The Security Threat Landscape

- Threat: has the potential to cause harm to an IT asset.
- Vulnerability: a weakness that compromises the security or functionality of a system.
- Exploit: uses a weakness to compromise the security or functionality of a system.
- Risk: the likelihood of a successful attack.
- Mitigation: techniques to eliminate or reduce the potential of and seriousness of an attack.

Malware

- Malware is malicious software, including:
- Viruses: software which inserts itself into other software and can spread from computer to computer. Requires human action to spread.
- Worms: a self-propagating virus that can replicate itself.
- Trojan horses: malicious software which looks legitimate to trick humans into triggering it. Often installs back doors.
- Ransomware: Encrypts data with the attacker’s key and asks the victim to pay a ransom to obtain the key

Hacking Tools

- Many hacking toolsets are available
- Penetration testers use the same tools as hackers to test for vulnerabilities
- Hacking tools typically run on Linux

Tools include:

- Password cracking tools
- Sniffers
- Ping sweepers
- Port and vulnerability scanners

Attack Types

Script Kiddies and Targeted Attacks

- ‘Script Kiddies’ is a derogatory term for low skilled attackers who download and use off-the-shelf hacking software to launch exploits.
- They will typically attempt to exploit any vulnerable host they can connect to.
- The attacks are mostly not targeted against a particular individual or organisation.
- More skilled attackers will also look for random victims in order to meet their goals, such as installing ransomware or a botnet.
- Organisations are constantly under these type of attacks.

Targeted Attacks

- Targeted attacks are directed against a particular individual or organisation.
- This type of attack is rarer.
- Skilled attackers will typically start off with very stealthy and low impact reconnaissance, and systematically escalate the attack from there.
- Evolution:
  1. External reconnaissance
  2. Initial compromise
  3. Escalation of privileges
  4. Internal reconnaissance
  5. Further compromise
  6. Further escalation of privileges
  7. End goal

Reconnaissance

- Reconnaissance obtains information about the intended victim.
- In a targeted attack the attacker will typically start with completely unobtrusive methods, such as searching whois information, phone directories, job listings etc.
- They will then dig deeper using tools such as ping sweeps, port and vulnerability scanners

Social Engineering

- Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information.
- It typically involves nothing more technical than the use of a telephone or email.
- The attacker will often pretend to be somebody else to trick the victim.

Phishing

- Phishing is a Social Engineering attack where the attacker pretends to be from a reputable company to get individuals to reveal personal information, such as passwords and credit card numbers.
- The victim is often directed to enter their details into the attacker's website which looks like the reputable company's legitimate website.

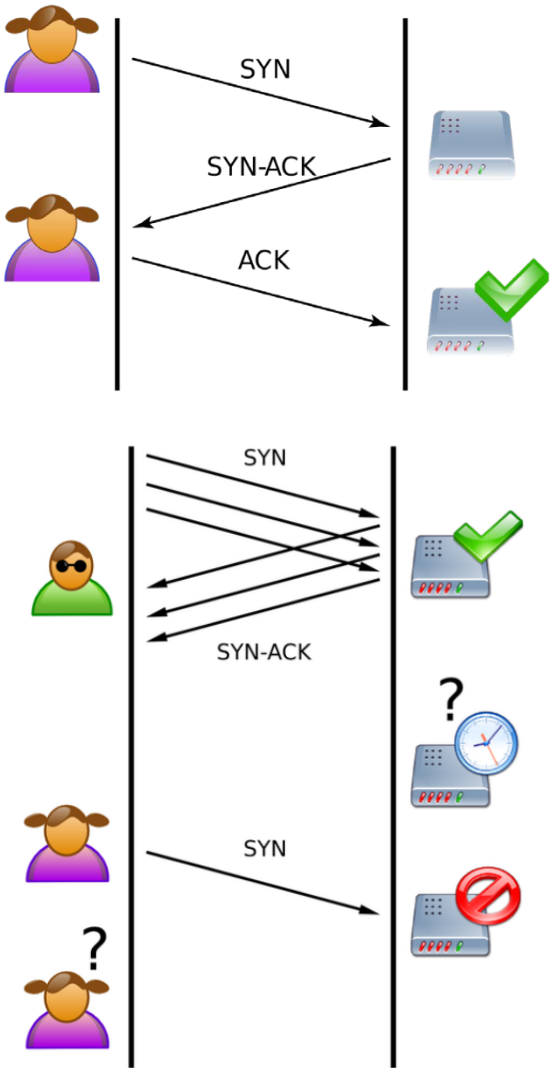
Data Exfiltration

- Data exfiltration is where data leaves an organization without authorization
- This can be by a hacker who has compromised a system
- Or by an internal staff member, either maliciously or by accident (for example sending an email which includes secret information, or leaving a USB stick on a bus)

DoS Denial of Service

- A Denial of Service (DoS) attack prevents legitimate users from accessing an IT resource.
- It is typically a brute force style of attack which floods the target system with more traffic than it can handle.
- DoS attacks from a single source can be easily stopped by blocking traffic from that host.

