Networks and Internet Systems

Network Security

Agenda

1. Security Basics
2. Access Control
3. Network & Data Security
4. Secure Protocols

Security Basics

Security Landscape

- *Security* is the degree of protection against danger, damage, loss, and criminal activity.

networks

- **Information Security is a never ending arms race!**
  - Technology is moving quickly
  - More and more devices are being connected (IoT, smart homes/cars/cities)
- Intrusion is inevitable! -> Effective detection, containment, eradication, and recovery is key!
- Goal is to minimise:
  - Threat surface
  - Damage

Security Challenges

- **Sophistication**
  - More complex -> more difficult to detect -> more difficult to stop
  - Why? *Internet* - attackers using common tools and protocols to evade firewalls.
  - Vary behaviour - same attack looks different
- **Proliferation of attack software**
  - Volume - lots more attacks now. Monetary reward & easier (attack software, malware available for sale on the dark web)!
- **Scale & Velocity**
  - Size and speed of attacks increasing - recon tools can be used to find vulnerabilities, internet can be used to spread attack
    - Slammer/sapphire worm - infected 55 million PCs per second
    - First malware - required user interaction to spread (floppy disk)
  - Distributed attacks

invincea 2016 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA, EUROPE, ASIA PACIFIC, & LATIN AMERICA

SURVEY DEMOGRAPHICS

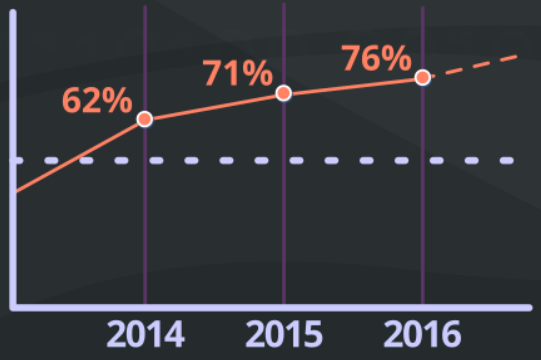
10 Countries represented around the world

20+ Industries represented

1,000 Qualified IT security decision makers & practitioners

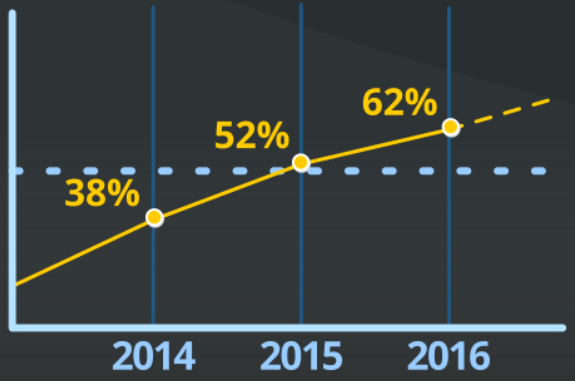
RISING CYBERATTACKS

The percentage of respondents affected by successful attacks is rising each year.



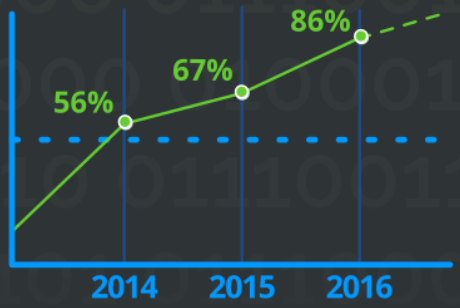
SINKING EXPECTATIONS

Respondents that believe a successful cyberattack is likely in the coming year is skyrocketing.



ENDPOINT PROTECTION REVOLUTION

The percentage of organizations evaluating new endpoint protection solutions to augment or replace their existing investments is skyrocketing.



THE YEAR OF ENDPOINT CONTAINERIZATION

The top four endpoint security technologies targeted for acquisition in 2016 include...

1. CONTAINERIZATION/ MICRO-VIRTUALIZATION
2. SELF-REMEDIATION FOR INFECTED ENDPOINTS
3. DIGITAL FORENSICS/ INCIDENT RESOLUTION
4. DATA LOSS/LEAK PREVENTION (DLP)

SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. LOW SECURITY AWARENESS AMONG EMPLOYEES
2. TOO MUCH DATA TO ANALYZE
3. LACK OF SKILLED PERSONNEL

CYBERTHREAT HEADACHES

Cyberthreats causing the greatest concern include...

1. MALWARE (VIRUSES, WORMS, TROJANS)
2. PHISHING/ SPEAR-PHISHING ATTACKS
3. SSL-ENCRYPTED THREATS

SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

1. MOBILE DEVICES
2. SOCIAL MEDIA APPLICATIONS
3. LAPTOPS/ NOTEBOOKS

SUSCEPTIBLE NATIONS

The percentage of respondents affected by successful attacks in 2015 varied by nation.

BRAZIL	89%
FRANCE	82%
CANADA	82%
GERMANY	78%
UNITED STATES	75%
JAPAN	75%
MEXICO	74%
SINGAPORE	73%
UNITED KINGDOM	71%
AUSTRALIA	63%

CIA of Information Security

- **Confidentiality -** Data remains secret (encryption)
- **Integrity -** Data is not modified (hashing)
- **Availability -** Data is available (systems are up and providing services)
- *Trade off between security and accessibility*
  - *Completely Secure == Unusable*
  - Remove **all** access (key cards, usb, mouse, keyboard, monitor) == secure :)
  - Remove **all** access (key cards, usb, mouse, keyboard, monitor) == not useable :(
  - Not useable == not an asset
- Weigh the risks and benefits of having a vulnerability versus the cost of it being exploited.
- Example: allowing physical access to the server, enabled USB port

Security Roles and Concepts

- **3 main components of Security:**
    1. Physical Security (fences, locked doors, hardware, software, etc)
    2. Users & Admins (people who use and manage the software, biggest vulnerability!)
    3. Policies (rules to protect critical information assets)
- **Assets** - something with value
- **Threat** - entity that can cause the loss or damage to an asset
- **Threat Agent** - person or entity that can carry out threat (external/internal attacker, funded/unfunded, opportunistic/targeted)
- **Vulnerability** - weakness that allows the threat to be carried out
- **Exploit** - procedure/software that takes advantage of vulnerability

Threat Agent Types 1

- External threats are not the only problem!
- **Employees (internal threats):**
  - Have greater access to information assets (disgruntled employee, financial incentive (bribery), unintentional (more of them!))
- **Corporate Espionage:**
  - Internal - hires a spy to get a job in the target company and returns information
  - External - hires a spy to attack from outside, exploit vulnerabilities
- **Hackers:** any threat agent that uses their technical knowledge to exploit vulnerabilities to gain access
  - Motivation - Attention/prestige, criminal - financial/political benefit, white-hat

Hackers

- **Script Kiddies:**
  - Little technical ability, download tools and run attacks
- **Cyber criminals:**
  - Take more risks because of financial gains, highly motivated, more tenacious
- **Cyber terrorist:**
  - Motivation - political cause or ideology
  - May still look for financial gain
  - Disrupt network
  - More cold and calculating - Could spend years to do recon and planning attack

General Attack Methodology

No two exploits are the same, but … many threat agents follow the same methodology

1. **Reconnaissance**
    - Gather information about system and users - probe target systems for vulnerabilities
        - **Organisational (Social Engineering):** Dumpster dive, Phone (intimidation/ sympathetic), Email/IMs/Social Networking
        - **Technical (passive/active, horizontal/vertical):** Port scan - nmap (finds holes), ping sweep (finds available systems), nslookup, WHOIS
2. **Breach**
    - Depends on the exploit:
        - Social engineering -> username and password
        - Technical -> access open port, crack password, etc

General Attack Methodology 2

3. Escalate privileges

- Typically will only have certain level of access -> try to get admin/root
- Create a way to get back in (backdoor) e.g., set up a user account (looks normal account)

4. Stage (optional)

- Depends on the attack - not for focused attacks like stealing credit card numbers, etc
- Worm spread - the attacker will use the breached host as a stage to spread the worm.

5. Exploit

- Exfiltrate data: identities, customer info, credit card numbers, embarrassing info, intellectual property
- Denial of service
- Corrupt information

General Defence Strategy

Layered defences (e.g., Byzantine)

- Multiple strategies to protect assets e.g., 2 factor auth
- Most attackers are looking for easy targets
  - Layered defences means your not a target of opportunity
  - Still open to targeted attacks.

Principle of least privilege

- Limiting user access
  - OSs treat privilege differently (explicit access/explicit denial of access)
  - Shared directories are problematic - can violate principal of least privilege

Varied Mechanisms

- Multiple layers of exact same defence is not useful (e.g., Byzantine again)
  - E.g. entering a password to access the system and then another password to access files.

General Defence Strategy

Randomness

- Humans are predictable! Same route to work, same routine when sit at desk, etc.
    - Attackers can identify patterns to find vulnerabilities. E.g, password change intervals - should be different.

Obscure information

- Block ping sweeps using a firewall - obscure the number of hosts on network, obscure IPS, obscure domain registration, etc.

Simple is best

- Simple != easily defeat-able
- Simple == mechanisms you understand! You need to understand configuration, output, etc.

Access Control

Access Control

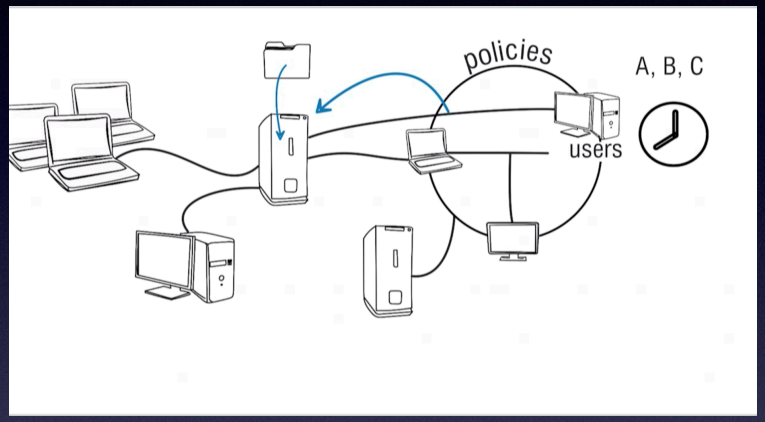
- *Access control:* ability to permit/deny the privileges that users have when accessing resources on a network or computer (3 entities: objects, subjects, system)
- Four main access control processes:
  - ***Identification:*** identifies the subject, e.g., username or a user ID number.
  - ***Authentication:*** validating a subject's identity
  - ***Authorisation:*** grant or deny a subject's access to an object.
  - ***Auditing/Accounting:*** is maintaining a record of a subject's activity
- Authentication, Authorisation, and Auditing are known as the **AAA** of access control.
- Access control measures can also be classified based on how they restrict or control access (***administrative, technical, physical***)

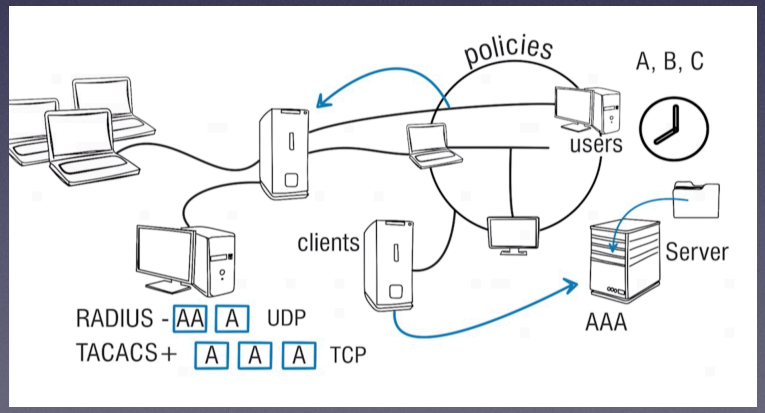
Authentication

- Process of validating a set of issued credentials (different to identification!)
- 5 Authentication factors:
    1. ***Something you know*** - e.g., password or some other data that you know
    2. ***Something you have*** - also called token-based authentication
    3. ***Something you are authentication*** - uses a biometric system
    4. ***Somewhere you are*** - also known as geolocation
    5. ***Something you do*** - is a supplementary authentication factor that requires an action to verify a user's identity.
- Metrics used to measure accuracy/performance of biometrics system: false negative, false positive, processing rate
- Can be combined to strengthen security: 2 factor, 3 factor, multi-factor, mutual

