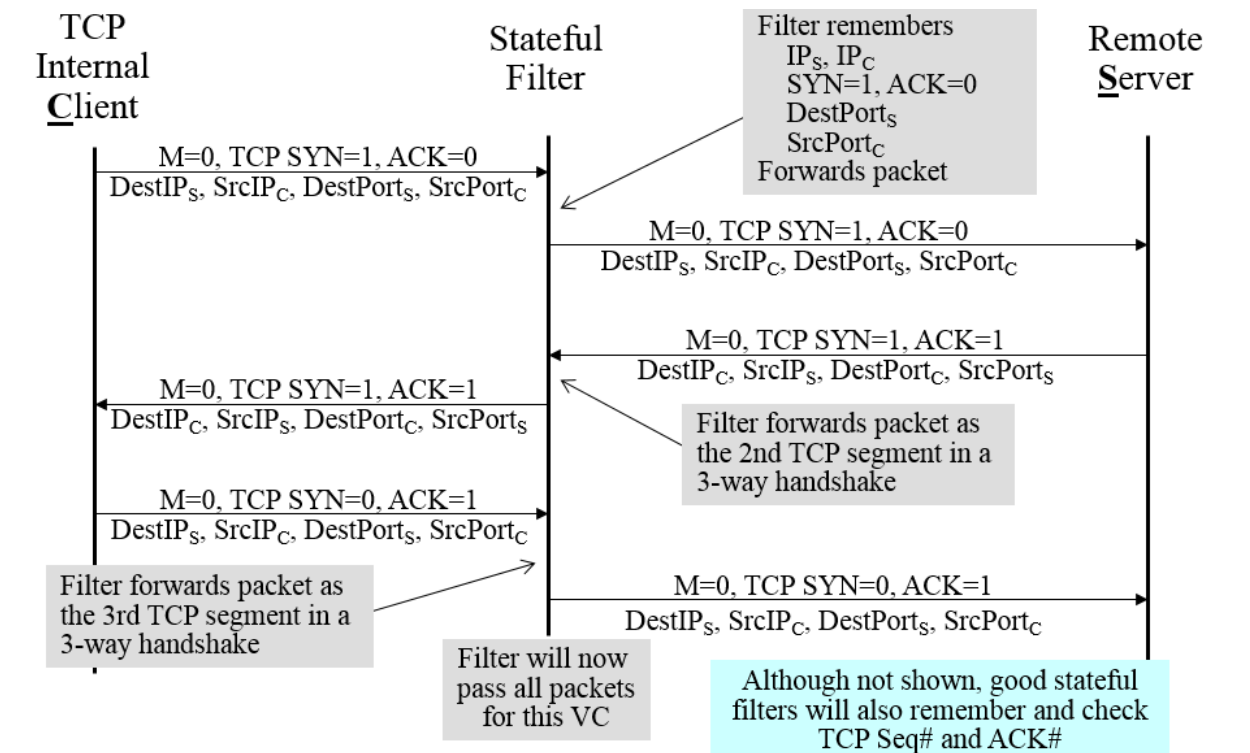
Rule Order	Direction	Protocol	Source IP	Source Port	Dest. IP	Dest. Port	Action
1	OUT	TCP	192.168.1.0/24	ANY	ANY	80	ALLOW
2	OUT	TCP	192.168.1.0/24	ANY	ANY	443	ALLOW
3	OUT	UDP	192.168.1.0/24	ANY	ANY	53	ALLOW
4	OUT	ANY	ANY	ANY	ANY	ANY	DROP
5	IN	TCP	ANY	80	192.168.1.0/24	ANY	ALLOW
6	IN	TCP	ANY	443	192.168.1.0/24	ANY	ALLOW
7	IN	UDP	ANY	53	192.168.1.0/24	ANY	ALLOW
8	IN	ANY	ANY	ANY	ANY	ANY	DROP

•All clients on the subnet 192.168.1.0/24:

- ☐ Can connect to any web server on the Internet via ports 80 and 443
- ☐ Can query any DNS server on the Internet via port 53
- ☐ Can receive replies from any server on the Internet that uses ports 80 and 443
- ☐ Can receive responses from any DNS server on the Internet that uses port 53

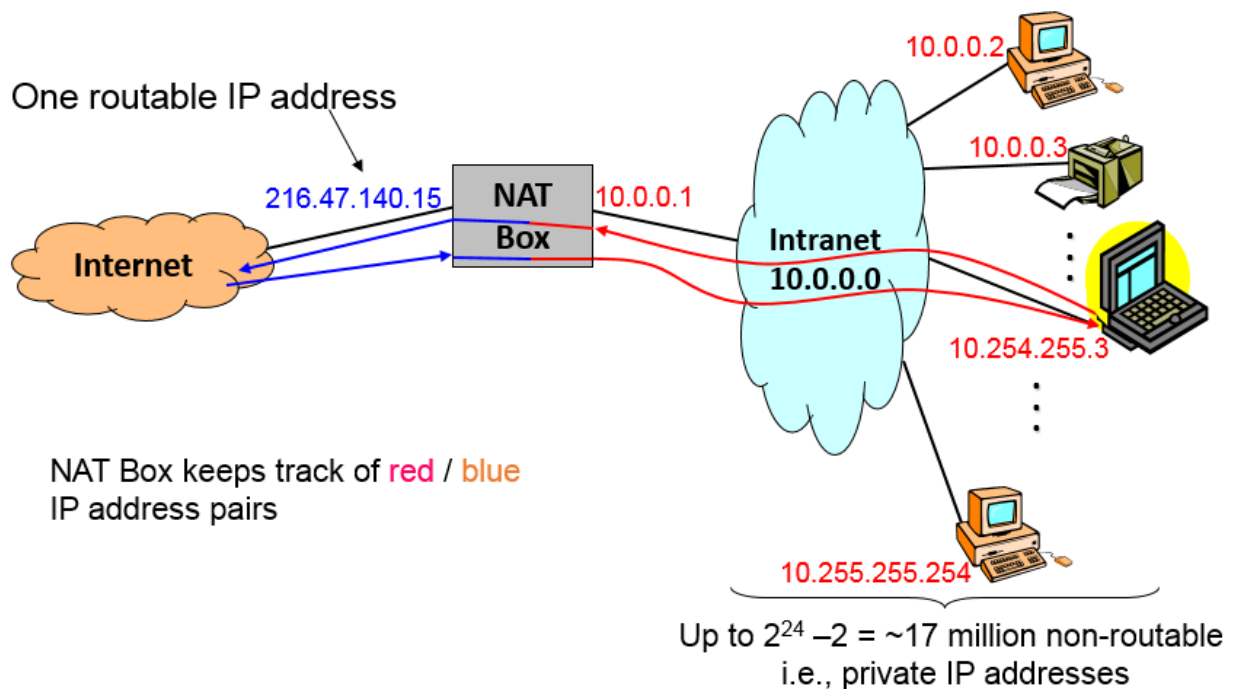
•Understand what header fields stateful packet filters evaluate





• Understand NAT and how it works

• Network Address Translation (NAT) is a function that translates all local Intranet IP addresses to a single Internet address and visa versa



NAT Box as a Firewall*

- Remote hosts on the Internet don't know what addresses are behind the NAT Box
- But it's reasonable to assume that there might be private (aka non-routable) addresses behind a NAT box. Would this do the attacker any good?
 - ☐ Non-routable IP addresses should be dropped by properly configured routers
 - ☐ So if an attacker tries to target a private address, routers should drop the attack packet(s)
 - ☐ Therefore the attack packet will never get to the target
- But unfortunately routers are sometimes improperly configured to route the non-routable IP addresses
- Must NAT Boxes be stateful? ☐ Yes!
- How can malware get into the Intranet through a NAT Box?
 - ☐ Via packet payloads such as email, ftp etc.
 - ☐ Also TCP hijacking

• iptables Hierarchy is:

☐ Tables (lower case name)

☐ Chains (upper case name)

☐ Rules

• Understand the difference between the iptables rule actions (ACCEPT, REJECT, DROP)

☐ ACCEPT

o Packet is accepted through the firewall into the system.