TCP Syn Flood Attack



DDoS Distributed Denial of Service

- A Distributed Denial of Service (DDoS) attack is a DoS attack from multiple sources.
- The attacker builds and controls a botnet army of infected zombie hosts.
- The botnet is built through malware such as worms and trojan horses.

DDoS and Botnets

- Infected hosts connect out to the attacker's command and control server. This circumvents firewalls because the connection is initiated from the inside.
- The attacker now has control of the botnet to launch attacks.
- DDoS attacks are more difficult to mitigate against because the attack comes from multiple sources which could normally be expected to send legitimate traffic.

Spoofing

- Spoofing is where an attacker fakes their identity.
- Spoofing types include:
    - IP address spoofing
    - MAC address spoofing
    - Application spoofing (eg rogue DHCP server)

Reflection and Amplification Attacks

- A reflection attack is a DoS attack where the attacker spoofs the victim's source address
- The attacker sends traffic supposedly from the victim which elicits a response from 'reflectors'
- Amplification causes a large amount of response traffic to the victim

Man In The Middle Attacks

- In man in the middle attacks, the attacker inserts themselves into the communication path between legitimate hosts
- The attacker can then read and optionally modify the data
- ARP spoofing is a well known man in the middle attack

Password Attacks

- If an attacker has connectivity to a login window, they can attempt to gain access to the system behind it
- Enumeration techniques attempt to discover usernames
- Password cracking techniques attempt to learn user passwords
- Methods include:
    - Guessing
    - Brute Force
    - Dictionary attacks

Buffer Overflow Attacks

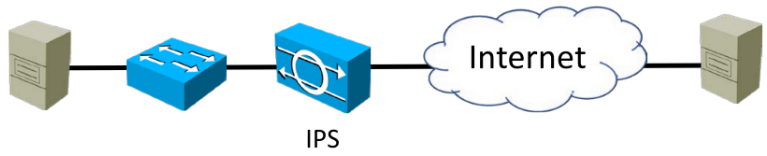
- Buffer overflow attacks send malformed and/or too much data to the target system
- This can cause a denial of service, or compromise of the target system

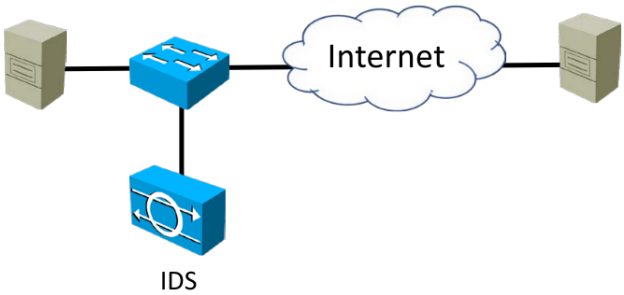
Packet Sniffers

- If an attacker has compromised a target system or inserted themselves into the network path, Packet Sniffers such as WireShark can be used to read the sent and received packets
- Any unencrypted sensitive information can be learned by the attacker
- They can use this to damage the organization or escalate their attack

IDS and IPS

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IDS and IPS use signatures to inspect packets up to layer 7 of the OSI stack, looking for traffic patterns which match known attacks
- They can also use anomaly-based inspection to look for unusual behaviour, such as a host sending more traffic than usual
- They require skilled staff to tune the IPS to their own particular environment and minimize false positives and negatives
- IDS sits alongside the traffic flow and informs security administrators of any potential concerns
- IPS sits inline with the traffic flow and can also block attacks
- (An IDS may also have the capability to tell a firewall to block attacks)





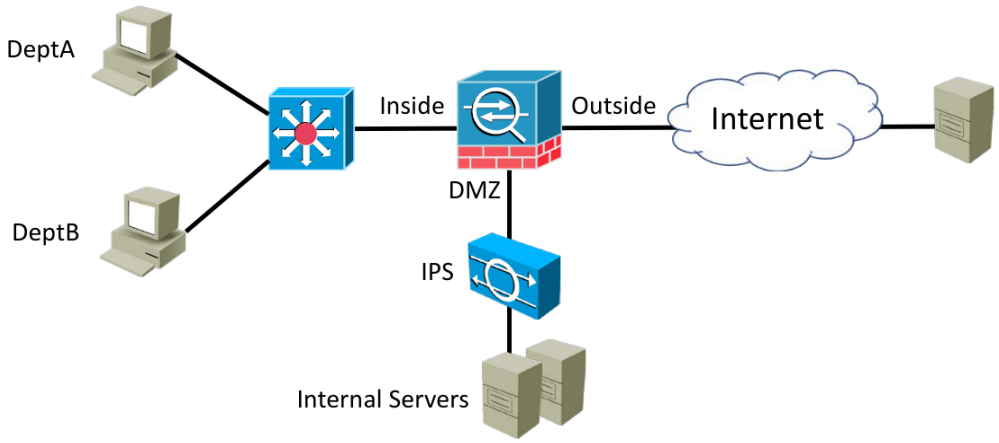
IPS vs Firewalls

- IPS use signatures to inspect packets up to layer 7 of the OSI stack, looking for traffic patterns which match known attacks
- Firewalls block or permit traffic based on rules such as destination IP address and port number