Remote Access Servers

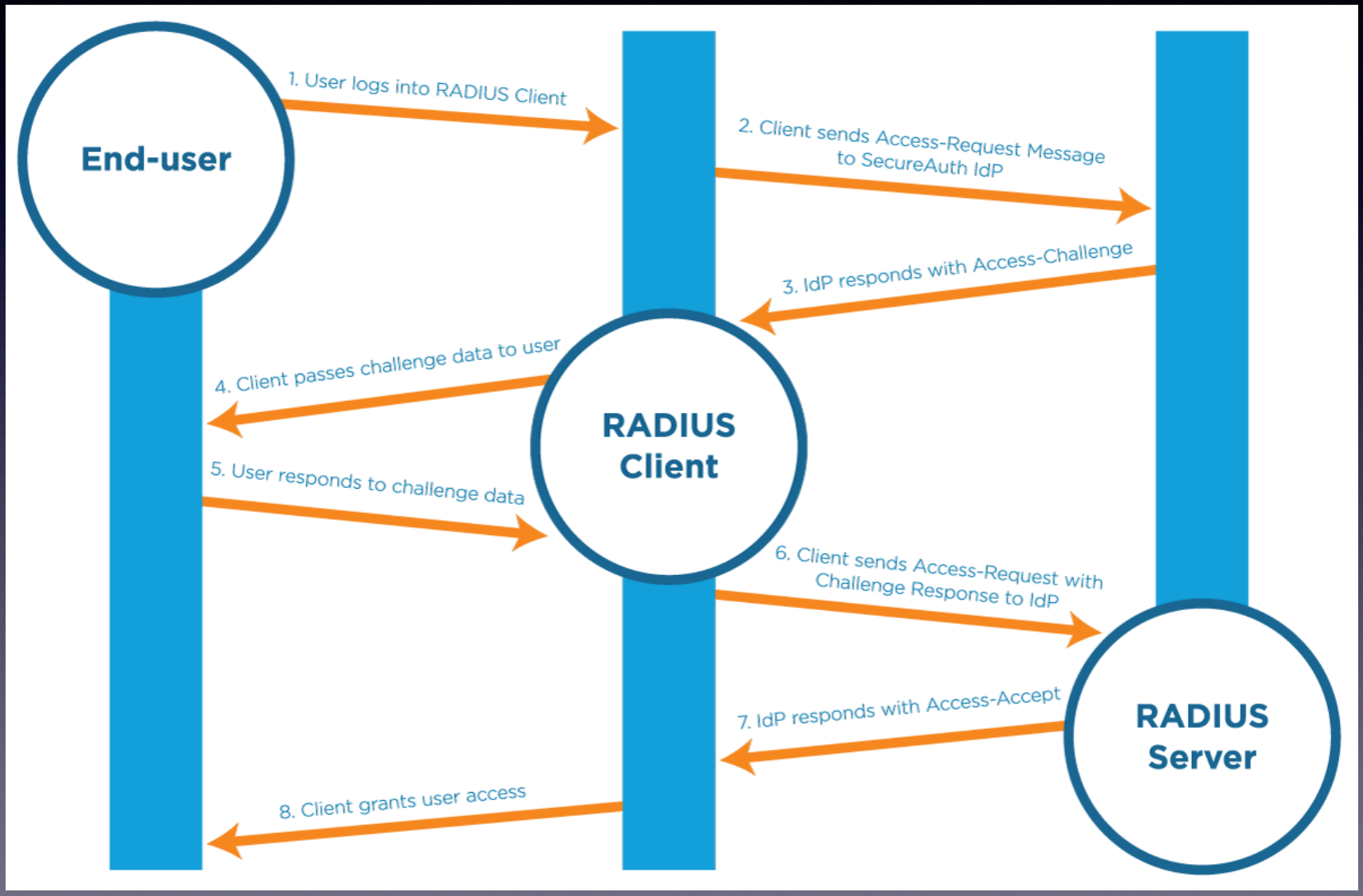
- Remote access policies identify authorised users and other required connection parameters
- **Small implementation** -> user accounts and remote access policies are defined on the Remote Access Server
  - You must define user accounts and policies on each RAS
- **Larger deployments** -> with multiple remote access servers, you can centralise the administration of remote access policies by using an AAA server
  - Connection requests from remote clients are received by the RAS and forwarded to the AAA server to be approved or denied
  - Policies defined on the AAA server apply to all clients connected to all RASs





Remote Authenticate Dial-In User Service (RADIUS) AAA

- RADIUS is used by Microsoft servers for centralized remote access administration
  - Authentication and authorization must be combined on a single server. Accounting can be separate
- RADIUS supports multiple protocols: PPP, CHAP, and PAP.
- Uses a challenge/response method for authentication.
- RADIUS encrypts only the password using MD5.
- Uses UDP ports 1812 and 1813 and can be vulnerable to buffer overflow attacks.
- Often uses vendor-specific extensions.
  - Different vendors might not be compatible.
- The RADIUS *server* provides AAA services,
  - The RASs are RADIUS *clients*.


End-user
1. User logs into RADIUS Client
2. Client sends Access-Request Message to SecureAuth IdP
3. IdP responds with Access-Challenge
4. Client passes challenge data to user
RADIUS Client
5. User responds to challenge data
6. Client sends Access-Request with Challenge Response to IdP
7. IdP responds with Access-Accept
RADIUS Server
8. Client grants user access

Terminal Access Controller Access Control System (TACACS)+ AAA

- TACACS+ was originally developed by Cisco:
- TACACS+:
  - Provides three protocols, one each for authentication, authorization, and accounting.
    - Each service can be provided by a different server.
  - Uses TCP port 49.
  - Encrypts the entire packet contents and not just authentication packets; the client server dialogs are also encrypted.
  - Supports more protocol suites than RADIUS.
  - The TACACS+ RASs become TACACS+ clients to the backend TACACS+ server.
  - TACACS and XTACACS are older protocols - less secure

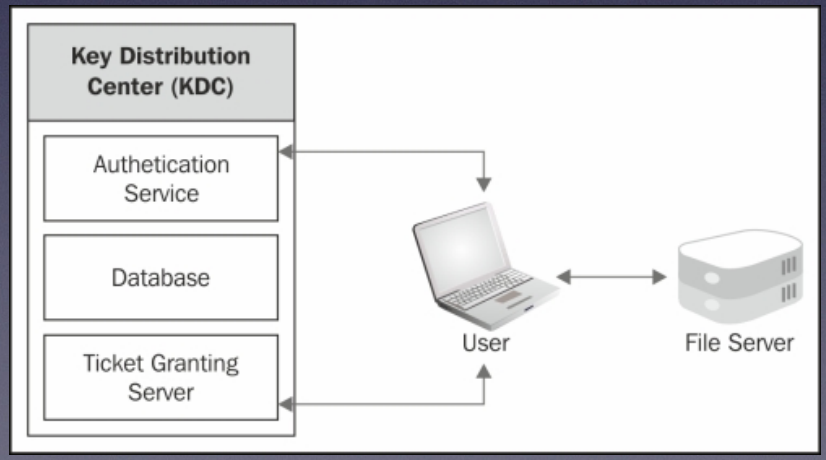
AAA Servers

- TACACS+ and RADIUS have **generally** replaced earlier protocols in more recent networks
- RADIUS is more interoperable because TACACS+ is Cisco proprietary
- RADIUS performs better due to less encryption, less overhead, and more compatibility with other systems
- TACACS+ is considered more reliable than RADIUS because of TCP
- TACACS+ is more secure than RADIUS because RADIUS encrypts only the password
- TACACS+ encrypts the entire session between the client and server
- RADIUS is more secure than the original TACACS
- PPTP not compatible with RADIUS and TACACS+; L2TP is compatible with RADIUS and TACACS+.

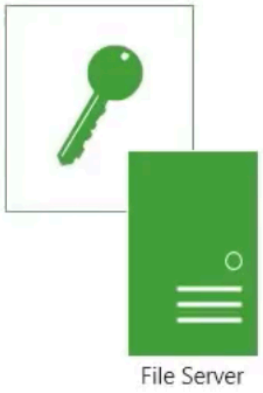
	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication and Authorization
Transport Protocol	TCP	UDP
Challenge/ Response	Bidirectional	Unidirectional
Protocol Support	Full Support	No ARA or NetBEUI
Confidentiality	Entire Session Encryppted	Password Encrypted

Network Authentication Protocols - Kerberos

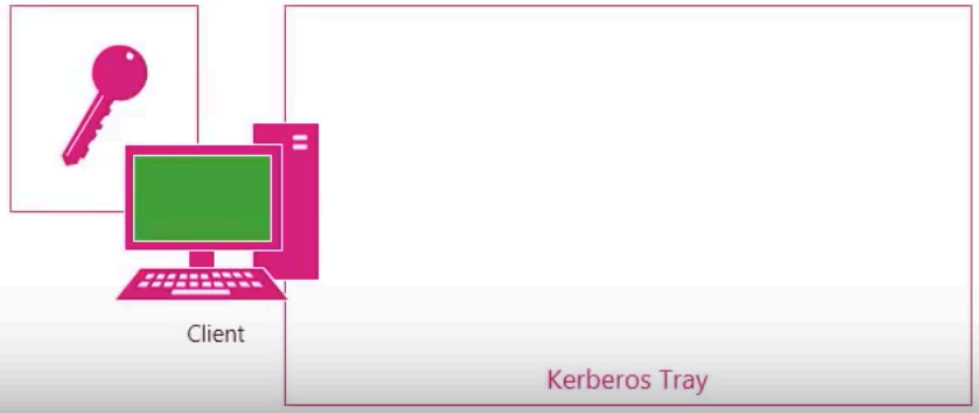
- Kerberos is used for both authentication and authorization
- The process of using tickets to validate permissions is called ***delegated authentication***.
- Kerberos uses the following components:
  - An authentication server (AS) accepts and processes authentication requests.
  - A service server (SS) is a server that provides or holds network resources.
  - A ticket granting server (TGS) grants tickets that are valid for specific resources on specific servers.
  - The authentication server and ticket granting server are often combined into a single entity known as the Key Distribution Center (KDC).



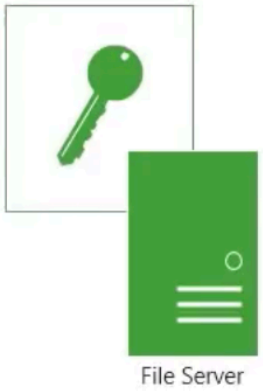
Kerberos Protocol



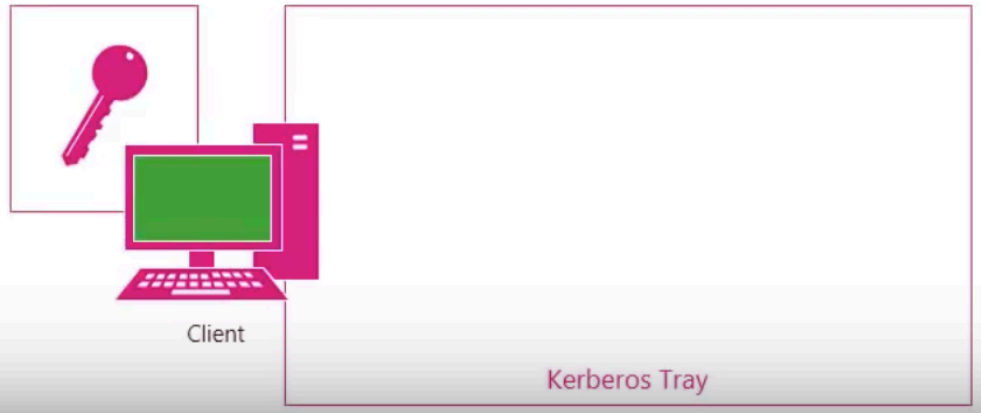
1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket



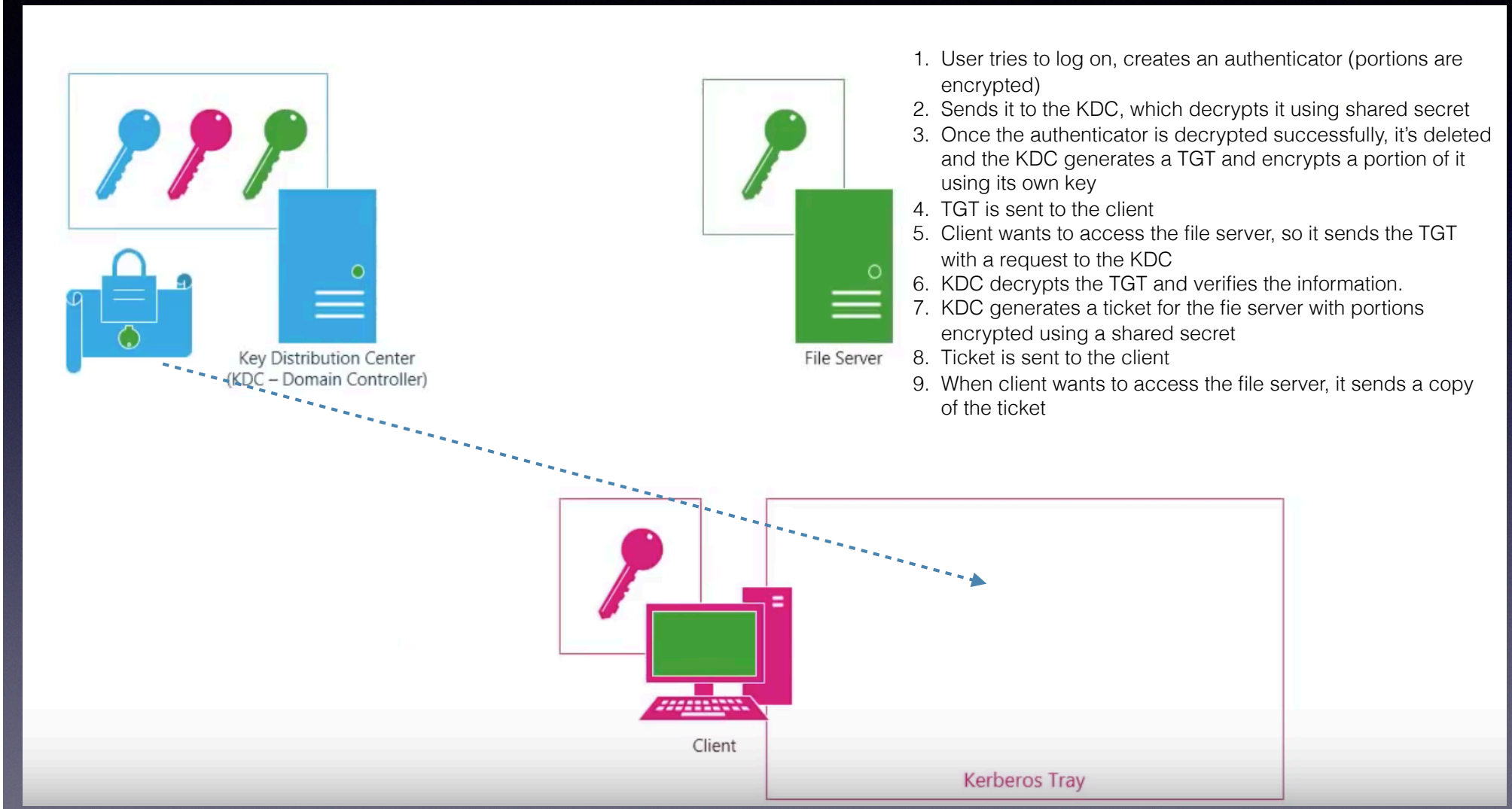
Kerberos Protocol



1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket

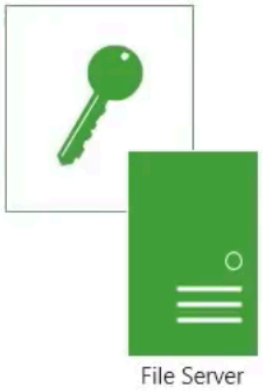


Kerberos Protocol

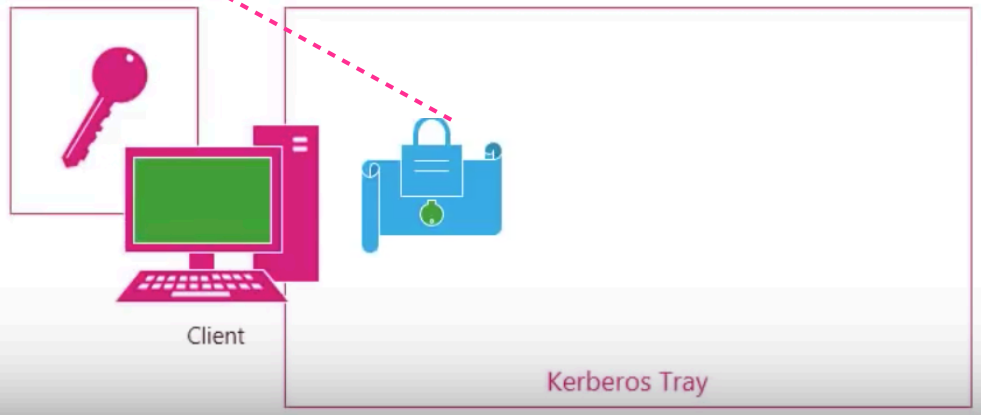


1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket

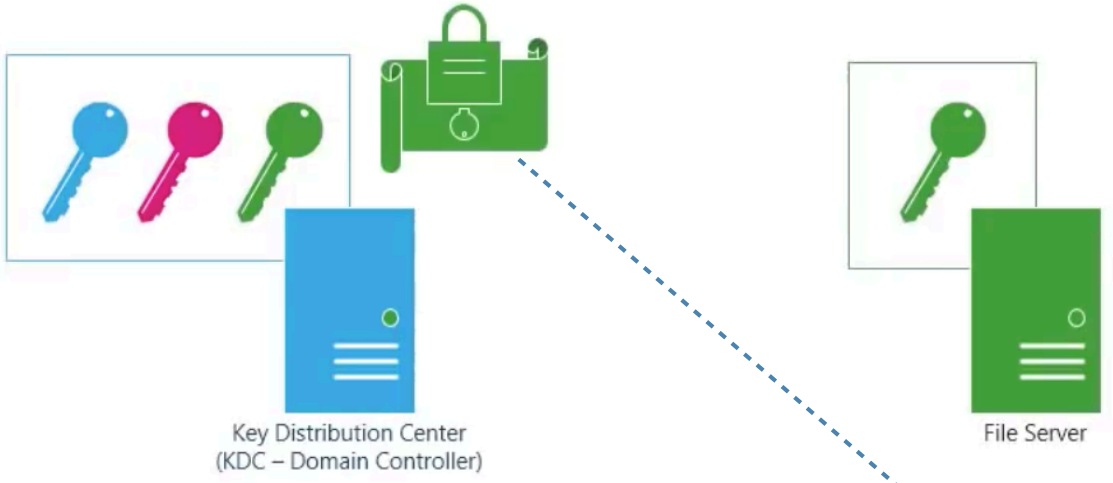
Kerberos Protocol



1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket

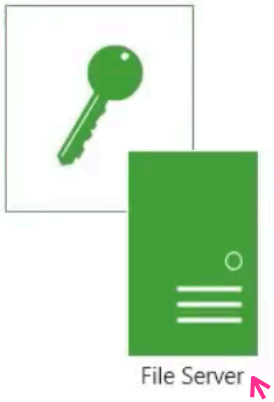


Kerberos Protocol

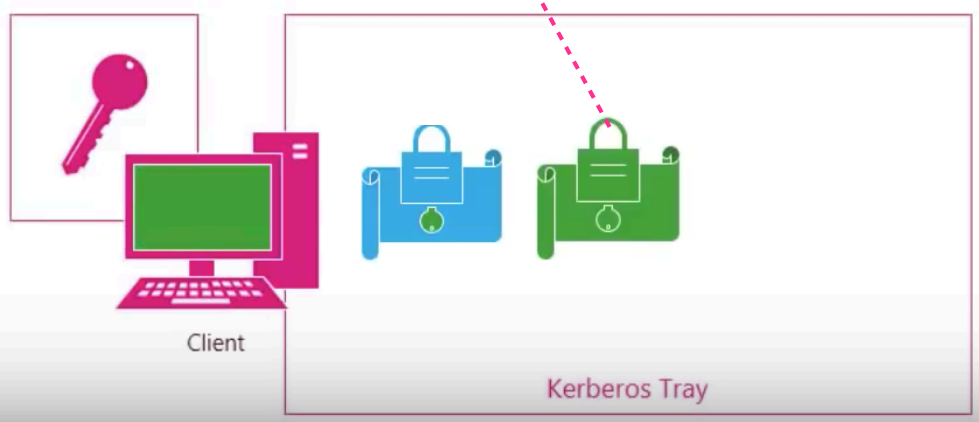


1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket

Kerberos Protocol



1. User tries to log on, creates an authenticator (portions are encrypted)
2. Sends it to the KDC, which decrypts it using shared secret
3. Once the authenticator is decrypted successfully, it's deleted and the KDC generates a TGT and encrypts a portion of it using its own key
4. TGT is sent to the client
5. Client wants to access the file server, so it sends the TGT with a request to the KDC
6. KDC decrypts the TGT and verifies the information.
7. KDC generates a ticket for the fie server with portions encrypted using a shared secret
8. Ticket is sent to the client
9. When client wants to access the file server, it sends a copy of the ticket



Kerberos

- Kerberos works as follows:

    1. The client sends an authentication request to the authentication server.
    2. The authentication server validates the user identity and grants a ticket granting ticket (TGT). The TGT validates the user identity and is good for a specific ticket granting server.
    3. When the client needs to access a resource, it submits its TGT to the TGS. The TGS validates that the user is allowed access, and issues a client-to-server ticket.
    4. The client connects to the service server and submits the client-to-server ticket as proof of access.
    5. The SS accepts the ticket and allows access.

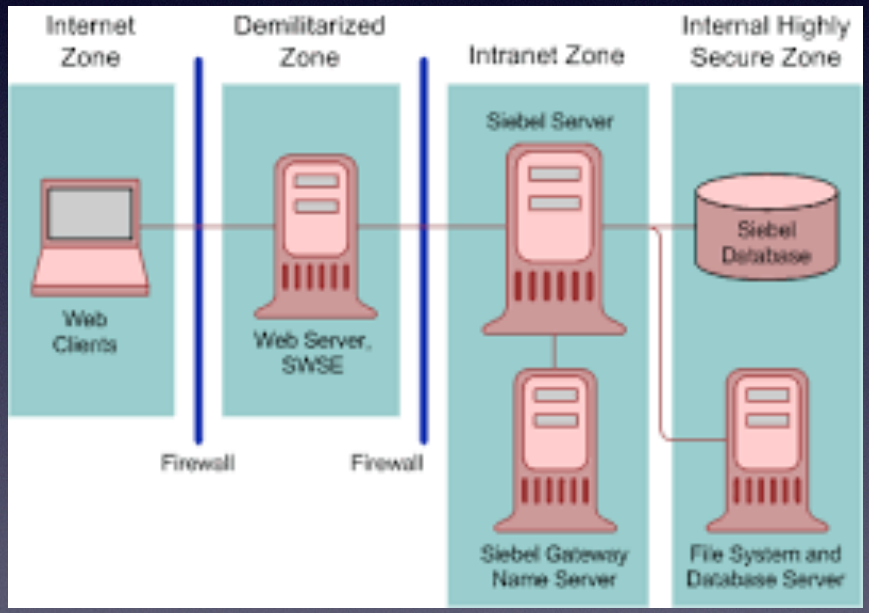
Kerberos

- Kerberos uses symmetric key cryptography.
- Tickets are valid during the entire session and do not need to be re-requested, thereby providing single sign-on, e.g., expire after 8hrs.
- Kerberos requires that all servers within the process have synchronised clocks
- Kerberos shares a different secret key with every entity on the network
- Knowledge of that secret key equals proof of identity (this system is called the *realm*).
- Kerberos uses TCP port 88.
- **Security issues with Kerberos:**
  - The KDC is a single point of failure.
  - Tickets are temporarily stored on the user's workstation and could be compromised.
  - Initial authentication is vulnerable to password guessing, the KDC cannot know if an attack is in progress.

Network Threats

Segmentation

- Main component of secure network architecture concepts is network segmentation
  - Limited damage if system compromised
  - Easier to identify suspicious network traffic
- Segment static IoT systems, wired from wireless, hosts from servers (DNS, Auth, SQL, etc.)
- Categorise systems into trust zones: zero, low, medium, high, very high
  - No trust -> no control == internet
  - Low trust (DMZ) -> some control, but internet facing == web server



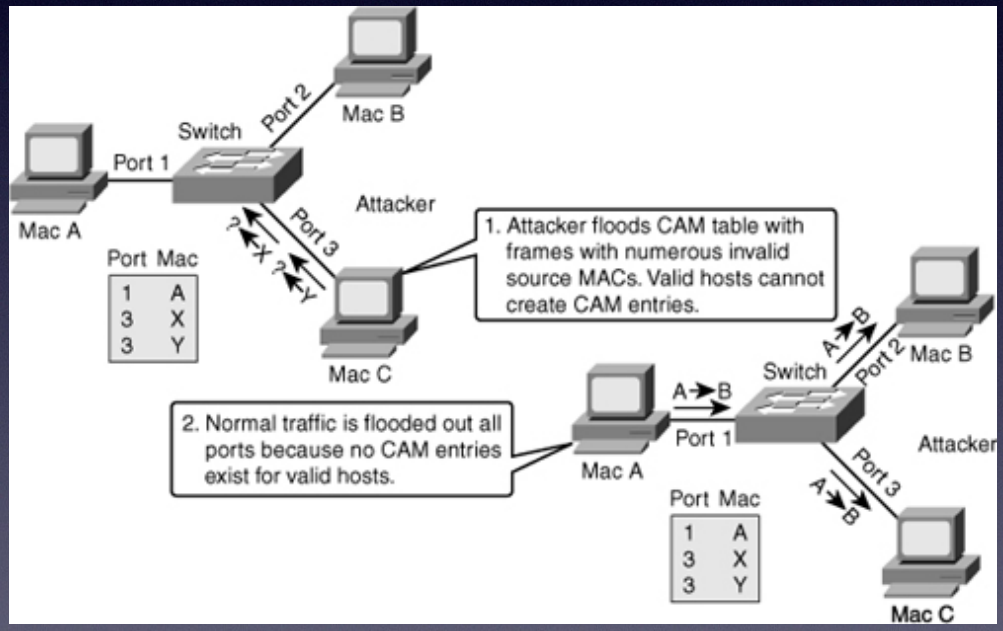
Network Threats

- Active: trying to compromise operations
- Passive: Sniffing - trying to intercept traffic
- External: From outside the network perimeter - attacker has 0 authorisation
- Internal: From inside the network perimeter - employees accessing unauthorised information
- Focus of security must be:
  - Entry points (public facing servers, workstations, wifi, personal devices)
  - Inherent vulnerabilities (legacy systems using old windows, IoT and SCADA)
  - Network baseline (now normal access and traffic patterns for anomaly detection)

L2 Attacks - MAC Flooding

- Overloads the switch's MAC forwarding table -> switch turns into a hub.

1. Attacker floods the switch with packets containing different src MAC.
2. Flood of packets fills up the forwarding table and consumes the memory -> switch enters fail open mode -> broadcasts all packets
3. Attacker captures all the traffic using a sniffer

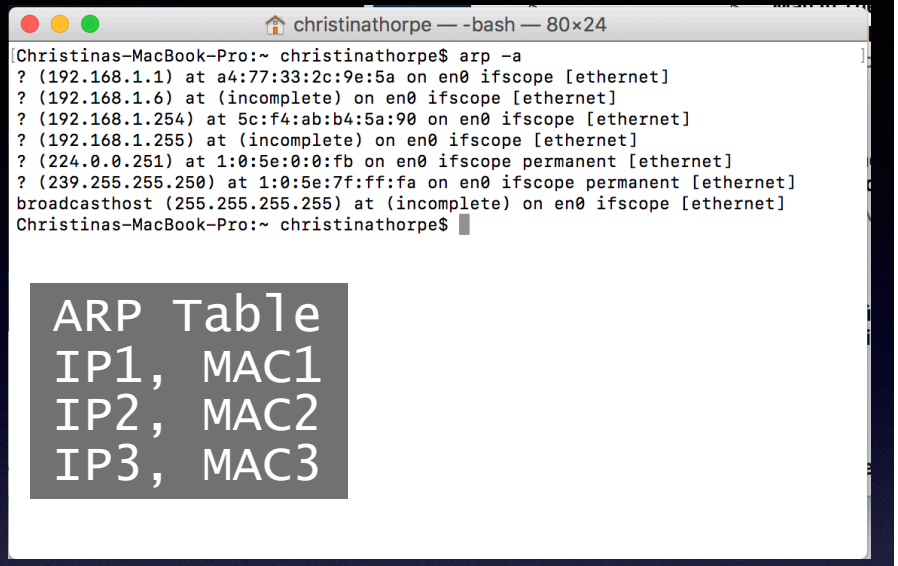


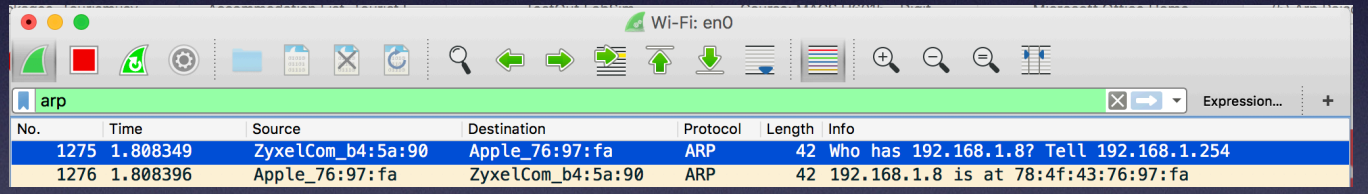
L2 Attacks - ARP Spoofing/Poisoning

Used to intercept communications going across a network (MITM)

Every computer has a unique ID - MAC address e.g, 00:04:5A:32:D4:FA (6 bytes)