☐ REJECT

o Packet is rejected and ICMP or TCP response is returned to sender.

☐ DROP

o Packet is rejected and no response is returned.

• Understand the difference between the NEW, ESTABLISHED, and RELATED states for ctstate in iptables

• --ctstate

□ List of the connection states to match

```
NEW      meaning that the packet has started a new connection, or otherwise associated with a connection which has not seen packets in both directions, and

ESTABLISHED
          meaning that the packet is associated with a connection which has seen packets in both directions,

RELATED
          meaning that the packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer, or an ICMP error.
```

• Be able to read/explain a few iptables stateful chain rule entries

• **sudo iptables -A INPUT -i eth0 -j DROP**

• **sudo iptables -A OUTPUT -o eth0 -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT**

• **sudo iptables -A OUTPUT -o eth0 -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT**

• **sudo iptables -A OUTPUT -o eth0 -p udp --dport 53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT**

• **sudo iptables -A INPUT -i eth0 -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT**

• **sudo iptables -A INPUT -i eth0 -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT**

• **sudo iptables -A INPUT -i eth0 -p udp --sport 53 -m conntrack --ctstate ESTABLISHED -j ACCEPT**

Week 12 –IDS/IPS

•Be able to define the six items on the “Terminology” slides

•Host-based IDS (HIDS):

- ☐ Monitors events between single host and network gateway

•Network-based IDS (NIDS):

- ☐ Monitors network traffic for particular network segment

•Sensors:

- ☐ Responsible for collecting data such as packets, log files, etc.
- ☐ Data is then sent to the analyzer

•Analyzers:

- ☐ Receive input from one or more sensors or from other analyzers
- ☐ Is responsible for determining if an intrusion has occurred

•User Interface:

- ☐ Allows analyst to view output from IDS and/or control the behavior of the system

•Intrusion Prevention System (IPS):

- ☐ Ability to not only detect but also prevent an attack

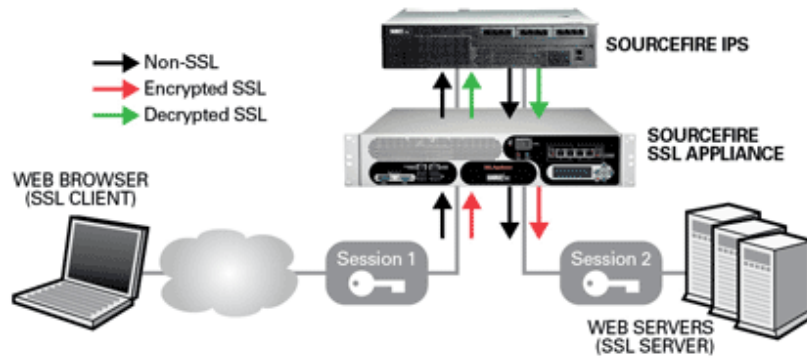
•Understand anomalies 反常 an IDS/IPS may detect

- ☐ Login frequency
- ☐ Time since last login
- ☐ Quantity of output
- ☐ Session resource utilization
- ☐ Password failures at local login and remote logins
- ☐ Command execution frequency
- ☐ Program resource utilization
- ☐ Execution denials.
- ☐ Read, write, create, delete frequency and failures
- ☐ Read, write of sensitive data locations

• Understand the difference between inline and passive sensors and what devices may be used for each

• **Inline Sensor**

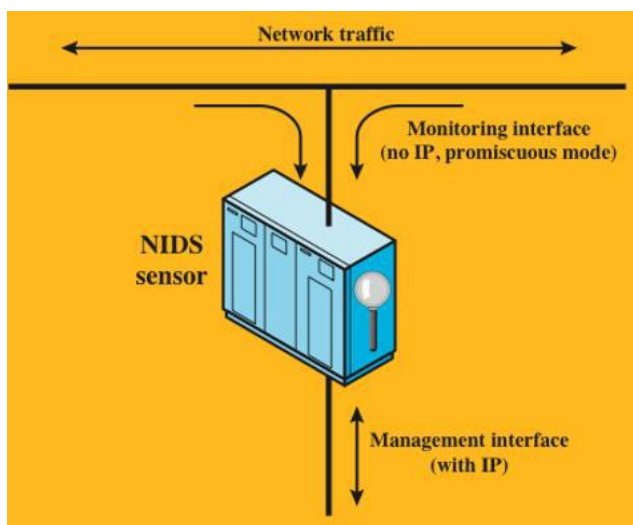
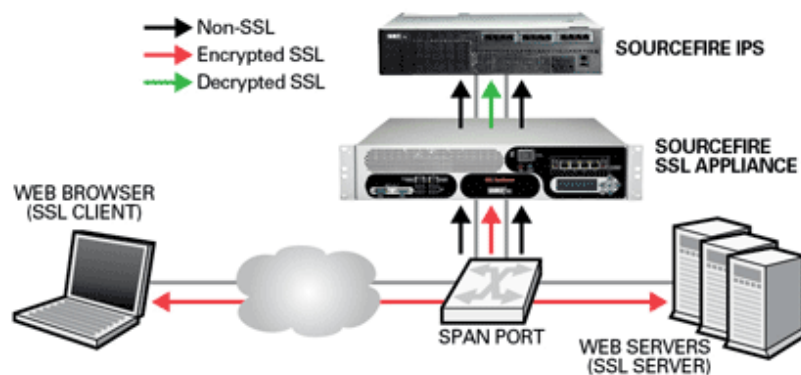
□ Traffic passed through the sensor



• **Passive Sensor**

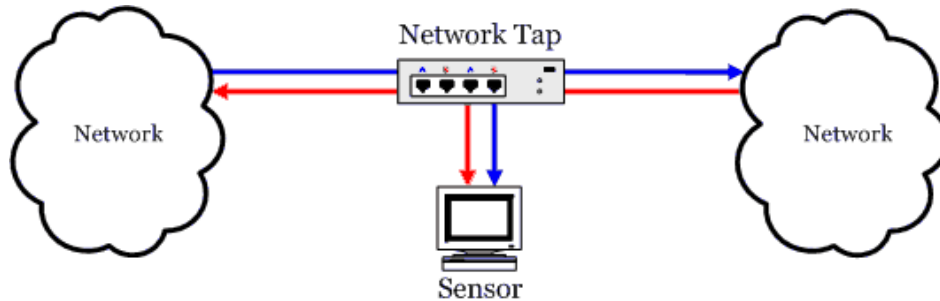
□ Traffic does not pass through the sensor