- Organizations always deploy firewalls on the Internet edge. They may also deploy them at suitable security points inside their internal network
- IPS's are an option which may be deployed in conjunction with a firewall

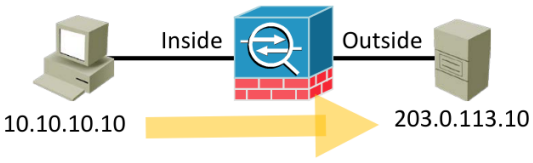
- The lines have blurred in recent years between IPS and Firewalls, particularly with the emergence of **Next Generation Firewalls**
- Modern firewalls often also have IPS capability
- They are also often capable of acting as the endpoint of VPN tunnels

- Organisations can deploy an all in one solution, or they may split out the functions to provide better scalability
- Specialised devices may also have more advanced features
- Another option for scalability and higher throughput is clustered devices

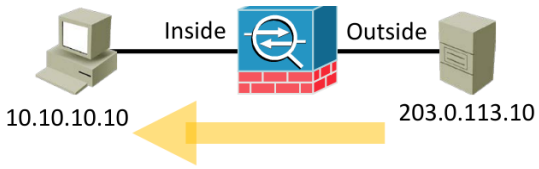


Stateful Firewall

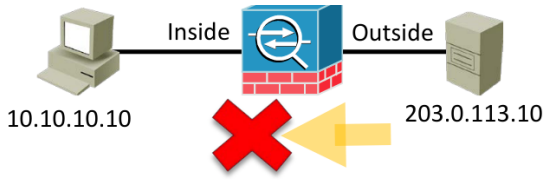
- Firewalls secure traffic passing through them by either permitting or denying it
- Stateful firewalls maintain a connection table which tracks the two-way 'state' of traffic passing through the firewall
- Return traffic is permitted by default
- Firewall rules example:
    - Deny all traffic from outside to inside
    - Permit outbound web traffic from 10.10.10.0/24



- Traffic is allowed by 'Permit outbound web traffic from 10.10.10.0/24' rule
- Connection table: 10.10.10.10:49160 > 203.0.113.10:80



- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is permitted because it is valid return traffic for a connection in the connection table
- This overrides the 'Deny all traffic from outside to inside' rule



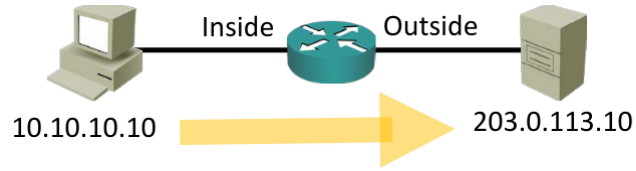
- In this example the connection has not been initiated from the host on the inside
- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is dropped according to the 'deny all traffic from outside to inside' rule

Next Generation Firewalls

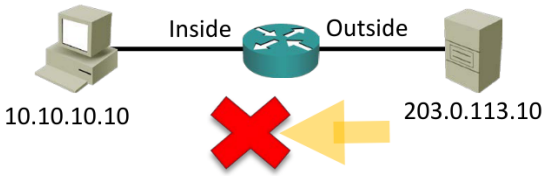
- Next Generation Firewalls move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and user based security
- Deep packet inspection analyses packets up to layer 7 of the OSI stack
- Different permissions can be applied to different users
- The Cisco ASA with FirePower is a Next Generation Firewall

How Packet Filters(ACL) Work

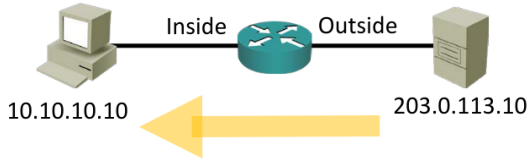
- An Access Control List security policy is a packet filter
- Packet filters do not maintain a connection table
- They affect traffic in one direction only and do not track the state of two way connections going through the router
- If you have an ACL applied on the way out only, the return traffic will be allowed because all traffic is allowed when an ACL is not applied
- If you have ACLs applied in both directions, you will need explicit entries to allow both the outbound and the return traffic
- Access Control List example:
    - Inbound ACL on outside interface: Deny all traffic
    - Inbound ACL on inside interface: Permit web traffic from 10.10.10.0/24



- Inbound ACL on inside interface: Permit web traffic from 10.10.10.0/24 allows traffic out to the web server
- The connection is not tracked in a connection table



- Traffic from 203.0.113.10:80 > 10.10.10.10:49160 is dropped because of Inbound ACL on outside interface: Deny all traffic



- To allow the return traffic you need to remove the 'deny all traffic from outside to inside' ACL on the outside interface
- Or add 'permit tcp any eq 80 10.10.10.0 0.0.0.255 range 49152 65535'
- Neither is a secure option for a router connected to the Internet