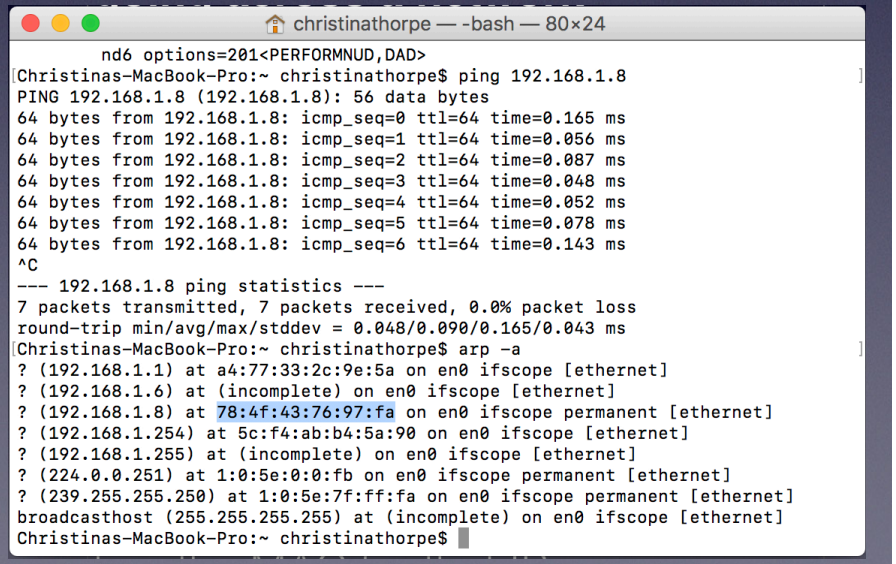
Every computer connected to a network has an ARP table





When hosts want to communicate with an IP, they can look up the ARP table to discover the MAC address

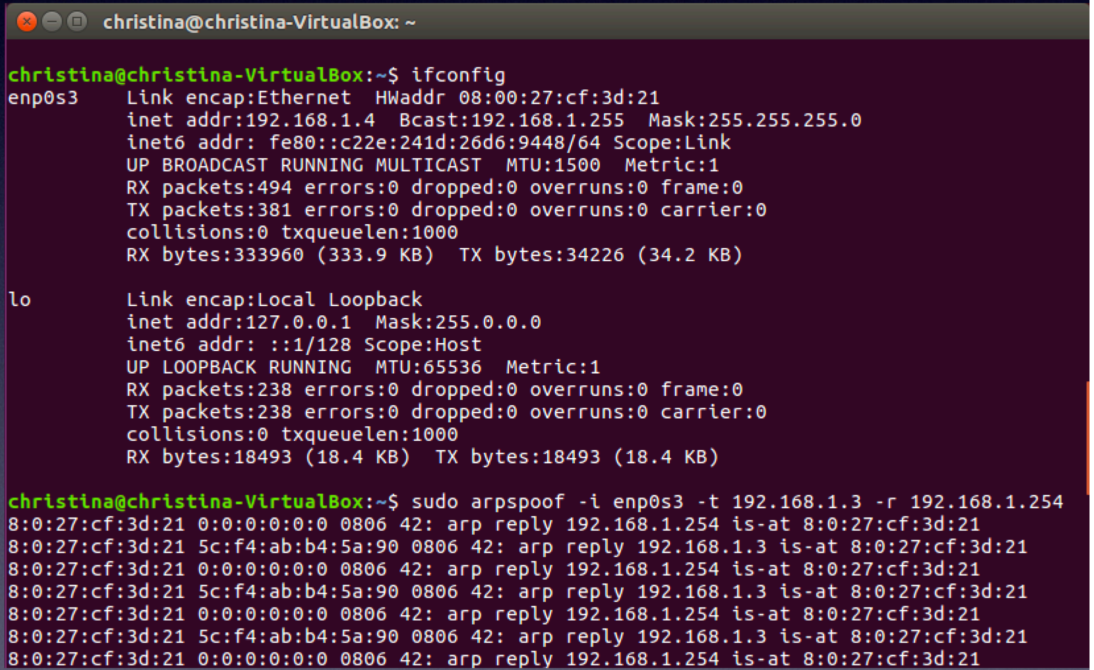
If not on the table, will broadcast an ARP MSG to the network to see who has the MAC for that IP.



L2 Attacks - ARP Spoofing/Poisoning

Associates the attacker's MAC with the IP of victim devices

1. Host sends ARP request to get MAC of known IP
2. Attacker responds with its MAC - (can be unsolicited)
3. Source sends frames to the attacker's MAC instead of correct device
4. **Switches don't verify MAC/IP association -> indirectly involved in attack**
5. Default gateway is the prime target - local traffic goes through GW to external networks.
    1. Passive Sniffing (forward traffic to GW)
    2. Man in the Middle (modify data before forwarding it, drop it)



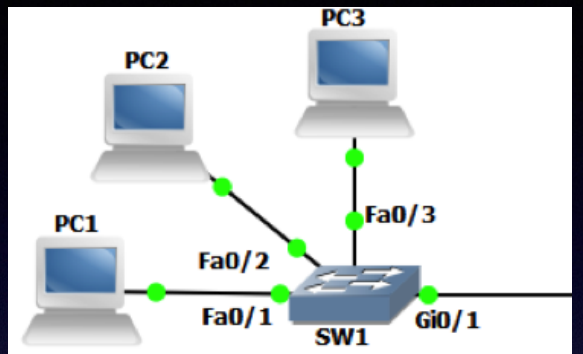
```
christina@christina-VirtualBox: ~
christina@christina-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:cf:3d:21
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c22e:241d:26d6:9448/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:494 errors:0 dropped:0 overruns:0 frame:0
          TX packets:381 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:333960 (333.9 KB)  TX bytes:34226 (34.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:238 errors:0 dropped:0 overruns:0 frame:0
          TX packets:238 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18493 (18.4 KB)  TX bytes:18493 (18.4 KB)

christina@christina-VirtualBox:~$ sudo arpspoof -i enp0s3 -t 192.168.1.3 -r 192.168.1.254
8:0:27:cf:3d:21 0:0:0:0:0:0 0806 42: arp reply 192.168.1.254 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 5c:f4:ab:b4:5a:90 0806 42: arp reply 192.168.1.3 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 0:0:0:0:0:0 0806 42: arp reply 192.168.1.254 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 5c:f4:ab:b4:5a:90 0806 42: arp reply 192.168.1.3 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 0:0:0:0:0:0 0806 42: arp reply 192.168.1.254 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 5c:f4:ab:b4:5a:90 0806 42: arp reply 192.168.1.3 is-at 8:0:27:cf:3d:21
8:0:27:cf:3d:21 0:0:0:0:0:0 0806 42: arp reply 192.168.1.254 is-at 8:0:27:cf:3d:21
```

L2 Attack MAC Spoofing

Changing the source MAC address on frames sent by attacker

- Used to bypass 802.1x port security and MAC filtering
- Hides the identity of attacker machine (or fakes identity)

1. Attacker machine sends frames with spoofed MAC
2. Switch associates the MAC to the port the attacker is connected



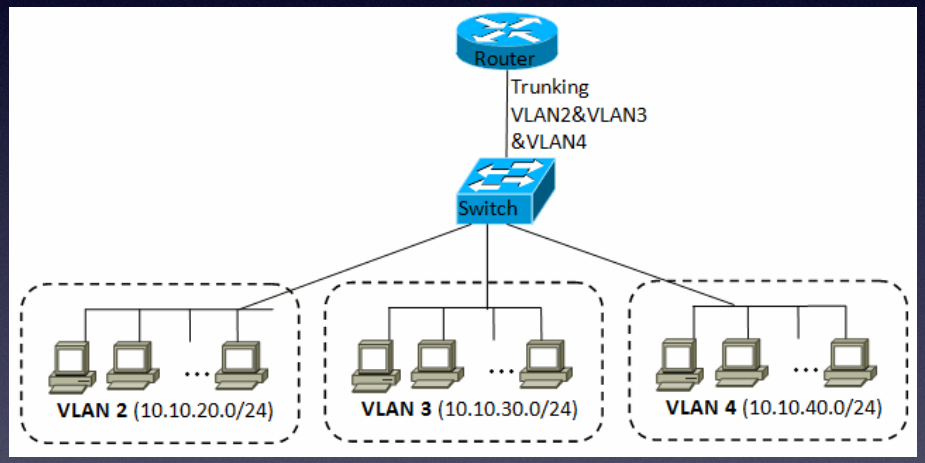
SW1# show mac address-table dynamic
Mac Address Table

Vlan	Mac Address	Type	Ports
20	0200.1111.1111	DYNAMIC	Fa0/1
20	0200.2222.2222	DYNAMIC	Fa0/2
20	0200.3333.3333	DYNAMIC	Fa0/3

```
christina@christina-VirtualBox: ~
christina@christina-VirtualBox:~$ ifconfig | grep HWaddr
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:cf:3d:21
christina@christina-VirtualBox:~$ ifconfig enp0s3 down
SIOCSIFFLAGS: Operation not permitted
christina@christina-VirtualBox:~$ sudo ifconfig enp0s3 down
[sudo] password for christina:
christina@christina-VirtualBox:~$ ifconfig enp0s3 hw ether de:ea:be:ef:c0:fe
SIOCSIFHWADDR: Operation not permitted
christina@christina-VirtualBox:~$ sudo ifconfig enp0s3 hw ether de:ea:be:ef:c0:f
e
christina@christina-VirtualBox:~$ sudo ifconfig enp0s3 up
christina@christina-VirtualBox:~$ ifconfig | grep HWaddr
enp0s3    Link encap:Ethernet  HWaddr de:ea:be:ef:c0:fe
christina@christina-VirtualBox:~$
```

Switch Security - VLAN

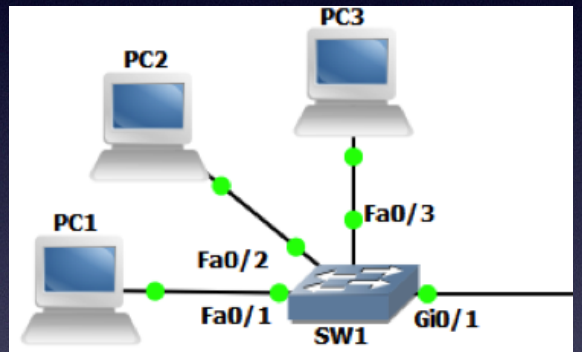
- VLAN - logical grouping of computers based on switch port (membership configured by assigning a port to VLAN)
  - Switch can have multiple VLANs, but port can only be member of 1 (one exception). VLANs can span multiple switches
  - Trunk port connects two switches together, member of a VLANs on switch.



  - Frames travelling between switches on trunk ports are tagged with an ID so receiving switch knows to which VLAN the frame belongs
  - Typically, hosts on 1 VLAN can't communicate with hosts on another. Router must be used to enable inter-VLAN communication.
  - VLANs can be used to create multiple broadcast domains.

Switch Security - MAC filtering

- MAC filtering restricts the devices that can connect through a port
  - MAC/port associations are stored in a table in RAM on switch
  - Table can be configured manually or built by learning devices
  - Can configure 1 or multiple allowed MACs per port
  - Can limit the number of MACs in automatic config
  - Port violation occurs when unauthorised device tries to connect
    - Switch can drop frames/shut down the port

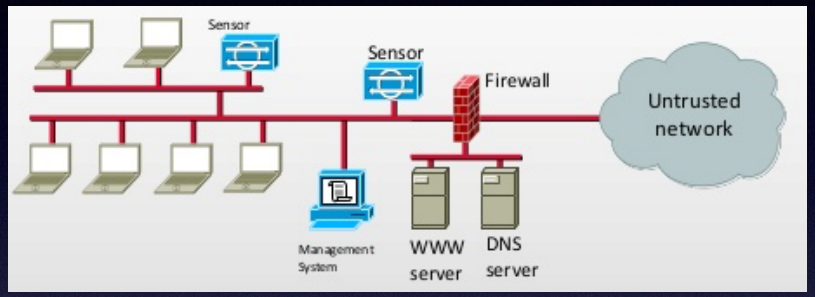



```
SW1# show mac address-table dynamic
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  20    0200.1111.1111    DYNAMIC     Fa0/1
  20    0200.2222.2222    DYNAMIC     Fa0/2
  20    0200.3333.3333    DYNAMIC     Fa0/3
```

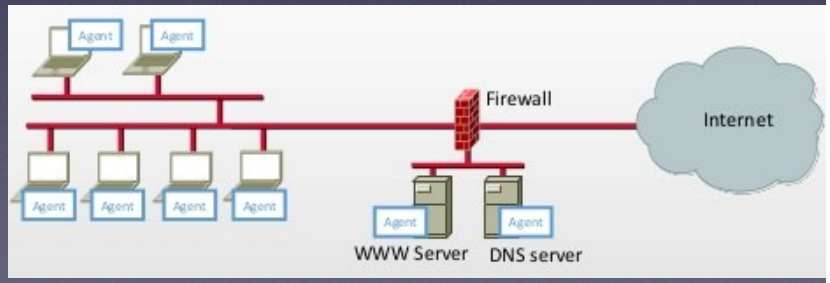
Intrusion Detection System

- An *intrusion detection system* is a network device that can detect attacks
- Uses multiple data sources to find attacks (audit files, systems logs, and real time traffic)
- A *sensor* passes data from the data source to the analyzer.
- The *engine* analyzes sensor data and events, generates alerts (indicates event of interest), and logs activity.
- The IDS labels traffic based on its interpretation of whether or not the traffic poses a threat
  - ***Positive, Fase positive, Negative, False negative***
- IDS can miss frames when the network is too busy.
- Logs become unreliable if the system is compromised -> attacker may have modified the log files.
- Stopping the intrusion is often more important than continuing trying to gather information on the attacker