□ Monitors copy of traffic

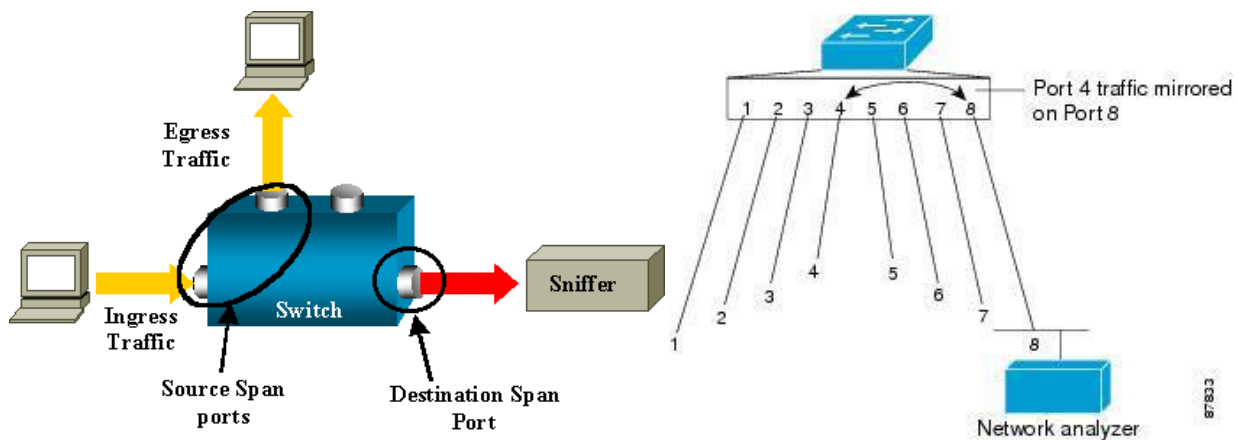


•May use:

☐ Network TAP



☐ Switch SPAN port



•Sensor Server usually needs 3 interfaces

☐ Ingress

☐ Egress

☐ Monitor

•Know the NIDS sensor placement choices and the advantages/disadvantages of each

NIDS/Sensor Placement Choices

•Behind the firewall

☐ Records all traffic that passes successfully through the firewall

☐ Requires dedicated server for NIDS sensor

1. In front of the firewall

☐ Records all inbound traffic

2. What are some disadvantages of in front placement?

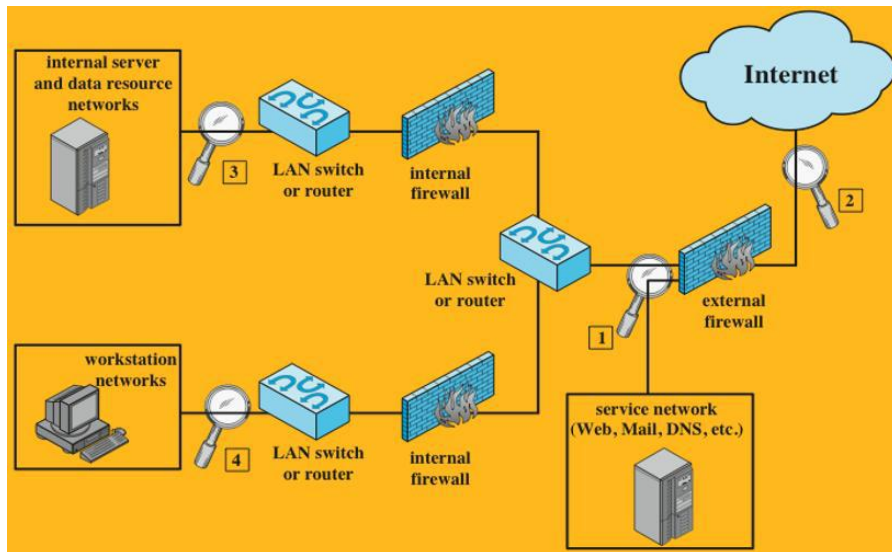
- ☐ Noisy since records all inbound traffic
- ☐ Hard to tell if an intrusion is successful as the firewall may block the attempt
- ☐ Requires dedicated server for NIDS sensor

3. In front of server networks

- ☐ Can set specific rules for server OS

4. In front of workstation networks

- ☐ Can set specific rules for workstation OS



1. Behind the firewall

2. In front of the firewall

3. In front of server networks

4. In front of workstation networks

• Know what a Honeypot is and its placement choices

Honeypot

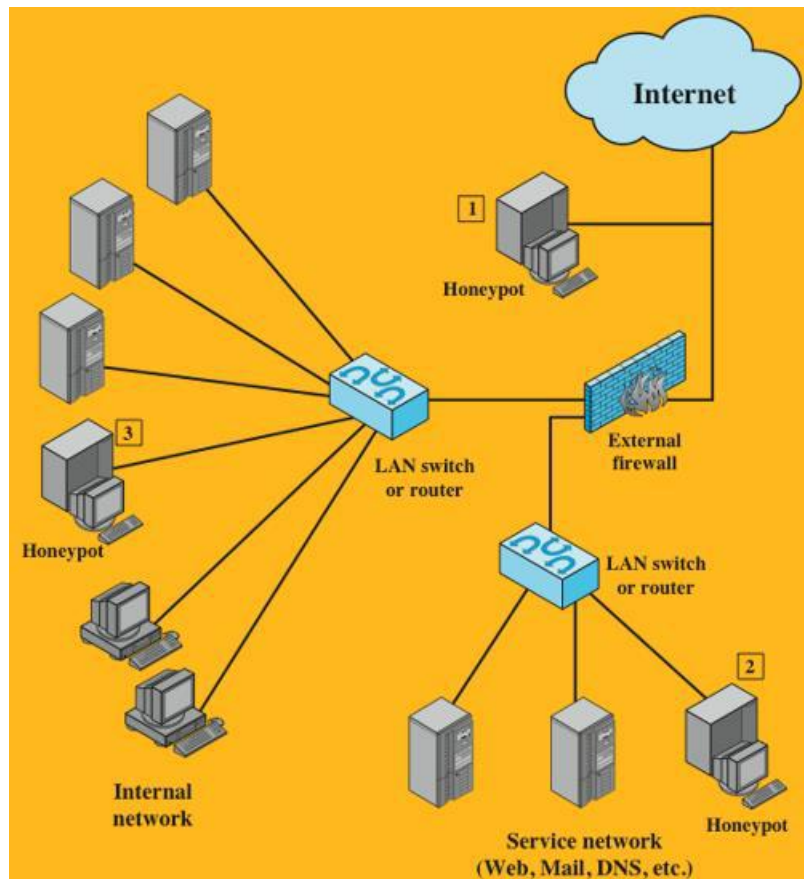
• Decoy system designed to:

- ☐ Lure a potential attacker away from critical systems
- ☐ Collect information about the attacker's activity
- ☐ Encourage the attacker to stay on the system long enough for administrators to respond

• Filled with fabricated information that appears valuable

- One attackers are in the honeypot, administrators can observe their behavior to figure out defenses

Honeypot Deployment



•Note:

- ☐ It can be dangerous to place a honeypot outside of the firewall
- ☐ Why???
- oCould be used as a launching pad for attacks on other organizations
- ☐ Why can't a honeypot inside the firewall attack other organizations???
- oThe firewall can stop outbound traffic from the honeypot

• Understand Snort's two modes and submodes

Snort can be used as an IDS or IPS

• Active

- ☐ Inline: Acts as IPS and forwards/denies all traffic based on ruleset
- ☐ Offline: Acts as pseudo IPS and monitors traffic but has ability to deny some traffic through sending RST or ICMP error messages

• Passive

- ☐ Inline: Acts as IDS and allows all traffic to pass through
 - ☐ Offline: Acts as IDS and watches copy of traffic from switch SPAN port or network TAP.
- **Most popular deployment****

• Be able to identify the header parts and option parts of a Snort rule

```
✓ Show Packet Data  ✓ Show Rule
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Possible CrimeBoss Generic URL Structure"; flow:established,to_server;
content:".php?action=iv&h="; http_uri; classtype:bad-unknown; sid:2016558; rev:3;)
/nsm/server_data/securityonion/rules/admin1-VirtualBox-eth1-1/downloaded.rules: Line 1849
```