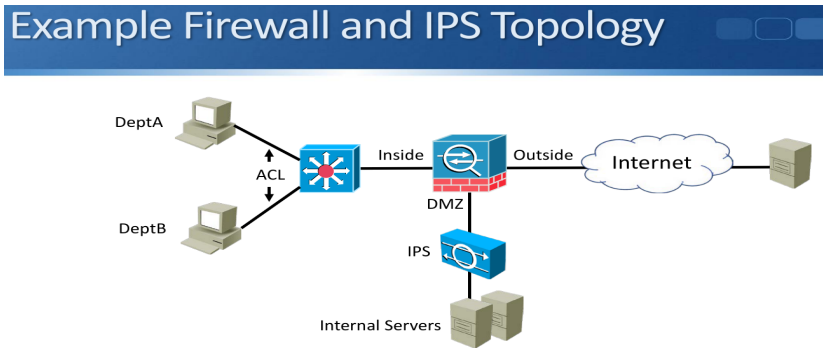
The 'Established' Keyword

```
R1(config)#access-list 100 permit tcp any eq 80
10.10.10.0 0.0.0.255 established
```

- The Established keyword in an ACL only checks for the 'Ack' flag in return traffic
- This does not make the router a stateful firewall and it still does not keep a connection table!

Internal and External Threats

- ACL packet filters on routers can add to an overall defence in depth strategy
- Standard practice is to use firewalls on major security boundaries, and augment this with internal ACLs
- Purely external threats are primarily covered with strong firewall and IPS protection on the network perimeter.
- Sensitive hosts should also have firewall and IPS protection from internal hosts



Cryptography

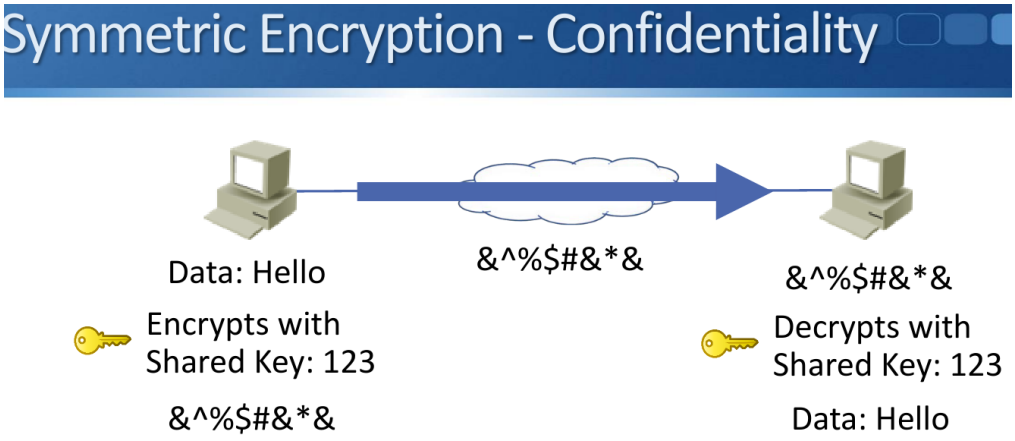
- Cryptography transforms readable messages into an unintelligible form and then later reverses the process
- It can be used to send sensitive data securely over an untrusted network
- It uses authentication and encryption methods

Cryptography Services

- Cryptography provides these services to data:
- Authenticity (proof of source)
- Confidentiality (privacy and secrecy)
- Integrity (has not changed in transit)
- Non-repudiation (non-deniability)

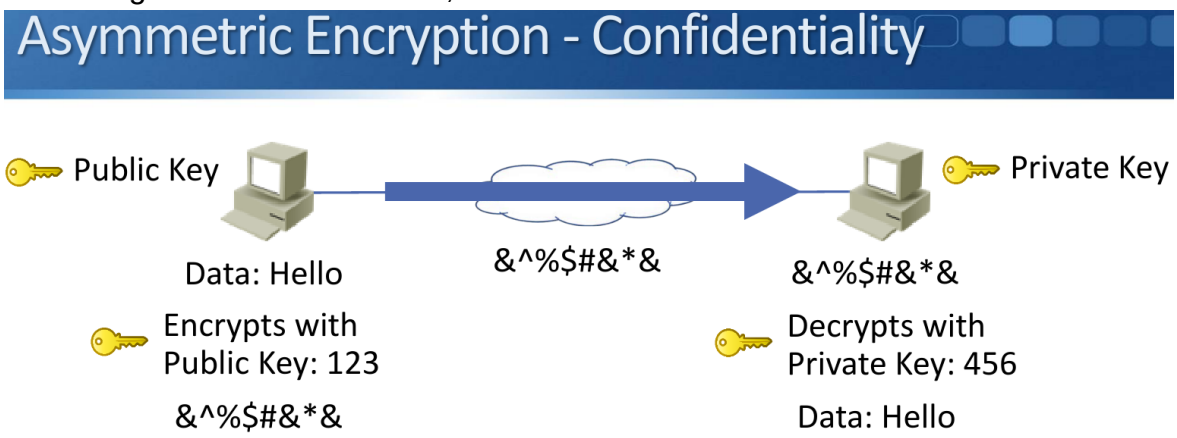
Symmetric Encryption

- With symmetric encryption, the same shared key both encrypts and decrypts the data
- The shared key is known by both the sender and receiver and must be kept secret
- Fast
- Used for large transmissions (eg email, secure web traffic, IPsec)
- Algorithms include DES, 3DES, AES, SEAL