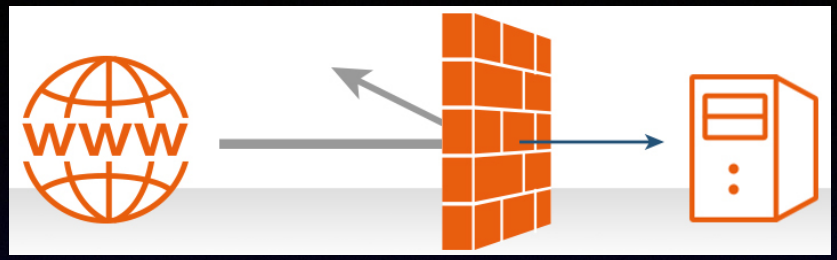
Network-based



Host-based



Firewall

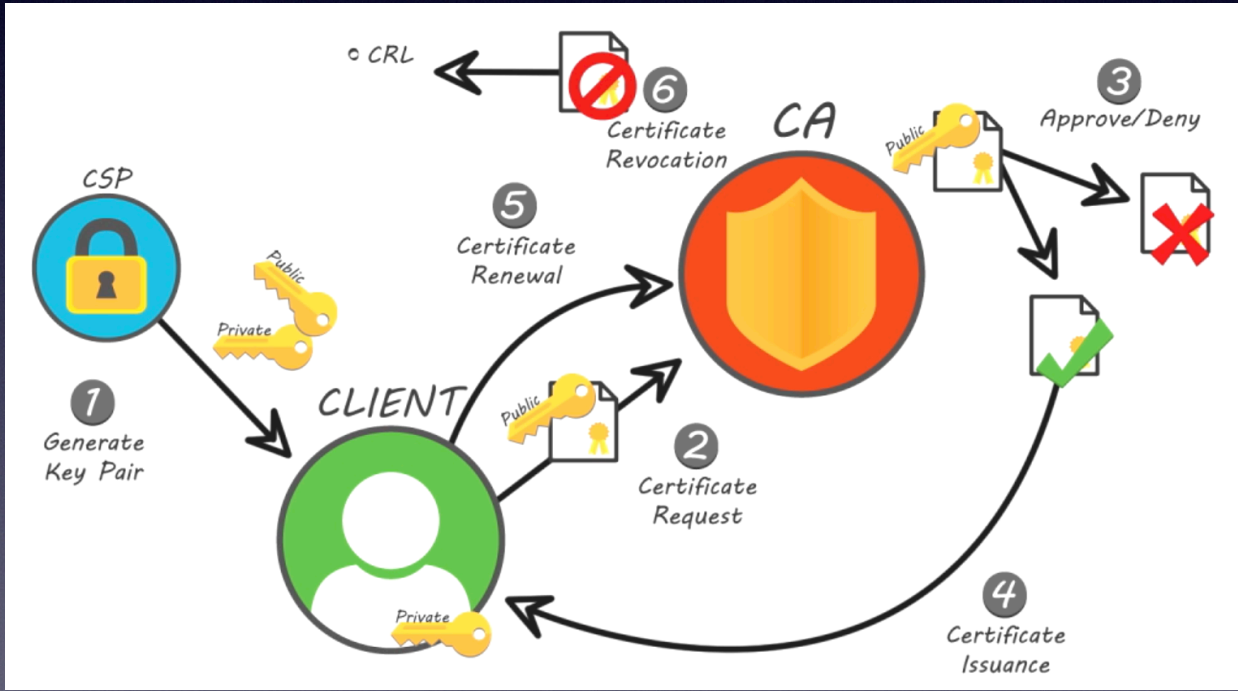


- A *firewall* is a device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules.
- A network-based firewall inspects traffic as it flows between networks.
- A host-based or application-based firewall inspects traffic received by a host.
- Firewalls use filtering rules, sometimes called access control lists (ACLs), to identify allowed and blocked traffic.
    - The interface, direction (inbound or outbound), Pkt info, action
- Can protect against many external attacks (not spoofed email)
- Can impede network availability - adds processing overhead, may drop pkts
- Main types: packet filtering (L3, pkt only), stateful (L5, session), application (L7)

Secure Protocols

Digital Certificates

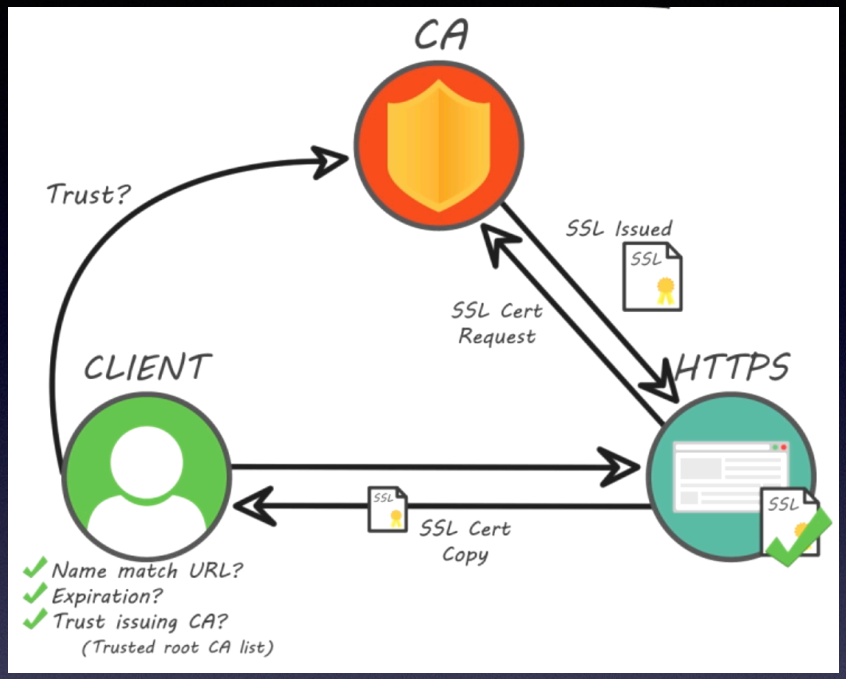
- A *digital certificate/*public key certificate/identity certificate, is an electronic document that uses a digital signature to bind a public key with an identity.
- A *public key infrastructure* (PKI) is a hierarchy of computers that issues and manages certificates.
- A Certificate Authority (CA) is the entity that issues certificates



1. The key pair is generated by an application called a cryptographic service provider (CSP)
2. The client requests a certificate from a CA, sending identifying information and a copy of the public key
3. The CA performs identity proofing by verifying the information submitted to prove identity
4. If the certificate request is approved, the certificate is issued to the client.
5. Certificates are issued with a valid lifetime period.
6. If a certificate becomes compromised, such as the private key being lost or stolen, it can be revoked.

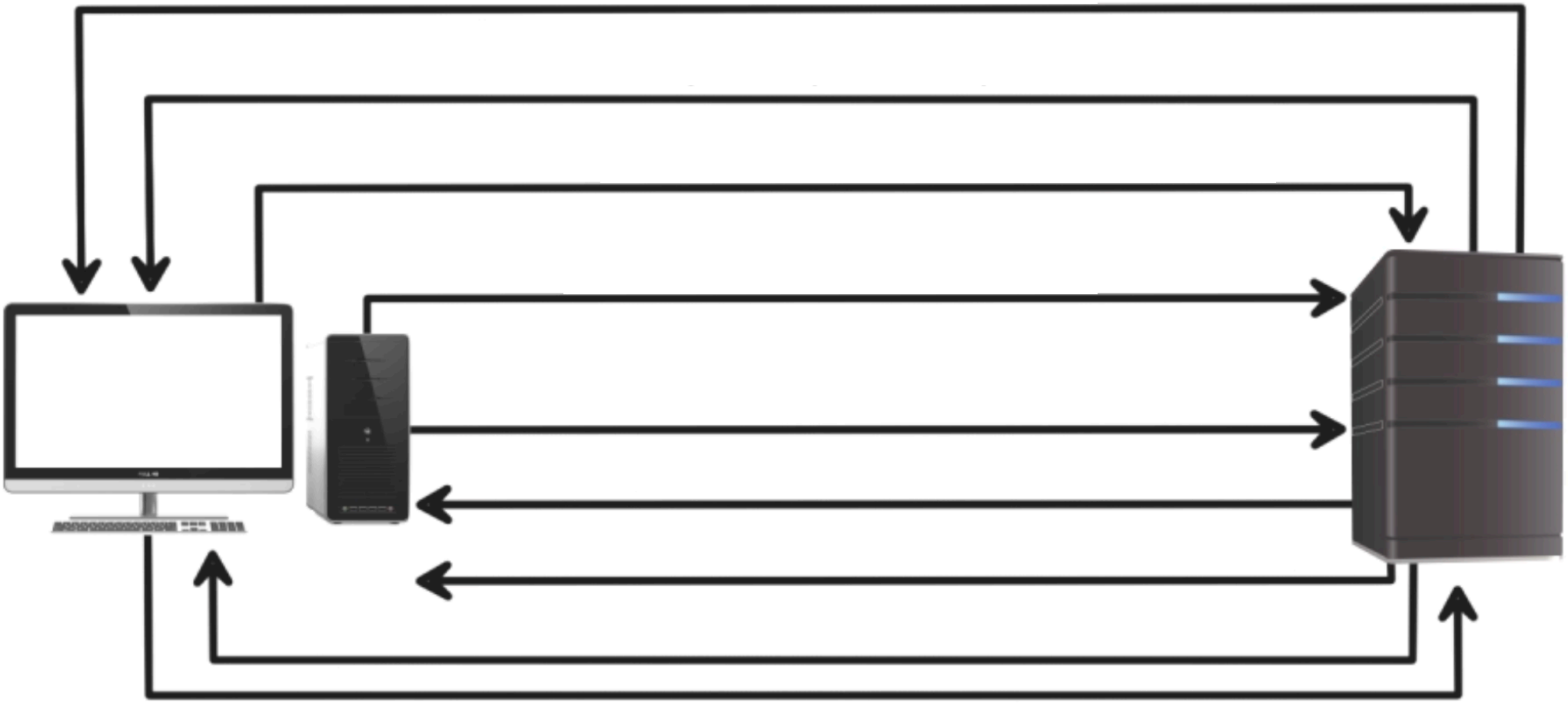
Secure Socket Layer

- SSL secures messages transmitted on the Internet.
- Uses the SSL Handshake Protocol to establish the secure channel.
- Provides an end-to-end encrypted tunnel that is impossible to monitor, scan, or sniff.
- Requires the server to have a certificate issued by a CA and uses asymmetric encryption.
- Uses RSA or the Key Exchange Protocol (KEA) for secure exchanging of encryption keys.
- Operates at the Session layer (layer 5) of the OSI model. Port 443



1. The client checks the server's certificate validity period (stops if outside)
2. The client compares the name on the certificate with the name on the URL.
3. The client verifies that the issuing Certificate Authority (CA) is on its list of trusted CA's.
4. The client uses the CA's *public* key to validate the CA's digital signature on the server certificate.
5. If the digital signature can be verified, the client accepts the server certificate as a valid certificate
6. A session key is used between the client and the server for the duration of the SSL session.
7. If all checks are successful, the client continues with the SSL handshake process.