• Rule Header

• Rule Options

```
alert tcp 192.168.1.15 5858 -> 121.14.1.2 80 (msg:
"Info here"; reference: url,http://whateversite.com;
content: "cb.php"; flow:to_server; nocase; sid:
1000001; rev:1)
```

•alert: Generate an alert and then log the packet

•tcp: Protocol (TCP, UDP, ICMP, IP)

```
alert tcp 192.168.1.15 5858 -> 121.14.1.2 80
      SrcIP      SrcPort  DestIP  DstPort
```

*\$HOME_NET can also be used as the SrcIP and is a variable in Snort for all private network ranges (Class A, B, and C)

Week 13 –User Authentication & Access Control

•Understand the four means of authenticating a user

•Something you know:

- ☐ Password, Pin, Security Question Answers

•Something you have:

- ☐ Token, Smartcard, Physical Key

•Something you are:

- ☐ Fingerprint, Retina, Iris, Facial Geometry, Hand Geometry

•Something you do:

- ☐ Voice Pattern, Handwriting, Typing Rhythm

•Understand how traditional password authentication works

- Admin creates user account on a server and assigns a user ID and password for the user
- Password is hashed with a one-way function and stored in a protected file on the server
- User enters User ID and password and submits it to authenticate
- Server takes password and performs one-way function to generate hash
- Generated hash is compared against the stored hash
- If they match, user is allowed access to the server

•Be able to define the five methods to crack a password

•Online Attack

- ☐ Use the system's logon mechanism to attempt to crack the password by continually submitting guesses

- ☐ Easy for security admins to catch in logs

•Offline Attack

- ☐ Steal the protected password list and crack the hashes offline

- ☐ Easier for attacker to hide their tracks

Methods to Crack a Password

•Dictionary Attack:

- ☐ Crack program has a large wordlist of most every word in the dictionary

- ☐ Will not crack the password if it is not in the wordlist

- ☐ Can use rules to enhance guesses

- o Capitalize first letter of word

- o Append words with numbers

- o Replacing S with \$, a with @, O with 0, i with !, etc.

- ☐ Fast

Methods to Crack a Password

•Brute Force Attack:

- ☐ Tries every combination

- oa, b, c, d...z; aa, ab...az;ba, bb...bz, etc.

- ☐ Will eventually crack any password

- ☐ Much slower and may take hundreds of years depending on length and complexity of password

•Lookup Table:

- ☐ Takes a wordlist and pre-calculates all of the hashes and stores them in a table

- ☐ Very fast

- ☐ Tables are huge

- ☐ Example is crackstation.net

- o Extracted every word from Wikipedia and from many password lists

- o For MD5 and SHA1 hashes, they have a 15-billion entry lookup table

•Reverse Lookup Table:

- ☐ So far the cracking methods haven't been concerned with the usernames

- ☐ This method uses a Lookup Table but also keeps track of which usernames are mapped to which hashes

- ☐ When a password hash is cracked, all users that had that same password are displayed

- ☐ Very fast

•Rainbow Table:

- ☐ Doesn't include all of the pre-calculated hashes

- ☐ Uses reduction function to reduce table size that is considerably smaller than a Lookup table

•Understand what a salt is and how it can prevent an attacker using lookup or rainbow tables

- A random string prepended or appended to the password before it is hashed

- Should you use the same salt for each password or a different salt?

- ☐A different salt

- Why???

- ☐If the same salt were used, the attacker could simply create a new lookup table with hashes pre-calculated with that salt

- Also, you should have a longer salt (8 characters or more)

- Why??

- ☐If a small salt such as 2 or 3 digits was used, the attacker could simply brute force it as well

- So now we know that a longer random salt can effectively stop lookup and rainbow tables

- Can a random and long salt also stop the use of dictionary and brute force cracking methods???

- ☐No

- Why Not???

- ☐In an online attack, the authentication function will add the correct salt automatically to the dictionary or brute force guesses

- ☐In an offline attack, the attacker already has the salt in the stolen file that contains the password hashes

•Understand the current Unix/Linux shadow file format for password entries and why the shadow file is more secure

- The password entry in /etc/passwd is replaced with an "x"

- The hashed password is put into /etc/shadow file

- So in /etc/passwd we have

loginName: x: uid: gid: userInfo: homeDirectory: loginProg

- Examples of /etc/passwd accounts

student: x: 1001: 1001: student: /home/student: /bin/bash

root: x: 0: 0: root: /root: /bin/bash

- In the **/etc/shadow** file there is for each login name the following line format:

```
loginName : passwordHash : #days_since_last_changed
: #days_before_may_be_changed : #days_after_which_must_be_changed
: #days_to_warn_user_of_expiring : #days_after_expired_account-disabled :
#days_since_account_disabled : reserved_files
```

- **Examples**

```
lidinsky:Qp47caKps8tN:723:0:99999:7:::
student:$1$3mkY0$edjui.5DE7bYn/F8v25s:14076:0:99999:7:::
root:$1$w6jJr$7jsF0g7za9J//ul9Wul:14076:0:99999:7:::
```

Linux Password Hash Format

• **\$1\$w6jJr\$7jsF0g7za9J//ul9Wul**

- \$ is delimiter

- 1st field is hashing algorithm used:

- ☐ \$1 = MD5
- ☐ \$2 = Blowfish
- ☐ \$5 = SHA-256
- ☐ \$6 = SHA-512

- 2nd field is salt value

- ☐ w6jJr

- 3rd field is hash of salt and plaintext password together

- ☐ 7jsF0g7za9J//ul9Wul

- **Why are hashed passwords are more secure in the /etc/shadow file???**

- ☐ By default, only the root user may access it.

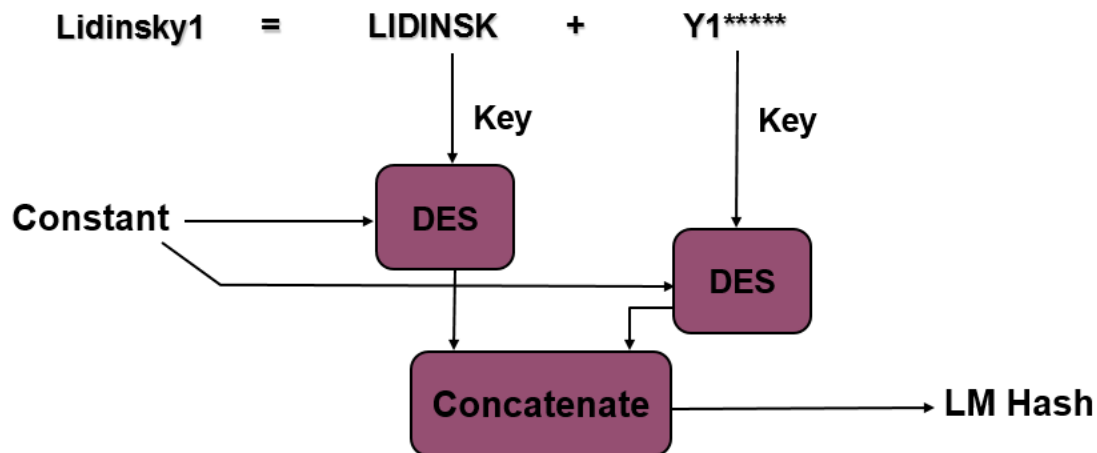
• Know the difference between LM and NT hash generation and where they are both stored