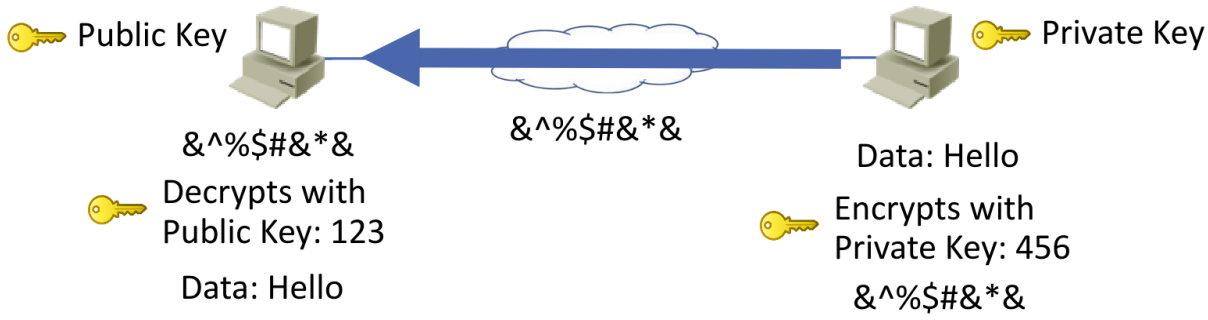
Asymmetric Encryption

- Asymmetric encryption uses private and public key pairs
- Data encrypted with the public key can only be decrypted with the private key, and vice versa
- Data encrypted with the public key cannot be decrypted with the public key
- Only the private key must be kept secret
- The public key can be available in the public domain
- Slow
- Used for small transmissions (symmetric key exchange, digital signatures)
- Algorithms include: RSA, ECDSA



- This allows anybody to send data securely to the host with the private key
- It is the only one with the private key so only one who can read the message
- Other hosts with the public key **cannot** read the message

Asymmetric Encryption – Authenticity and Non-Repudiation

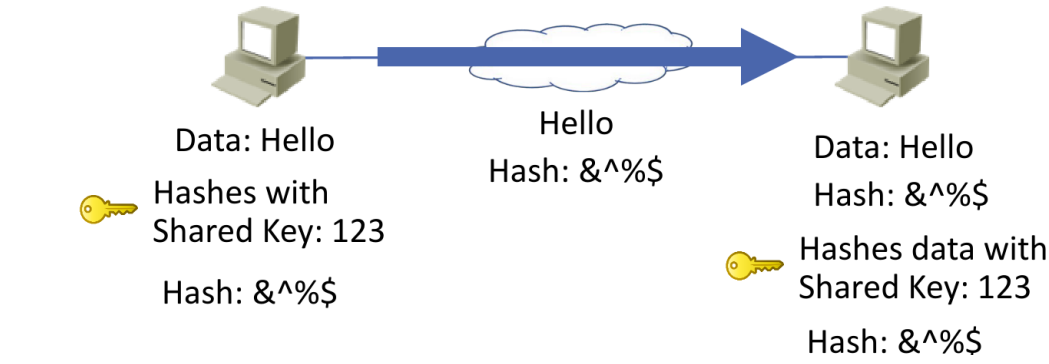


- This provides authenticity of the host with the private key
- All receivers need to know what is the genuine public key

HMAC Hash-Based Message Authentication Codes

- HMAC codes provide data integrity
- The sender creates a hash value from the data to be sent using a symmetric key
- The hash value is appended to the data
- The receiver hashes the data with the same shared key
- If the hash values are the same the data has not been altered in transit
- Used for large transmissions (eg email, secure web traffic, IPsec)
- Algorithms include: MD5, SHA

HMAC - Integrity



Key Distribution

- Cryptography can be used to send sensitive data securely over an untrusted network
- Symmetric key encryption is used for bulk data transmissions
- Each side needs to know the shared key
- This leads to a key distribution problem
- When you buy something online, you want your credit card details to be encrypted over the Internet
- The online store can’t send you the shared key over the same Internet channel - it’s not secure
- It’s not practical for them to phone the customer every time someone wants to make a purchase

Public Key Infrastructure PKI

- PKI solves the secure key distribution problem
- It uses a trusted introducer (the Certificate Authority) for the two parties who need secure communication
- Both parties need to trust the Certificate Authority