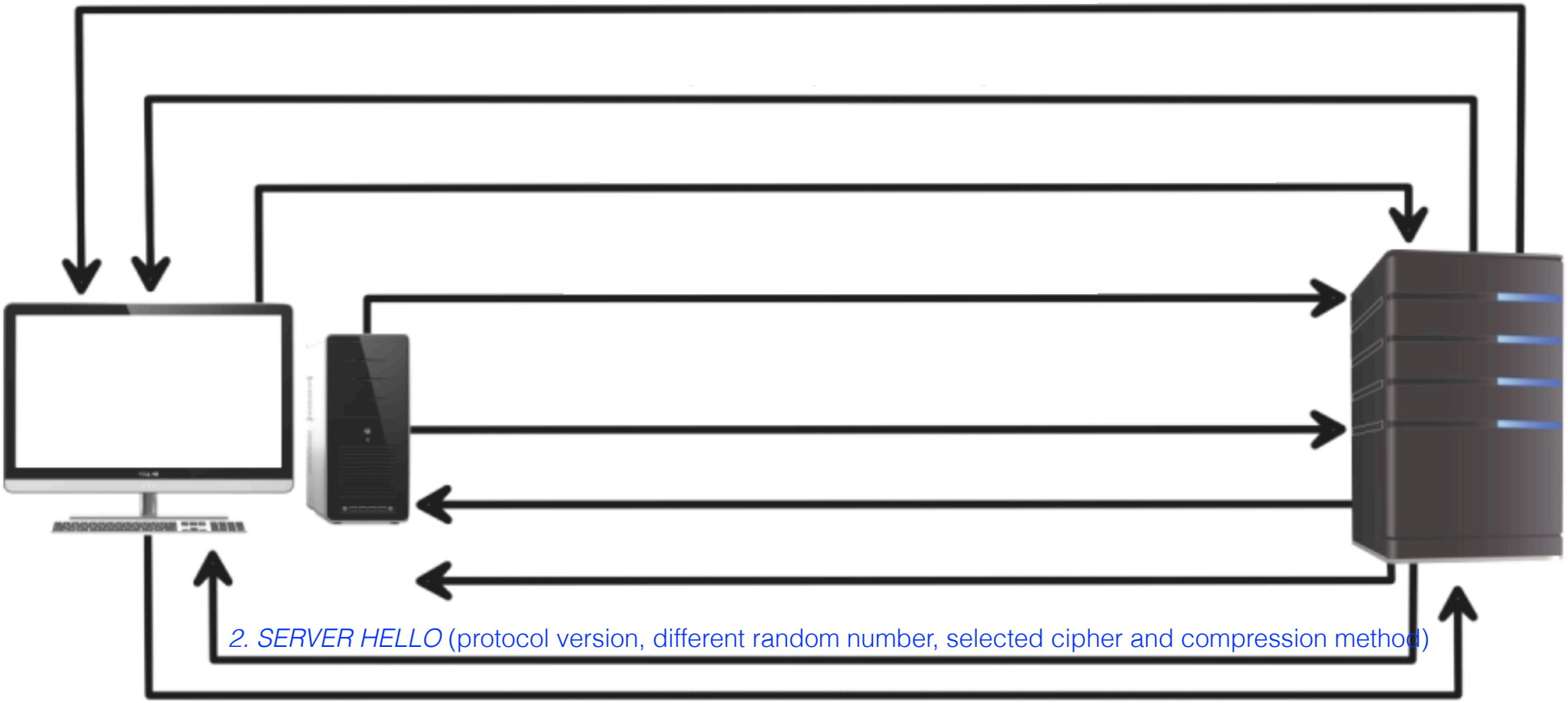
SSL/TLS Handshake



1. CLIENT HELLO (Highest SSL/TLS, random number, a list of ciphers, and compression methods)

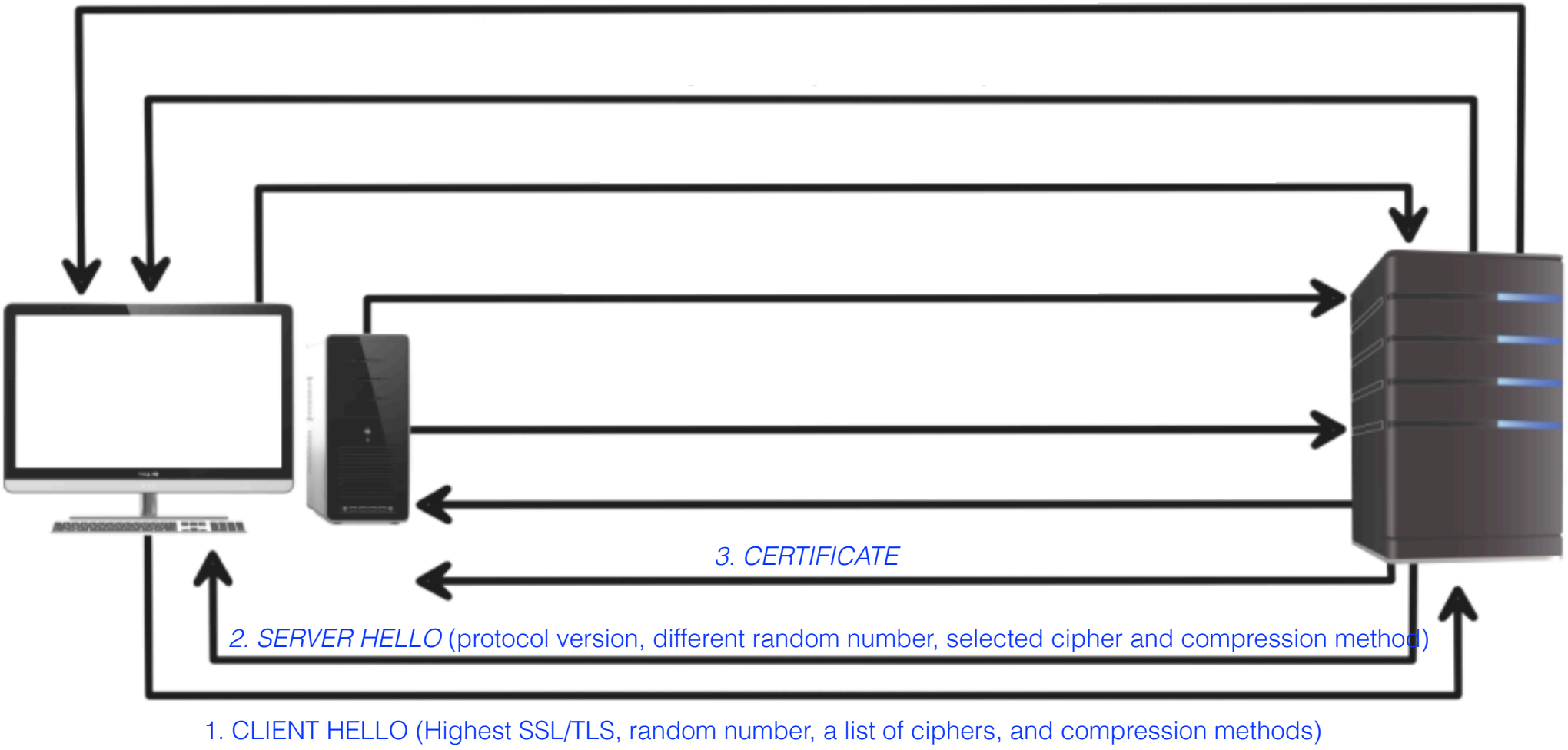
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



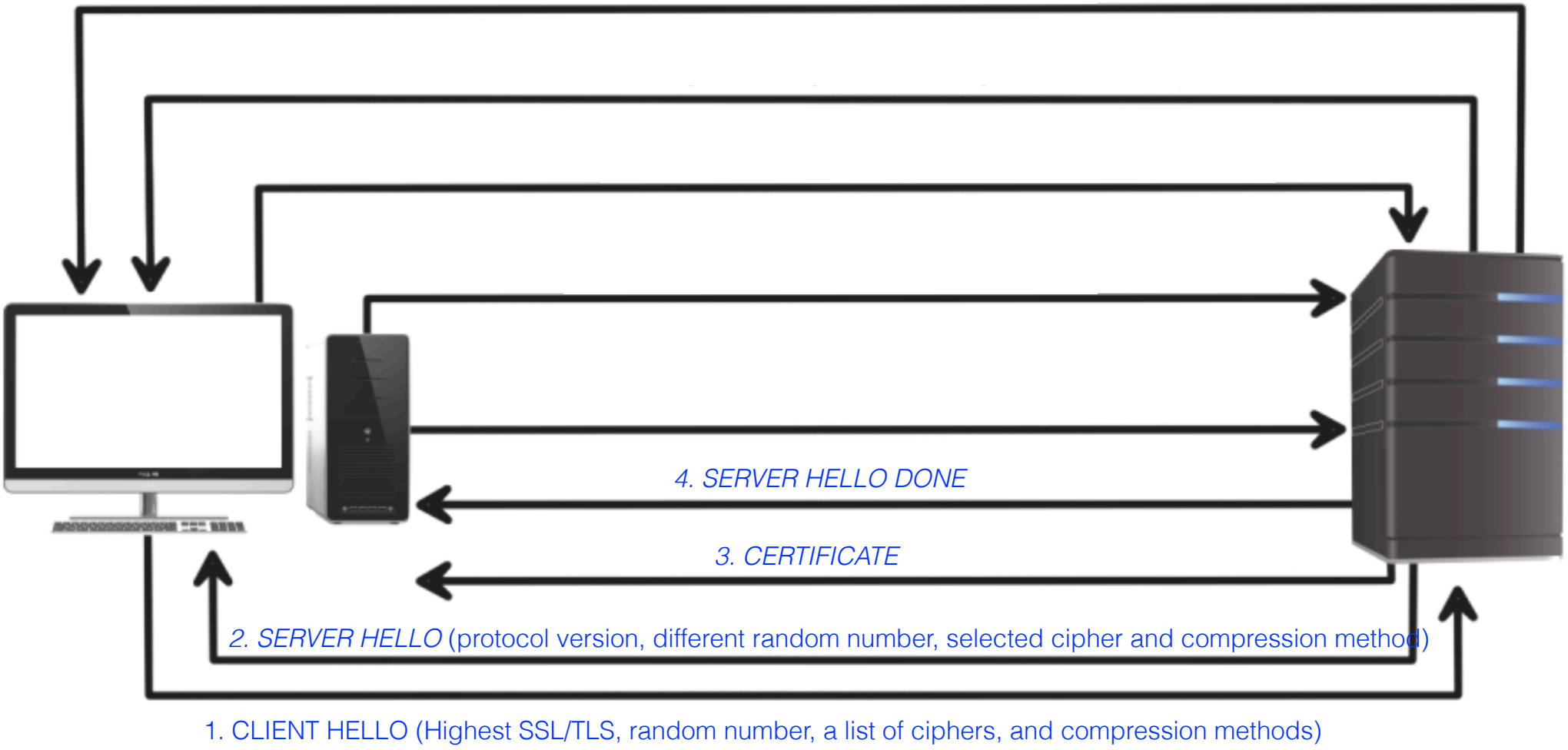
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



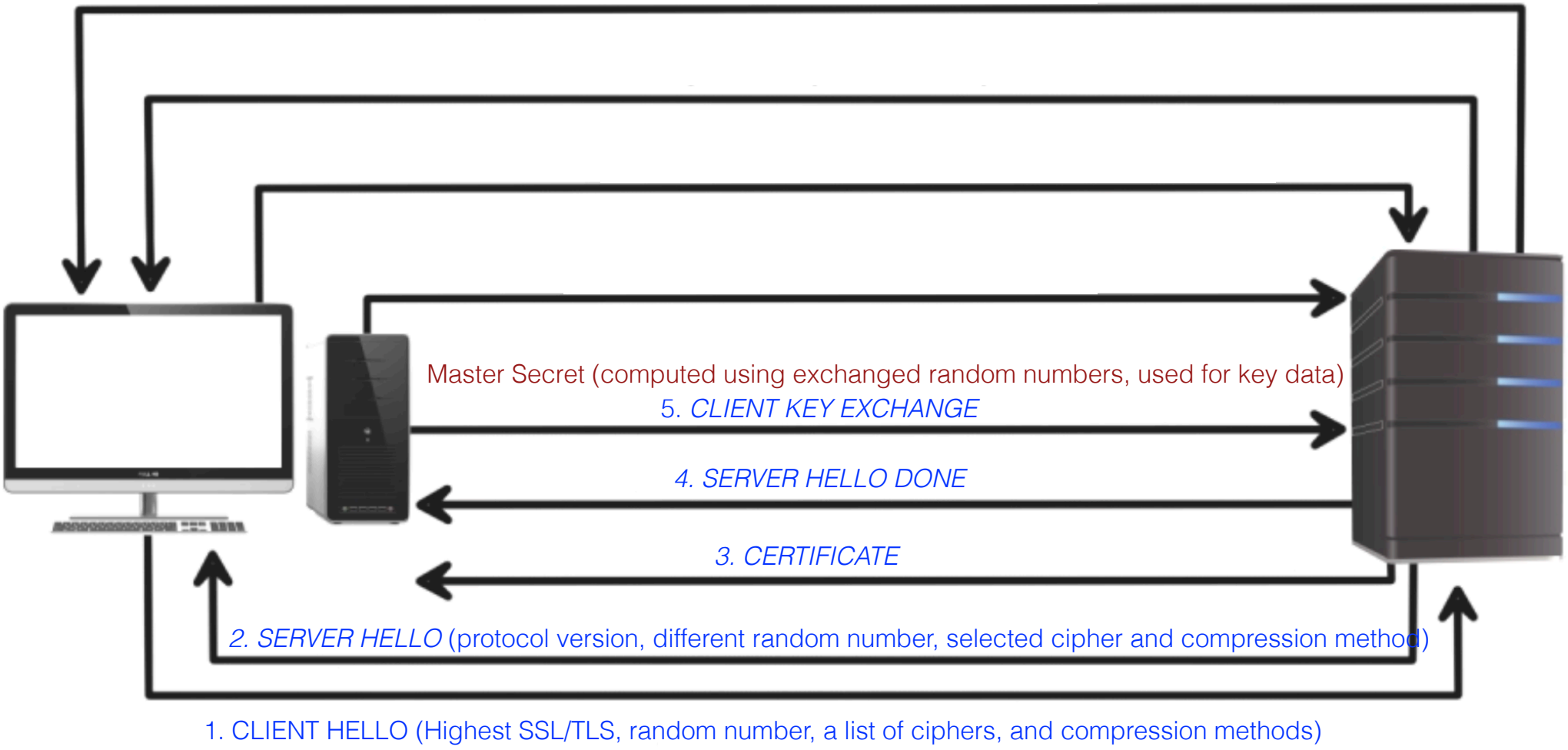
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



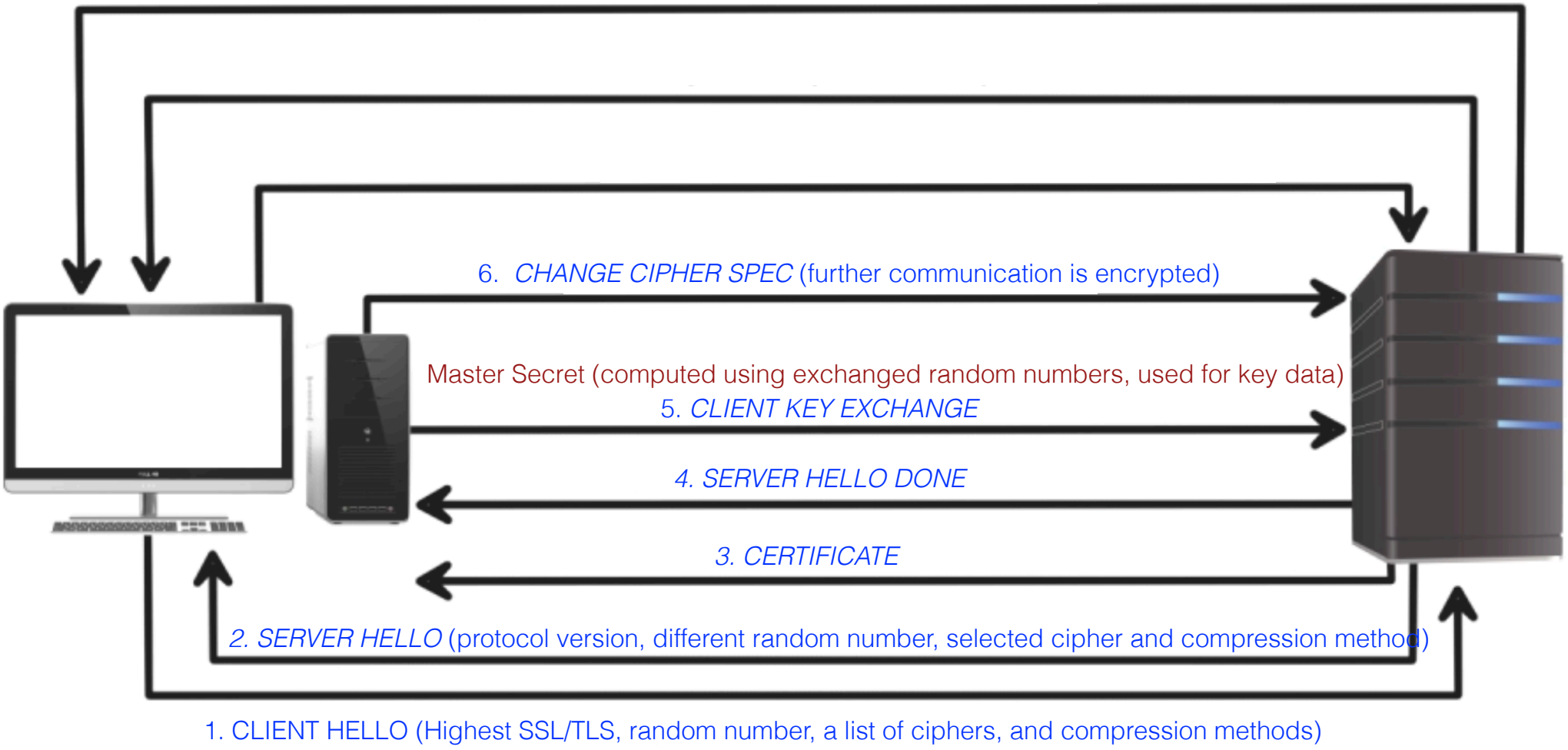
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