☐ LM or LM Hash

- Passwords <=14 characters or bytes are padded with nulls
- To each 7-byte part an odd parity byte is added
- This 8-byte value becomes a DES key
- DES is used with a fixed salt to create each 8-byte hash
- The two hashes are concatenated together to create the 16-byte LM hash
- LM provides rather weak hashing

LM Hash Generation

- Converted to upper case
- Padded with NULL to 14 characters
- Separated into two 7 character strings which are hashed separately

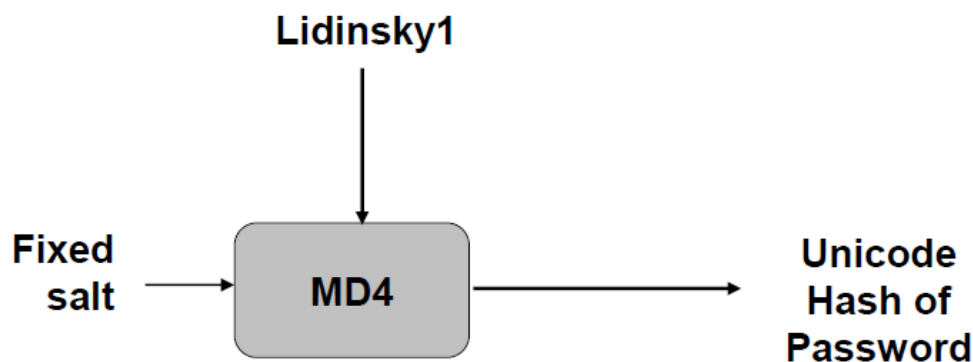


☐ NT or NT Hash

- NT hash allows alphanumeric characters & symbols (☐)
- ☐ Characters and symbols are represented as Unicode
- Keeps both lower and upper case characters (☐)
- Does not split up the plaintext password (☐)
- But still uses a fixed salt (☐)
- Creates a 16-byte hash

NT Hash Generation

- Just hash the password
- Then store it



- From Win2K forward the two hashes are both calculated and stored in the SAM (Security and Account Manager) part of the registry

- There are ways to eliminate the LM hash

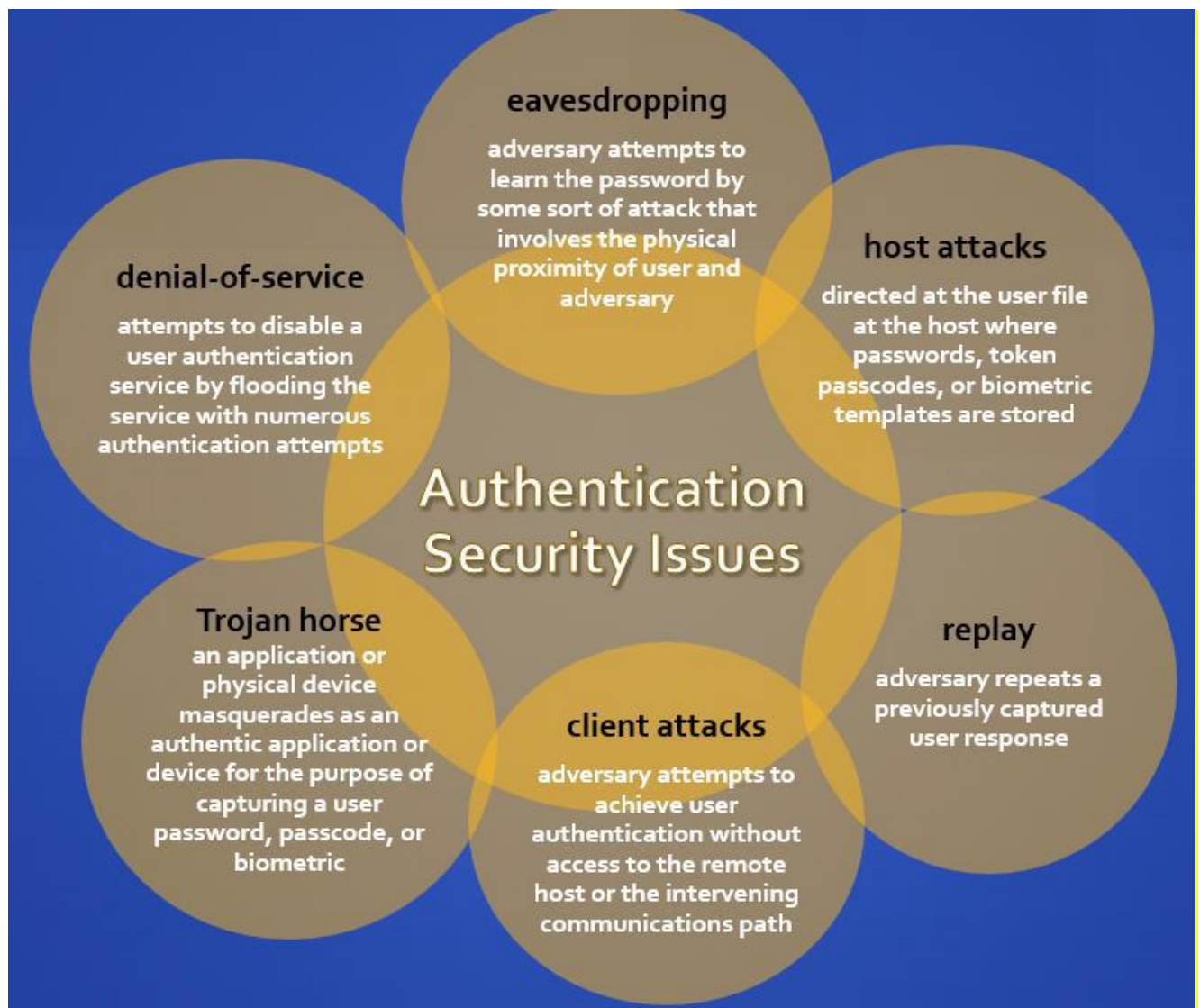
- But then backward compatibility is compromised

- Windows stores encrypted password hashes in the Windows Registry

- Need special tools to extract passwords and other account information

- e.g., pwdump, pwdump2, pwdump3, samdump...

- Know what the six general authentication security issues are



Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

•Understand what components a Kerberos environment consists of

•Kerberos environment consists of:

□Key Distribution Center (KDC) contains:

oUser Database

oAuthentication Server (AS)

oTicket Granting Server (TGS)

□Kerberos-Aware Application Servers

□Clients registered with KDC

•Understand what a Ticket Granting Ticket (TGT) does

What is the difference between a Kerberos ticket granting ticket and a service granting ticket?

A ticket-granting ticket (TGT) is created by a Kerberos-aware Application Server to begin the authentication process. After the client receives the TGT, it will add some other information which can verify the user. This TGT will be sent to a Ticket Granting Server (TGS). After TGS decrypts the TGT and verifies everything which it needs to check, it will issue a service granting ticket (SGT). The SGT and a session key (which includes a form of password) are sent back to the client and open the Application Server (AS).

The big difference between these two tickets is TGT is added the information by the client and SGT is added by the server. The attacker can get the copy of TGT but could not get the SGT. Then, the attacker cannot hacker into the AS.

TGT allows authenticated user to request tickets to access application servers.

User can use TGT to request a SGT for access to a specific application server.

•Understand how to change permissions via letters and numbers

- You will need to provide the full command on a few scenarios for each

Letter:

File Type:

-indicates test6 is a regular file

d would indicate a directory

•Only the owner of the file can change permissions of it

rwx rwx rwx

↑ ↑ ↑
User Group Others

Permission	File	Directory
Read	View what's in the file.	See what files and subdirectories it contains.
Write	Change the file's content, rename it, or delete it.	Add files or subdirectories to the directory. Remove files or directories from the directory.
Execute	Run the file as a program.	Change to the directory as the current directory, search through the directory, or execute a program from the directory. Access file meta data (file size, time stamps, and so on) of files in that directory.