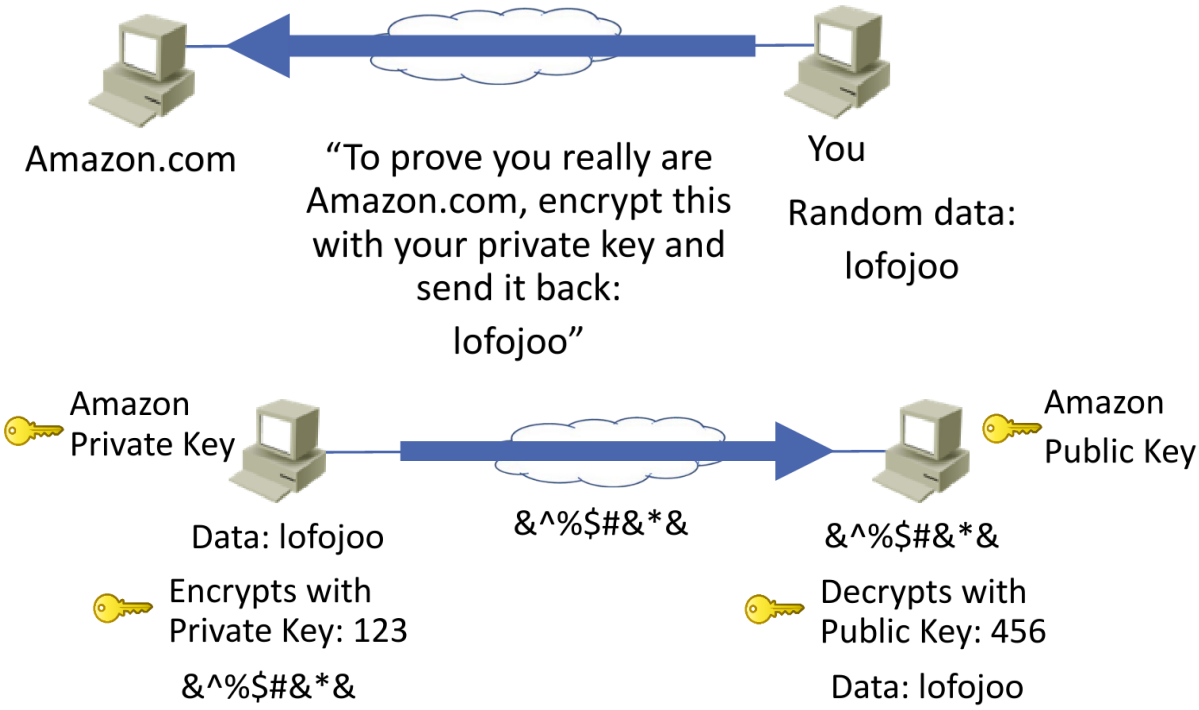
TLS

- SSL: Secure Sockets Layer (deprecated)
- TLS: Transport Layer Security (successor to SSL)
- Can be used to provide secure web browsing with HTTPS (can also be used with other applications such as email)
- Uses symmetric cryptography to encrypt transmitted data
- Symmetric keys are generated uniquely for each connection
- Authentication is provided by public key cryptography
- Message Authentication Code provides integrity

HTTPS Example

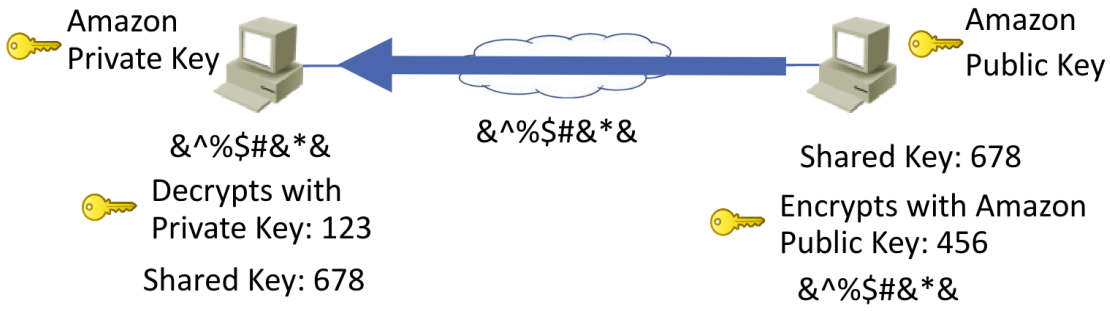
- Your browser trusts Verisign and has its public key (that information is installed with your web browser)
- It checks the certificate with Verisign’s public key
- Verisign is the only entity with their private key, so if it checks out it must have been signed by Verisign and you trust the certificate
- You now know that who you are communicating with has sent you the valid certificate for Amazon.com…
- But you don’t know that you are communicating with Amazon.com yet!

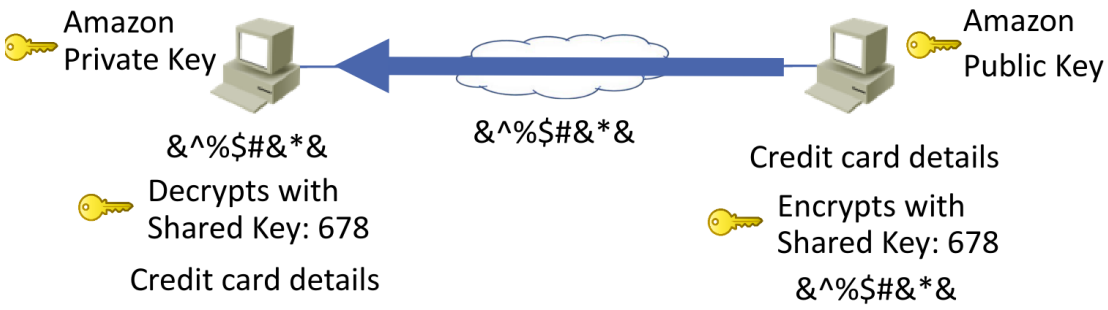
- Anybody could have sent you the valid certificate for Amazon.com and be pretending to be them
- You have not authenticated them yet