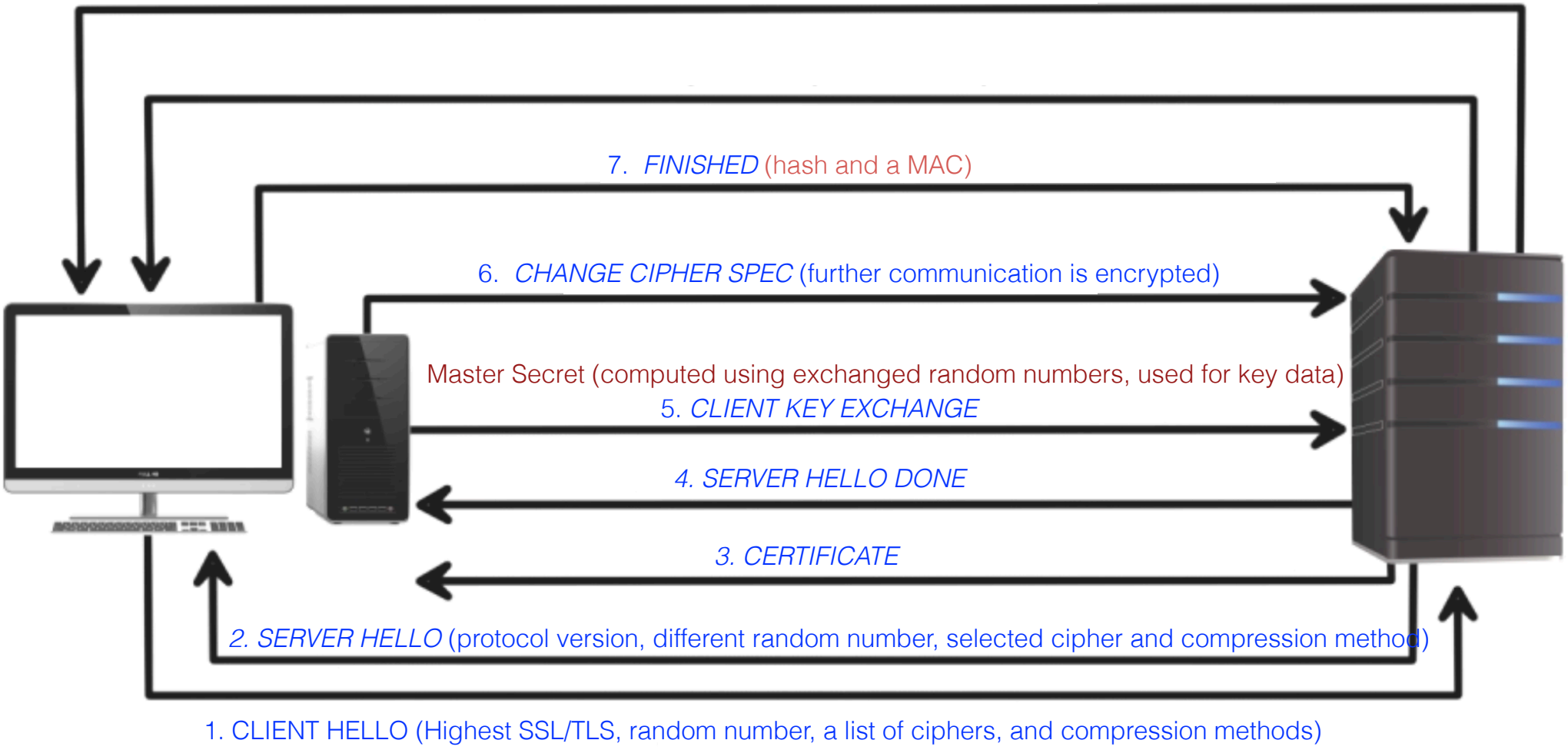
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



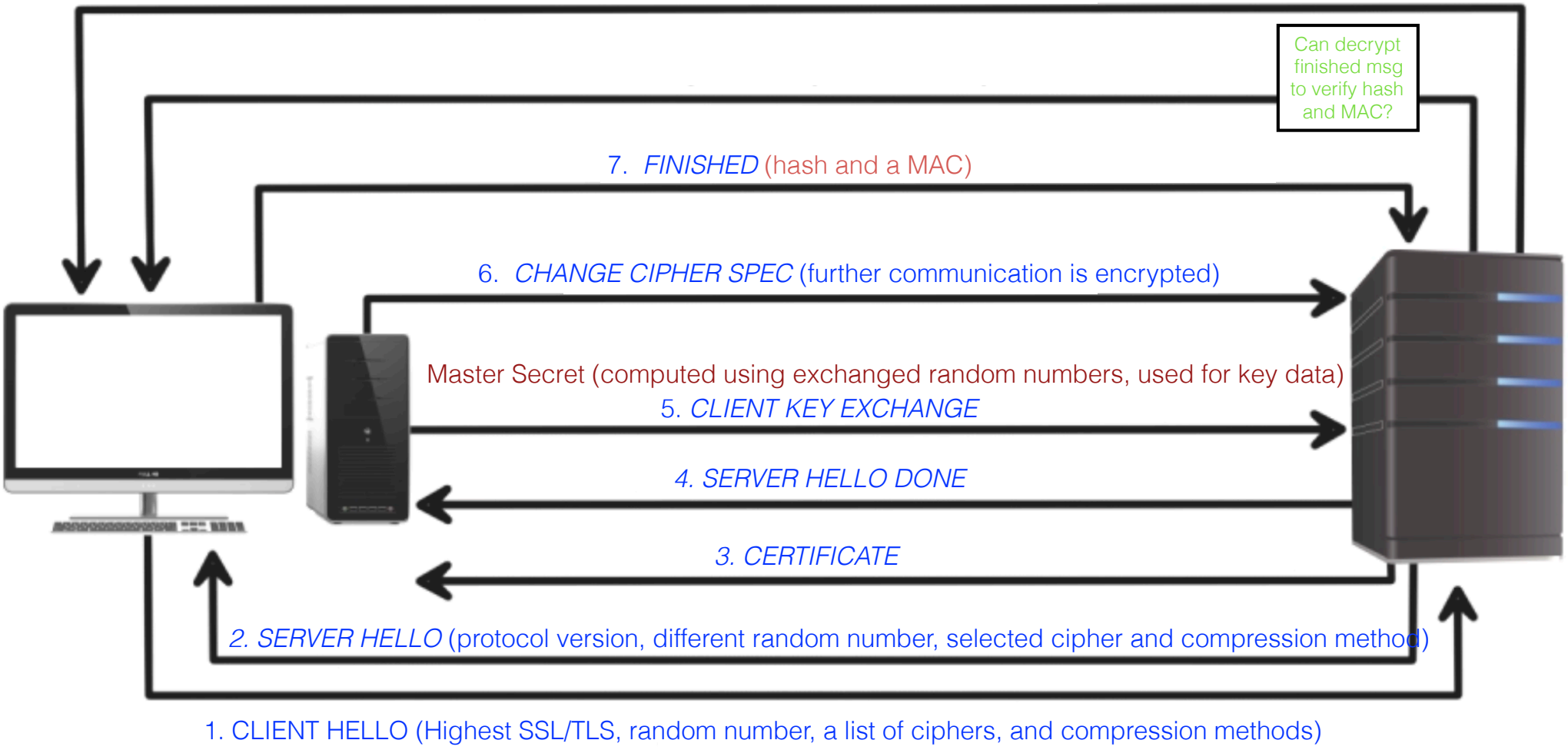
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



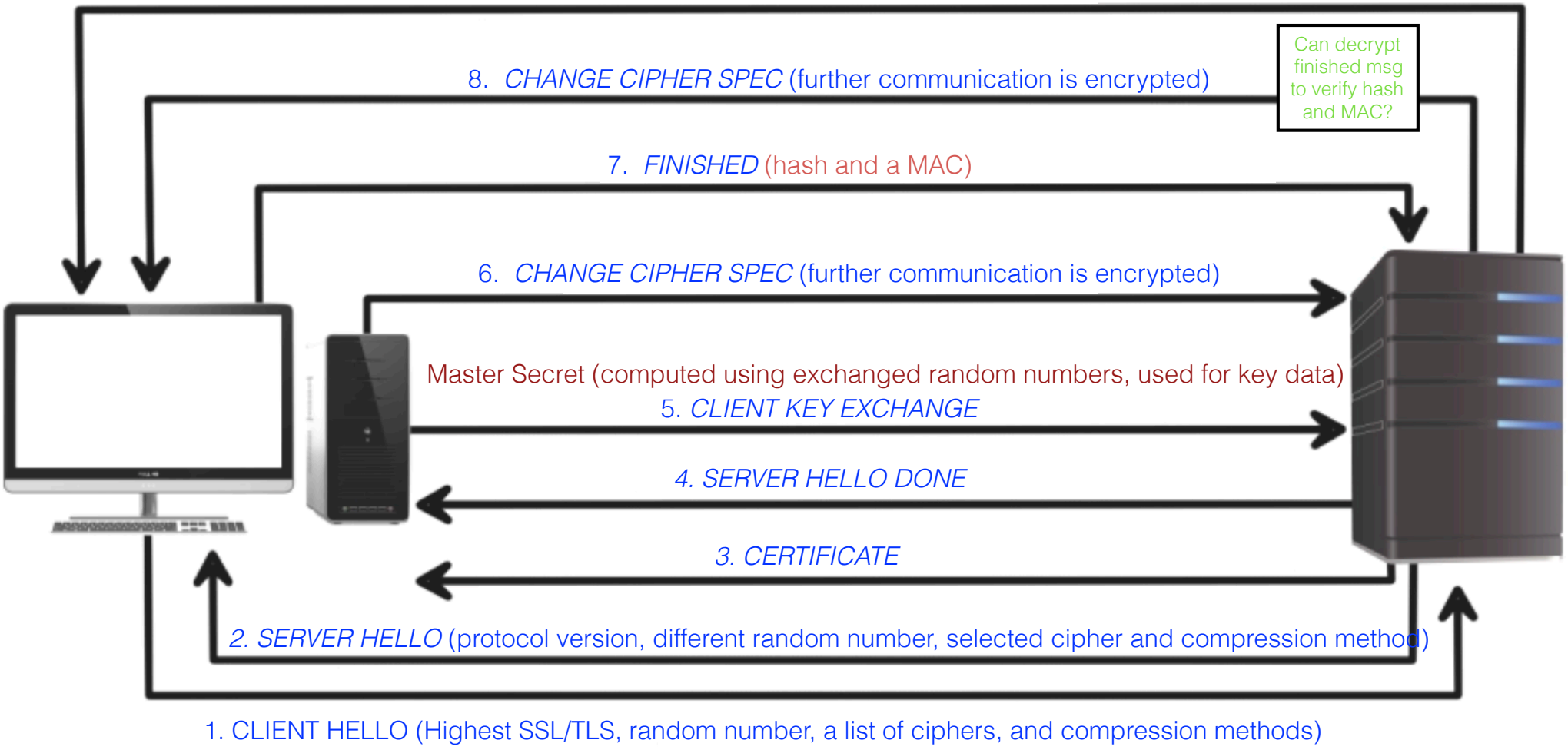
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



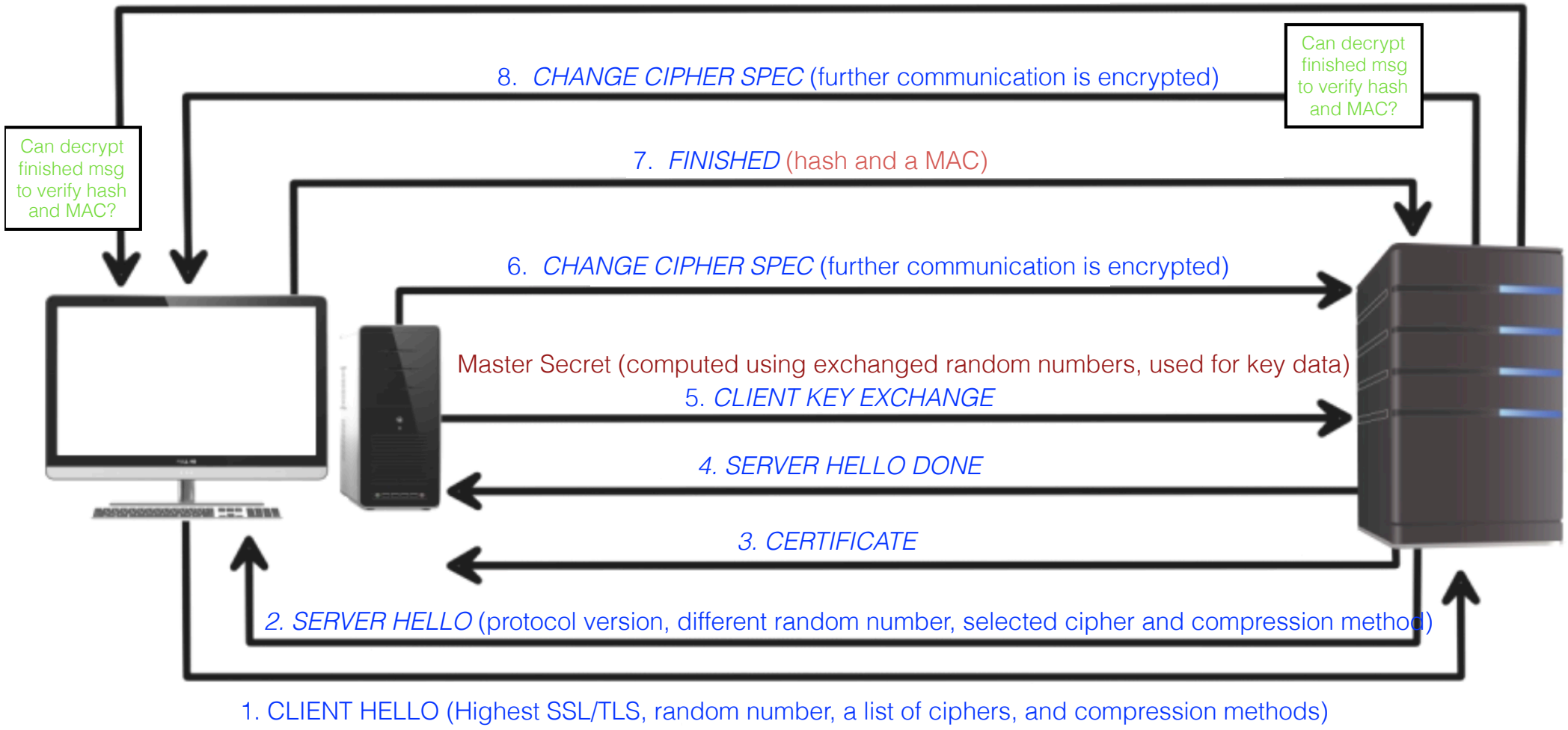
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