1. Changing Permissions Via Letters

- Change permissions via letters with `chmod` command

☐ Turned on with plus (+) and off with minus (-)

☐ Bit sets are designated by **u = user** **g = group** **o = other** **a = all users**

(u = user is really the “Owner”)

☐ **`chmod a+x testfile1`**

2. Changing Permissions Via Numbers

- Each permission is assigned a number.

r = 4 **w = 2** **x = 1** **no permission = 0**

- Example: `rWX rW- r--`

 owner group other
 because (4+2+1) (4+2+0) (4+0+0)
 Permissions = 7 6 4

- Know why you would need to ever set an ACL in Linux

Allow other groups users to read or execute the file.

```
$ getfacl testfile1
# file: testfile1
# owner: bduggan
# group: sales
user::rwx
group::-
other::-
```

- **Syntax: `setfacl -m u:username:perms filename`**

- Explanation:

- ❑ m indicates setting an ACL.
- ❑ u indicates setting ACL permission for a user.
- ❑ username is the account to assign the ACL permission.
- ❑ perms are the ACL permissions, options allowed read(r), write(w), execute (x).
- ❑ filename is the file setting ACL permissions on.

• **setfacl -m u:jerry:r testfile1**

```
-rwxr-----+ 1 bduggan sales 0 Nov 15 00:33 testfile1
```

```
$ getfacl testfile1
# file: testfile1
# owner: bduggan
# group: sales
user::rwx
user:jerry:r--
group::---
mask::r--
other::---
```

Even though jerry is not in the owner group, he can still read this file due to the ACL

Week 14 –Computer Forensics

•Understand the three federal laws involving computer forensics

Computer Fraud and Abuse Act (CFAA)

•Gain unauthorized access to a “protected” computer:

- ☐To harm U.S. or benefit foreign nation
- ☐To obtain protected financial or credit information
- ☐With intent to defraud
- ☐To damage it (malware, etc.)
- ☐To engage in trafficking of computer passwords
- ☐To threaten it with intent of extorting money

Electronic Communications Privacy Act (ECPA)

- Illegal to intercept stored or transmitted electronic communication without authorization
- Includes any transfer of signs, signals, writing, images, sounds, data, or intelligence transmitted in whole or in part by wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce.

Digital Millennium Copyright Act (DMCA)

•Prohibits circumventing a technological measure designed to protect a copyright

•Examples:

- ☐Keygens
- ☐Circumventing DVD anti-piracy measures
- ☐Accessing online videos without permission
- ☐Reverse engineering of software
- ☐Etc.

•Understand the differences between allocated/unallocated space and partitioned/non-partitioned space and what items may be found or not found in each

Allocated vs. Unallocated Space

•Allocated

- ☐Active files on the filesystem that may be in use
- ☐Doesn't include deleted files

- ☐ Most evidence found here
- Unallocated
- ☐ Free Space
- ☐ Non-active files
- ☐ Deleted files or fragments of former files found here
- ☐ Some evidence occasionally found here

Partitioned vs. Un-partitioned Space

- Partitioned Space
 - ☐ Holds a filesystem
 - ☐ Can be used as a volume to store files or can hold an Operating System
 - ☐ Identified by logical drive letters C:, D:, etc.
- Un-partitioned Space
 - ☐ Space on disk not in use and not occupied by a partition

• Know the different types of evidence acquisition imaging methods and how they work

• Physical Drive Images

- Bit by Bit copy of entire physical hard drive
- Contains allocated and unallocated space
- Contains partitioned and un-partitioned space
- Contains deleted files, fragments of files, etc. from entire disk
- Contains file system metadata

• Logical Drive Images

- Bit by Bit copy of drive partition only such as C:
- Contains only contents from partitioned space
- Contains allocated and unallocated space only from selected partition
- Contains deleted files, fragments of files, etc. only from selected partition
- Contains file system metadata

*FTK Imager option. Some software's logical images may not contain unallocated space or deleted files

•Contents of a Folder

- Only contains active files in a folder
- Also, sometimes referred to as a “Logical Image” which can lead to confusion
 - ☐Not the same thing as a “Logical Drive Image”
- Not a bit by bit copy
- Does not contain unallocated space, deleted files, file fragments, filesystem metadata, etc.

•Memory Acquisition

- Collection of volatile memory (RAM) from running system
- May contain information on:
 - ☐Encryption Keys
 - ☐Malware / Root Kits
 - ☐Open Files
 - ☐Network Connections
 - ☐Running Processes
 - ☐Etc.

•Be able to explain the differences of Dead vs. Live Acquisitions

- Dead Acquisition:
 - ☐Computer is off when you arrive
 - ☐Don't turn it on
 - ☐Drive is removed and physical image is taken
- Live Acquisition:
 - ☐Computer is running
 - ☐What you do next is dependent on a few things...
- The old standard was to pull the plug on a running computer, take out the drive, and perform a physical image on it
- Why wouldn't we want to do that now???
- ☐We would lose all of the artifacts in memory that are volatile and would disappear!
- ☐Computer might also have full disk encryption and examiner wouldn't be able to logon when restarting it but could have grabbed the decryption key from RAM while the system was running

- Always check to see if a system has full disk encryption before shutting it down
- If you are certain it is not encrypted:
 - ☐ Capture the RAM anyways for other artifacts
 - ☐ Shut down the computer, pull the drive, and take a physical image of it
- If system's drive is encrypted:
 - ☐ Capture the RAM and the Protected Registry Files
 - ☐ Perform a "Logical Drive" image or "Export to Logical Image" (for files/folders) with FTK and you will capture the unencrypted data
- There might be also be times where you encounter a non-encrypted computer or server that cannot be shut down
- Then, you would:
 - ☐ Capture the RAM and Registry Files with FTK
- oRegistry files cannot be copied from a live running system through the Windows OS
- ☐ Use FTK to perform a physical drive, logical drive, or logical folder image.
- Note, that FTK does allow you to use their "Physical Drive" image function on a live system
- However, if encrypted, you will simple have an image of the encrypted data

•Know some or the potential questions forensic analysis can answer

- Was a computer used to:
 - ☐ Transmit malware?
 - ☐ Open a specific file?
 - ☐ Send a specific email or emails?
 - ☐ Steal information onto a USB key?
 - ☐ Used in a hacking attack and connected to a specific access point?
 - ☐ Search the internet for specific terms?
 - ☐ Download restricted information or images?