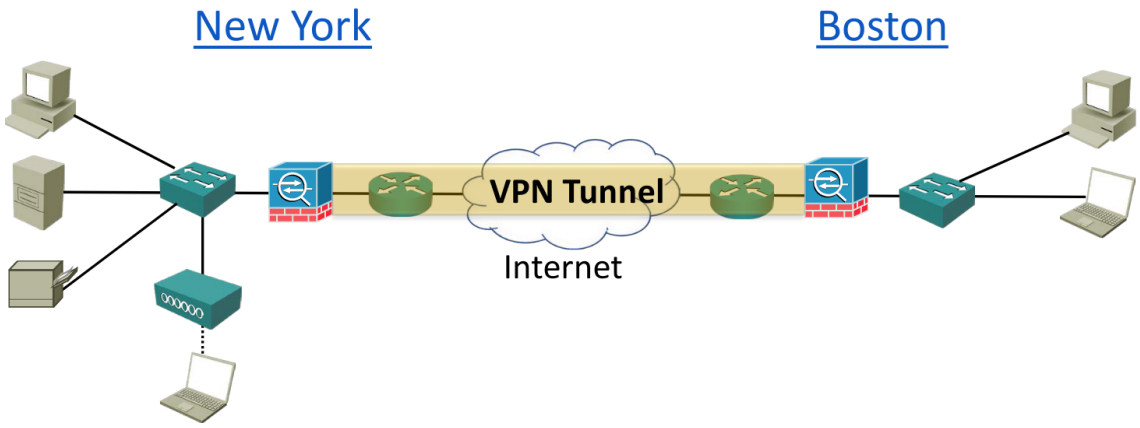
- The real Amazon.com is the only entity with their private key
- You have now authenticated Amazon.com

- Your browser could now encrypt your credit card details with Amazon's public key when you make a purchase, and nobody else would be able to read the details
- But asymmetric key encryption is slow and not suitable for bulk data exchange like web browsing
- Symmetric key encryption should be used, but Amazon and you do not have a shared key…





Site-to-Site VPNs



- Site-to-Site VPNs use symmetric encryption algorithms such as DES, 3DES and AES to send encrypted traffic between locations over an untrusted network such as the Internet
- Traffic inside an office is often unencrypted as it is seen as a trusted network
- VPN tunnels can however also be deployed internally
- Cisco TrustSec is another solution for internal authentication and encryption
- Site-to-Site VPN tunnels typically terminate on a firewall or router on both sides
- A pre shared key can be configured on both sides of the tunnel or certificates can be used
- Certificates offer a more scalable solution

IPsec

- IPsec is a framework of open standards that provides secure encrypted communication to an IP network.
- Internet Key Exchange (IKE) handles negotiation of protocols and algorithms, and generates the encryption and authentication keys
- Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating and communicating peer creation

and management of Security Associations. It typically uses IKE for key exchange.

- IKE and ISAKMP are sometimes used synonymously.
-
- Authentication Header (AH) provides integrity, authentication and protection from replay attacks
- Encapsulating Security Payload (ESP) provides confidentiality, integrity, authentication and protection from replay attacks
- ESP is more commonly used
-

ESP Tunnel Mode

- Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by another set of IP headers.
- It is widely implemented in site-to-site VPN scenarios.

ESP Transport Mode

- The transport mode encrypts only the payload and ESP trailer; so the IP header of the original packet is not encrypted.
- The IPsec Transport mode is implemented for client-to-site VPN scenarios.
- The transport mode is usually used when another tunneling protocol (such as GRE, L2TP) is used to first encapsulate the IP data packet, then IPsec is used to protect the GRE/L2TP tunnel packets.

IPsec VPN Implementation

- Interesting traffic: The VPN devices recognize the traffic to protect.
- ISAKMP / IKE Phase 1: The VPN devices negotiate an IKE security policy, authenticate each other and establish a secure channel.
- ISAKMP / IKE Phase 2: The VPN devices negotiate an IPsec security policy to protect IPsec data.
- Data transfer: The VPN devices apply security services to traffic, then transmit the traffic.

Phase 1

R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#crypto isakmp key Flackbox address 203.0.113.5

ACL to Define Interesting Traffic

R1(config)#ip access-list extended FlackboxVPN-ACL
R1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255

Phase 2

R1(config-ext-nacl)#crypto ipsec transform-set FlackboxTS esp-aes esp-sha-hmac
R1(config)#crypto map FlackboxCM 10 ipsec-isakmp
R1(config-crypto-map)#set peer 203.0.113.5
R1(config-crypto-map)#set transform-set FlackboxTS
R1(config-crypto-map)#match address FlackboxVPN-ACL
R1(config-crypto-map)#interface Serial0/1/0
R1(config-if)#crypto map FlackboxCM