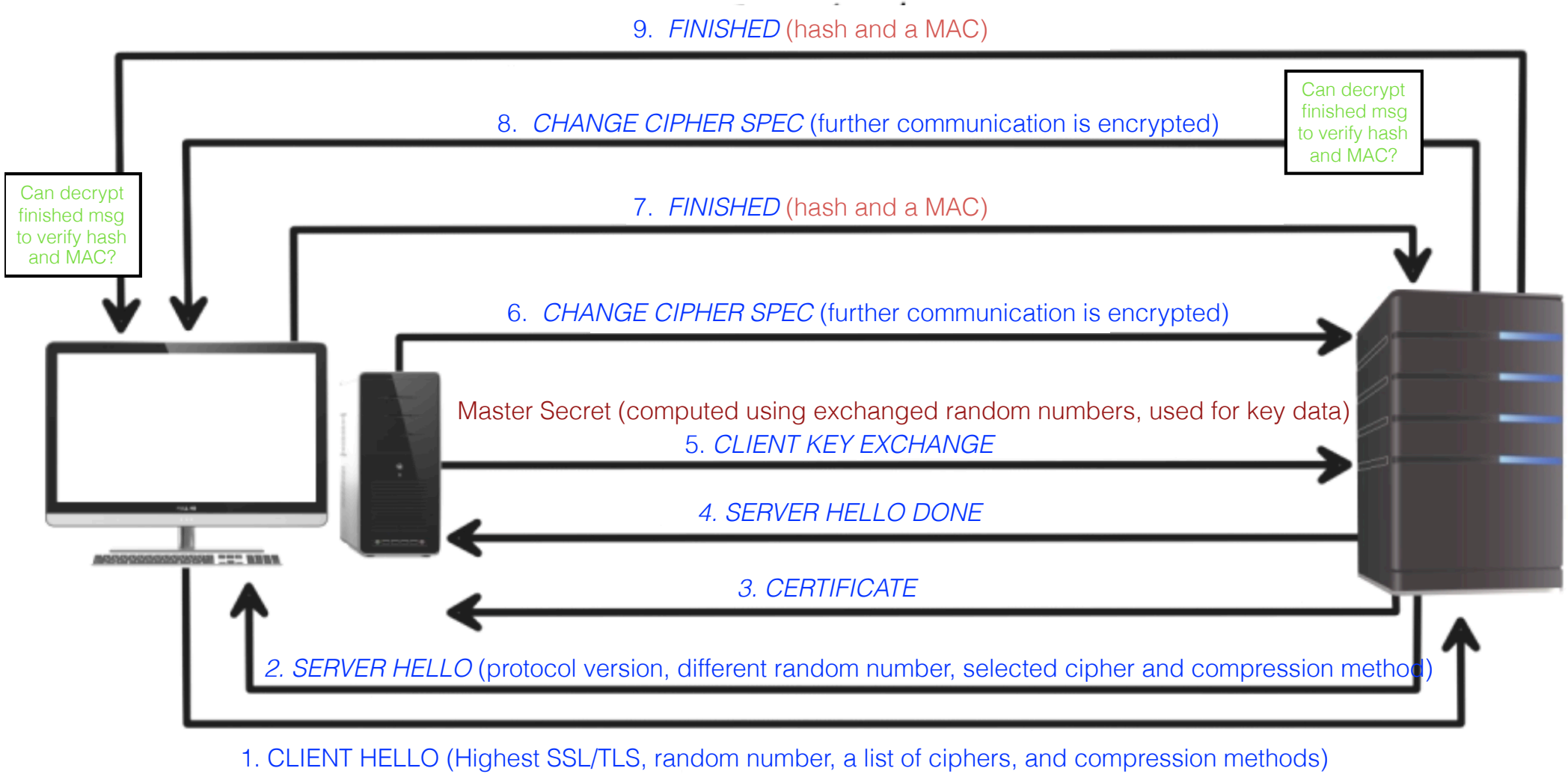
- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

SSL/TLS Handshake



- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

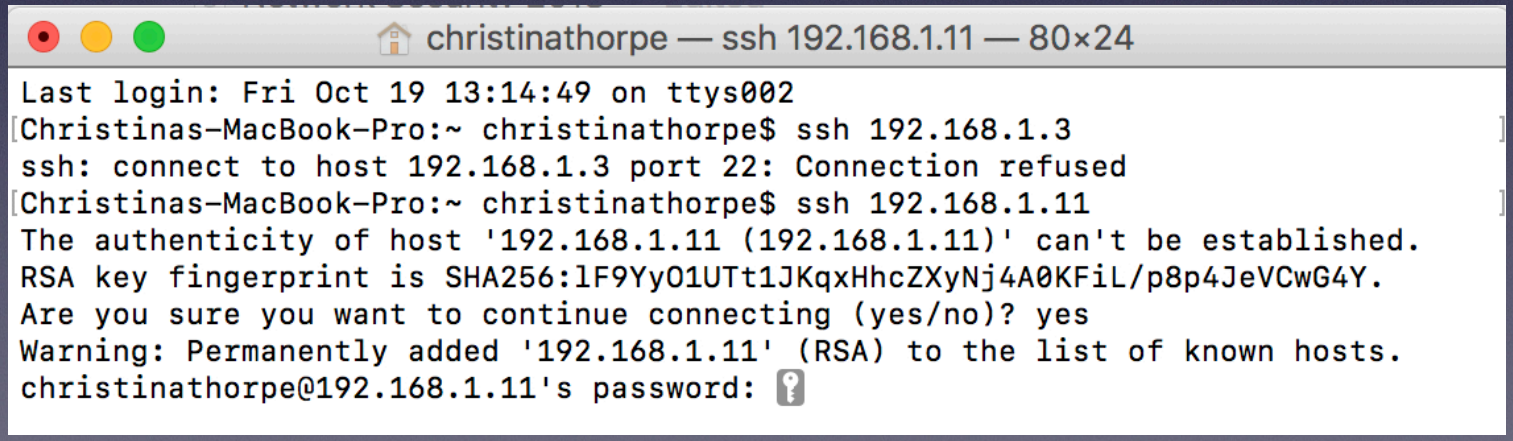
SSL/TLS Handshake



- Transport Layer Security (TLS) is the successor to SSL 3.0 (similar, but not compatible. Applications can use both.

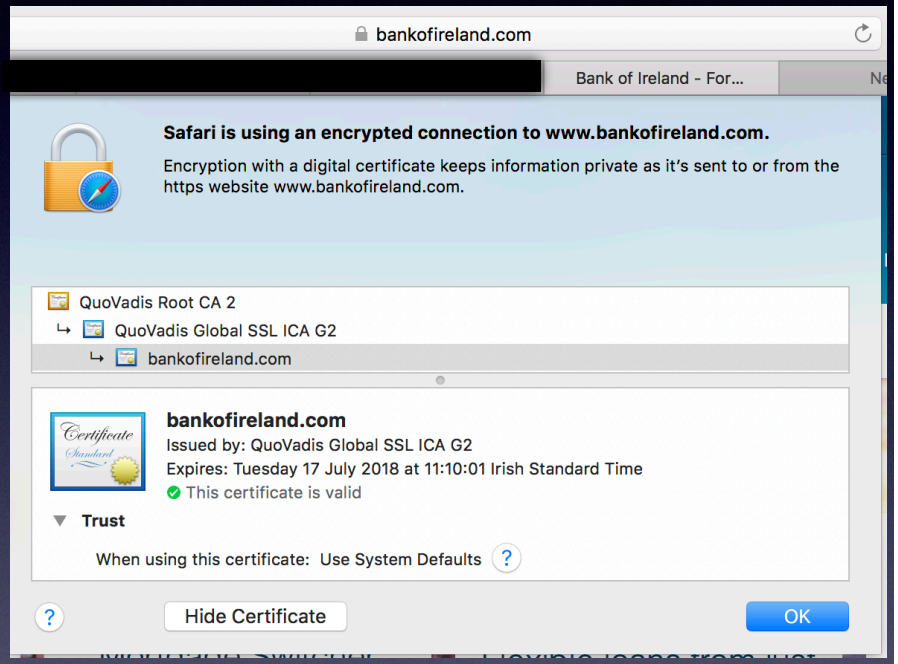
SSH

- SSH allows for secure interactive control of remote systems
  - SSH uses RSA public key cryptography for both connection and authentication.
  - SSH uses the IDEA algorithm for encryption by default, but is able to use Blowfish and DES.
  - SSH is a secure and acceptable alternative to Telnet.
  - SSH is used by unsecured protocols to establish a secure channel. For example, SFTP and SCP are secure file copy protocols that use SSH.



HTTPS

- Hyper Text Transfer Protocol Secure (HTTPS) is a secure form of HTTP that uses either SSL or TLS
  - Is stateful, which means that it keeps track of the client (same HTTPS server for the duration of the session, no load balancing)
  - Requires TCP port 443 inbound on the Web server to be open.
  - Can be identified by verifying that the URL starts with *https://*, or by looking for a lock symbol in the browser. Double clicking on the lock icon will display the certificate.

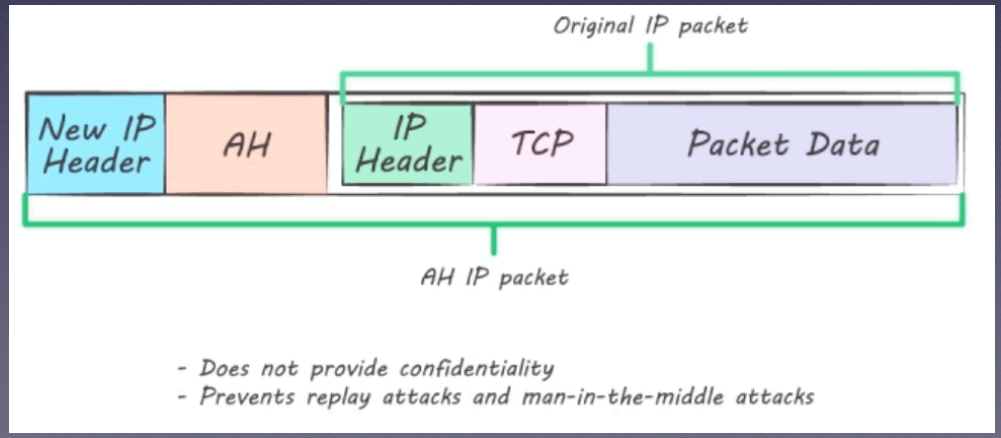


IPSec (L3)

- IP Security (IPSec) provides secure data transmission over unprotected TCP/IP.
- It provides mutual authentication, integrity, non-repudiation and confidentiality
- Two protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- There are **two** modes of operation that can be implemented with IPSec:
  - *Transport mode* - encrypts only the payload (data).
  - *Tunnel mode* - encrypts the entire packet. Both the data inside the packet and the IP headers are encrypted - encapsulated in a new packet.
- A Security Association (SA) is the establishment of shared security information between two network entities to support secure communications.
  - May include algorithm selection, cryptographic keys and/or digital certificates.
  - Can be established manually or automatically through a protocol called Internet Key Exchange (IKE)

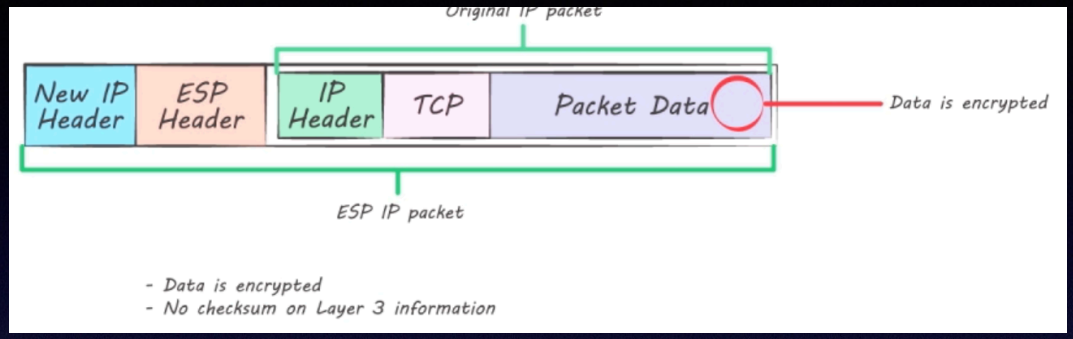
IPSec Protocols

- AH (port 51) provides authenticity, non-repudiation, and integrity.
  - Does *not* provide confidentiality because the data in the packet is not encrypted.
  - Provides protection against replay and man-in the-middle attacks.
  - Uses a *keyed hash* based on all the bytes in the packet for the authentication information.
  - Authenticates packets by digitally signing them.



IPSec Protocols

- ESP (port 50, most common protocol) provides all the security of AH plus confidentiality.
  - Provides data encryption



- IKE (UDP port 500):
  - Provides a secure exchange of shared keys before a full IPSec transmission begins (tunnel setup).
  - Uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived.
  - Uses mutual authentication that is provided by either pre-shared keys on both endpoints or certificates issued by a CA.
  - Can be implemented to automate the selection of the best security association for each connection.
  - Phase 1 ISAKMP SA (management between sites, agree how to do crypto) - policy set - Just one bidirectional AS
  - Phase 2 IPsec SA - transfer set (how to secure end user data) - 2 unidirectional SAs: outbound and inbound