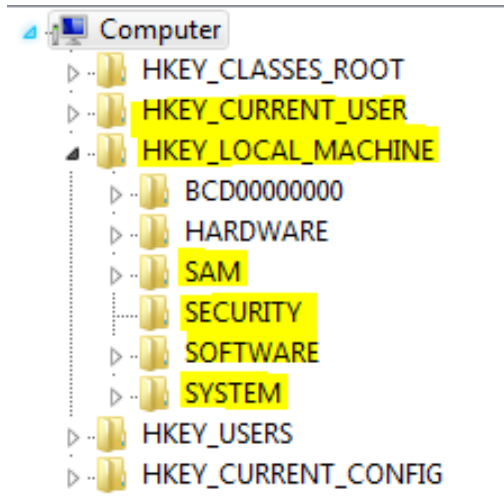
•Understand the main tasks we performed with EnCase

String Searching

Internet Records

Other Artifacts

- Understand the differences in the registry and internet artifact tools



RegRipper

Plugin File

regripper reports

- Go ahead and run regripper on the software and system hives
- Choose the correct path for each hive file
- Create a report file with the same name as the hive like before and store in the regripperreports folder
- Choose the correct plugin for each

• IE History

XP: %userprofile%\Local Settings\History\History.IE5\index.dat

Vista+: %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

• Firefox History

XP: %userprofile%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite

Vista+: %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite

• Chrome History

XP: %userprofile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History

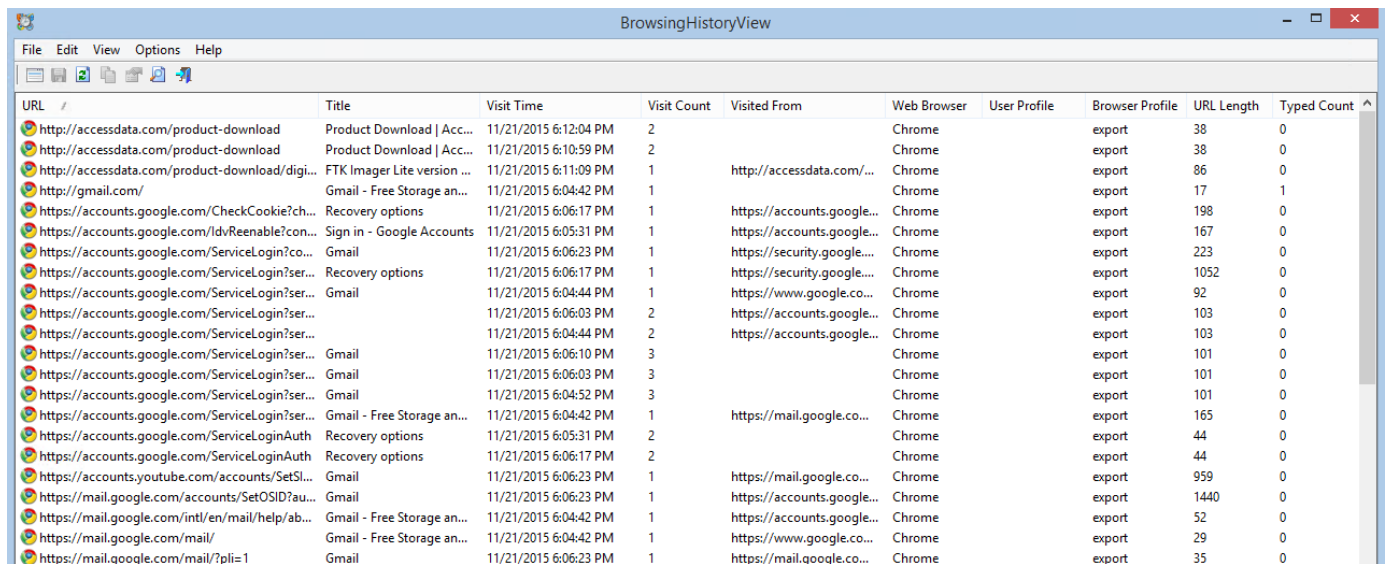
Vista+: %userprofile%\AppData\Local\Google\Chrome\User Data\Default\History

Browser Forensics Interesting Items

- History
- Cookies

- Cache
- Session Restore
- Flash/Super Cookies
- Download History
- Auto-Complete/Form History
- Installed Extensions

We are going to use EnCase to export the browser history file for Chrome



URL	Title	Visit Time	Visit Count	Visited From	Web Browser	User Profile	Browser Profile	URL Length	Typed Count
http://accessdata.com/product-download	Product Download Acc...	11/21/2015 6:12:04 PM	2		Chrome		export	38	0
http://accessdata.com/product-download	Product Download Acc...	11/21/2015 6:10:59 PM	2		Chrome		export	38	0
http://accessdata.com/product-download/digi...	FTK Imager Lite version ...	11/21/2015 6:11:09 PM	1	http://accessdata.com/...	Chrome		export	86	0
http://gmail.com/	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1		Chrome		export	17	1
https://accounts.google.com/CheckCookie?ch...	Recovery options	11/21/2015 6:06:17 PM	1	https://accounts.google...	Chrome		export	198	0
https://accounts.google.com/ldvReenable?con...	Sign in - Google Accounts	11/21/2015 6:05:31 PM	1	https://accounts.google...	Chrome		export	167	0
https://accounts.google.com/ServiceLogin?co...	Gmail	11/21/2015 6:06:23 PM	1	https://security.google...	Chrome		export	223	0
https://accounts.google.com/ServiceLogin?ser...	Recovery options	11/21/2015 6:06:17 PM	1	https://security.google...	Chrome		export	1052	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:04:44 PM	1	https://www.google.co...	Chrome		export	92	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:06:03 PM	2	https://accounts.google...	Chrome		export	103	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:04:44 PM	2	https://accounts.google...	Chrome		export	103	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:06:10 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:06:03 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail	11/21/2015 6:04:52 PM	3		Chrome		export	101	0
https://accounts.google.com/ServiceLogin?ser...	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://mail.google.co...	Chrome		export	165	0
https://accounts.google.com/ServiceLoginAuth	Recovery options	11/21/2015 6:05:31 PM	2		Chrome		export	44	0
https://accounts.google.com/ServiceLoginAuth	Recovery options	11/21/2015 6:06:17 PM	2		Chrome		export	44	0
https://accounts.youtube.com/accounts/SetSI...	Gmail	11/21/2015 6:06:23 PM	1	https://mail.google.co...	Chrome		export	959	0
https://mail.google.com/accounts/SetOSID?au...	Gmail	11/21/2015 6:06:23 PM	1	https://accounts.google...	Chrome		export	1440	0
https://mail.google.com/intl/en/mail/help/ab...	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://accounts.google...	Chrome		export	52	0
https://mail.google.com/mail/	Gmail - Free Storage an...	11/21/2015 6:04:42 PM	1	https://www.google.co...	Chrome		export	29	0
https://mail.google.com/mail/?pli=1	Gmail	11/21/2015 6:06:23 PM	1	https://mail.google.co...	Chrome		export	35	0

- Be familiar with common items found in memory captures

FTK Imager can be used to capture memory from a live system

- Allows analyst to look at artifacts such as:

- ☐ Which processes were running
- ☐ Open network connections
- ☐ Executed commands

Week 15 –Wireless Network Security & Attacks

- Understand the difference between a Wireless Router and a Wireless Access Point

Typical Wireless Router

- Public interface connects to modem
- Serves as network gateway
- Single, dual, or triple band wireless radio(s)
- 4-port wired switch
- DHCP server & NAT
- ☐Hands out private IP addresses to connected clients

Typical Wireless Access Point

- AP's switch interface connects to network switch
- Does not serve as network gateway
- No DHCP server or NAT
- Single, dual, or triple band wireless radio(s)
- AP Receives its IP address from network DHCP server
- Wireless clients connected to the AP receive their IP addresses from network DHCP server

- Be able to define each of the IEEE 802.11 architecture terms

802.11 Media Access Control (MAC): Addressing, CSMA/CA

•Station (STA)

- ☐The wireless client (laptop, phone, etc.)