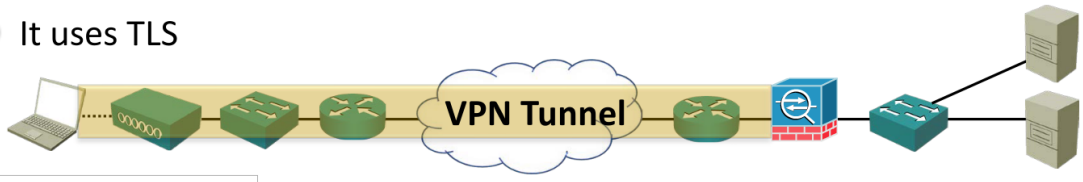
Exclude VPN Traffic from NAT ACL

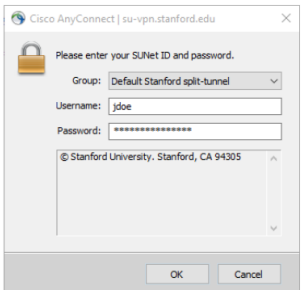
R1(config)#ip access-list extended FlackboxNAT-ACL
R1(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
R1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any

Remote Access VPN

Cisco AnyConnect Secure Mobility Client

- Cisco AnyConnect is a Remote Access VPN application which uses the ASA firewall
- It uses TLS





Threat Defense Solutions

Malware

- Anti malware software should be installed on host systems
- It uses signatures and heuristics to detect malicious software and block it
- from running
- Controls should be in place to prevent users from disabling the software
- An IPS can also be used to detect and block network traffic containing malware

Malware, Phishing and Data Exfiltration

- The Cisco ESA Email Security Appliance scans links and attachments in incoming email for malware, phishing attacks and spam
- The Cisco WSA Web Security Appliance prevents users from accessing dangerous websites
- Policies can also be implemented on the ESA and WSA to prevent sensitive information from being sent out of the organization
- Policies and procedures should be implemented, for example about how and what information can be sent or taken outside the company premises
- Security awareness training should also be implemented

Reconnaissance and Social Engineering

- Low level reconnaissance (Google research etc.) and Social Engineering can use very low tech methods to gain information and access to the target organization
- As such it is difficult for IT departments to use technical solutions to protect against them
- The way to defend against them is through staff security awareness
- Policies and procedures should be implemented
- Staff should be educated about security concerns
- An IPS can defend against deeper reconnaissance which uses port and vulnerability scanners
- It is not normal behaviour for a host to scan through a range of port numbers

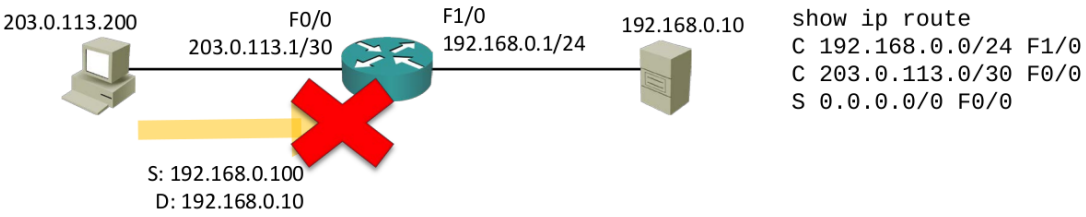
- An IPS can detect and drop the traffic
- A determined attacker may attempt to circumvent this by running the scan over a longer time period

DDoS Distributed Denial of Service

- An IPS can detect DDoS attacks through anomaly-based inspection
- Advanced firewalls can offload incoming connection attempts from servers when the traffic rate reaches a threshold, and respond with quicker connection timeouts and/or cookies.
- Anti DDoS services such as Arbor Networks monitor global Internet traffic to detects botnets and Command and Control servers
- They have on premises and cloud based solutions which scrub traffic when an organization is under DDoS attack
- Geographic dispersion of an organization’s services can help mitigate DdoS attacks

Spoofing, Man In The Middle and Reflection Attacks

- Unicast Reverse Path Forwarding (uRPF) verifies a source IP address is reachable through the same interface it was received on



- When an attacker spoofs their source IP address they do not receive return traffic so they do not see the sequence numbers in TCP
- responses from the target. A target may be more vulnerable to attacks if it uses predictable TCP sequence numbers.
- Applications should be up to date and patched to prevent this.
- When they are in the traffic path, advanced firewalls can also randomize TCP sequence numbers.
- Secure authentication proves that systems are communicating with who they think they are.
- Dynamic ARP Inspection detects and blocks ARP spoofing attacks

Password Attacks

- Firewalls and packet filters should be configured to prevent illegitimate users from having connectivity to login windows
- Policies should be in place to enforce secure passwords
- Password complexity settings include minimum password length, special character requirements, how often passwords must be changed, and prevention of old passwords being reused
- Multi factor authentication should be used where suitable. This uses something the user knows (a password) and something they have (a biometric reader, or a code generated on a mobile app or security device)
- Staff should be educated to guard against social engineering attacks

Buffer Overflow Attacks

- Software should be up to date and patched so that it rejects malformed packets

Packet Sniffers

- Packet filters and firewalls should be used to ensure traffic paths are controlled
- Traffic should be authenticated and encrypted if it passes over an untrusted network

Penetration Testing

- A penetration tester can be employed to test the organisation’s security defence
- The penetration tester uses the same tools and methods as a hacker
- Internal security teams should do their own testing of their security systems and policies
- An external penetration tester can be used for validation