•Basic Service Set (BSS)

- ☐Wireless network of one AP supporting one or many clients

•Extended Service Set (ESS)

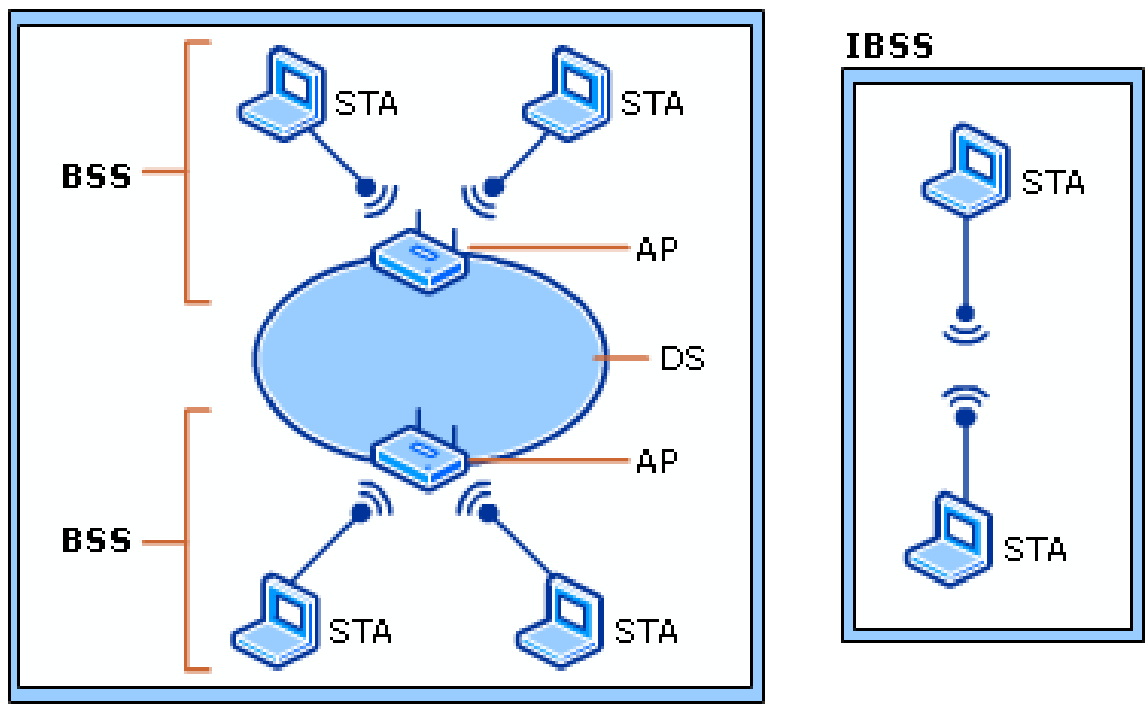
- ☐Two or more BSSs that are connected via a wired network

•Distribution System (DS)

- ☐In an ESS, multiple BSSs are connected by the DS
- ☐Allows a client to move or roam from one BSS to another BSS

•Independent Basic Service Set (IBSS)

- Ad hoc wireless network where clients connect directly to each other (No APs involved)



• Know the differences between the three wireless security protocols

• Wired Equivalent Privacy (WEP)

- Original security protocol for wireless
- Highly insecure due to vulnerabilities
- Encrypts data sent between a client and an AP
- Uses RC4 symmetric stream cipher with 40-bit and 104-bit encryption key options
- Uses Initialization Vector (IV) to randomize keys
- User may enter Passphrase of secure345# for example
- WEP combines secure345# with the IV to create the encryption key
- WEP encrypts packet with key and sends IV to other side in plain text
- Unfortunately, WEP uses small IV and keys are reused
- Attacker generates large amount of traffic to collect ciphertext and plaintext IVs
- Attacker can spoof MAC of a connected client, associate to the AP and generate various traffic
- Attacker can take packet capture of traffic and use cryptanalysis to determine WEP key in a short time

•Wi-Fi Protected Access (WPA)

- Temporary quick replacement for WEP until WPA2 could be finished
- Clients didn't need to upgrade hardware
- Uses RC4 cipher with Temporal Key Integrity Protocol (TKIP)
- TKIP was a little better than WEP but was eventually cracked as well
- Later, strong AES cipher introduced as replacement for TKIP
 - Required software updates
- If you have to use WPA, try to use it with AES only
 - Again, you may have to upgrade software in older clients
- WPA has since been replaced with WPA2
- Client can use Pre-Shared Keys (PSK) or Enterprise Mode to generate master key

•Wi-Fi Protected Access v2 (WPA2)

- Also known as 802.11i
- Also known as IEEE 802.11i as well as Robust Security Network (RSN)
- Replaced WEP and WPA
- Most secure option available currently
- Uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on AES
- Can use 802.1X

•Be able to define each of the common wireless security threats

MAC Spoofing

- Ex: Attacker eavesdrops on network traffic of AP secured by WEP
- Sends disassociation message but is blocked by MAC filtering
- Spoofs own computer with MAC of a client connected to the AP
- Attacker successfully sends disassociation message with spoofed MAC
- Attacker generates other traffic with spoofed MAC and eventually cracks WEP key
- Attacker connects to network using spoofed MAC and WEP key, effectively evading MAC address filtering

Rogue Access Points

- AP placed on a LAN by insider or attacker
- Sometimes hidden in wiring closets or near a window with an open network port
- SSID broadcast often disabled
- Attacker captures traffic in parking lot

Evil Twins

- An AP with the same SSID as a legitimate AP
- Often placed in public free hotspots
 - ☐Coffee Shops
 - ☐Airports
 - ☐Hotels
- Attacker may serve up “logon” web page to capture credentials
- ...or just capture all of the traffic

Ad-Hoc Privileges

- No authentication usually
 - ☐Anyone nearby can connect
- Ex: Two clients connected directly to each other’s wireless cards
 - ☐If client A is logged in as an administrator, client B may have administrative rights to client A’s system
- Connect as a limited privilege user if using Ad-Hoc wireless

MiTM Attacks

- Wireless clients are more susceptible since APs broadcast all traffic
- Can skip flooding a switch, arp spoofing, etc. to be able to see all traffic

DoS

- Attacker continually bombards an AP with traffic
- Attacker can also spoof MAC of AP and send deauthenticationand disassociation frames
- Power Save Exploits
 - ☐Mobile wireless clients can enter sleep state to conserve battery life
 - ☐AP caches traffic until client wakes up

❑ Attacker can send spoofed power save poll message to make the AP transmit and discard the traffic destined for the sleeping client before the client wakes up

• Attacker can circumvent MAC backoff wait time to gain access to a wireless channel before a legitimate device does

• Unintentional DoS can occur if too many neighboring APs are on the same channel

DoS Countermeasures

• Motorola has a Wireless Intrusion Prevention System (WIPS) that can help pick optimum channels and use triangulation to try to find the malicious attacker

• Preventing DoS is difficult on a WLAN

❑ A determined attacker can always disrupt a wireless network

Vulnerable Wireless Drivers

• Can attack client even if not connected to a network!

RADIUS Server Impersonation Attack

• Attacker impersonates AP and RADIUS Server

• Attacker issues rogue certificate to authenticating client

• Client proceeds to authenticate

• Attacker captures authentication traffic and attempts to crack it offline

Anonymity Attacks

• Attack involving an attacker attempting to locate a specific target's Wi-Fi network

• Wireless cards search for preferred networks by name periodically

• Attacker can use a sniffer to capture management frames containing the SSID names

• Additionally, attacker can use Wigleto determine the location of a specific SSID if you know the general location

• Ex: I have seen an SSID named PrettyFly4aWifi downtown a few times

Car Attacks

• Two main methods:

1. Interception and replay of code (if static)

❑ Defense is to use rolling codes

2. Amplification of remote keyless entry signal from car searching for nearby keys

❑ Defense is to put remote in freezer