Understanding Security Threats

Malicious Software

- **CIA** Triad
  - **Confidentiality** - keeping things hidden
  - **Integrity** - keeping our data accurate & untampered with
  - **Availability** - the information we have is readily accessible to those people that should have it
- Essential security terms
  - **Risk** - the possibility of suffering a loss in the event of an attack on the system
  - **Vulnerability** - a flaw in the system that could be exploited to compromise the system
  - **0-day vulnerability (Zero Day)** - a vulnerability that is not known to the software developer or vendor, but it is known to an attacker
  - **Exploit** - software that is used to take advantage of a security bug or vulnerability
  - **Threat** - the possibility of danger that could exploit a vulnerability
  - **Hacker** - someone who attempts to break into or exploit a system
  - **Attack** - an actual attempt at causing harm to a system
- **Malware** - a type of malicious software that can be used to obtain your sensitive information, or delete or modify files
  - **Virus** - much like a flu virus, is designed to spread from host to host and has the ability to replicate itself - requires an active host program or an already-infected and active operating system
  - **Worm** - stand-alone malicious programs that can self-replicate and propagate via computer networks, without human help - it does not need to attach itself to a software program in order to cause damage
  - **Adware** - software that displays advertisements and collects data
  - **Trojan** - malware that disguises itself as one thing but does something else
  - **Spyware** - a type of malware that's meant to spy on you
  - **Keylogger** - common type of spyware that's used to record every keystroke you make
  - **Ransomware** - type of attack that holds your data or system hostage until you pay some sort of ransom
  - **Botnets** - designed to utilize the power of the internet-connected machines to perform some distributed function
  - **Backdoor** - a way to get into a system if the other methods to get in the system aren't allowed
  - **Rootkit** - a collection of software or tools that an Admin would use, allows admin level modification to an OS
  - **Logic Bomb** - a type of malware that's intentionally installed

Attacks

- Network attacks
  - **DNS Cache Poisoning attack** - Also known as DNS spoofing, DNS cache poisoning is an attack designed to locate and then exploit vulnerabilities that exist in a DNS, or domain name system, in order to draw organic traffic away from a legitimate server and over to a fake one.
  - **Man-in-the-middle attack (MiTM)** - A man-in-the-middle attack is like eavesdropping. When data is sent between a computer and a server, a cybercriminal can get in between and spy.
    - **Session/Cookie Hijacking**
    - **Rogue AP** - an access point that is installed on the network without the network administrator's knowledge

- **Evil Twin** - An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. The evil twin is the wireless LAN equivalent of the phishing scam.

- Denial-of-Service
    - **DoS attack** - an attack that tries to prevent access to service for legitimate users by overwhelming the network or server
        - **Ping of Death (POD)** - A Ping of Death attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash. The original Ping of Death attack is less common today. A related attack known as an ICMP flood attack is more prevalent.
        - **Ping Flood** - Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.
        - **SYN Flood (Half Open Attack)** - Attacker sends SYN packets, server sends SYN-ACK, attacked does not send ACK, keeps spamming SYN.
    - **DDoS** - a DoS attack using multiple systems

Other Attacks

- Client -side attacks
    - **Injection attacks** (mitigated by **input validation** & **data sanitization**)
        - **Cross-site scripting (XSS) attacks** - a type of injection attack where the attacker can insert malicious code and target the user of the service
            - Common for session hijacking
        - **SQL Injection (SQLi)** - SQL injection is a code injection technique, used to attack data-driven applications, in which diabolical SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
    - **Password attacks** - utilize software like password-crackers that try and guess your password
        - **Brute force attack** - an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly
        - **Dictionary attack** - a method of hacking into a password-protected computer or server by systematically entering every word in a dictionary/wordlist as a password
    - Deceptive attacks - **social engineering**: an attack method that relies heavily on interactions with humans instead of computers
        - **Phishing** attack - malicious email
        - **Spear Phishing** - phishing targeted towards a specific individual, organization or business
        - **Spoofing** - a source masquerading around as something else
        - **Baiting** - physical malicious hardware (leaving around USB's)
        - **Tailgating** - gaining access into a restricted area or building by following a real employee in

Cryptology

Intro

- **Encryption** - act of taking a message, called **plaintext**, and applying an operation to it, called a **cipher**, so that you receive a garbled, unreadable message as the output, called **ciphertext**. Decryption is the opposite process

- Cipher made up of two components
    - **Encryption algorithm** - the underlying logic of process that's used to convert the plaintext into ciphertext
    - **Key** - insert something unique into the cipher
- Kerckhoffs principle - **Cryptosystem**
    - A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure - even if everything about the system is known, except the key | aka Shanin's Maxim
    - The system should remain secure even if your adversary knows exactly what kind of encryption systems you're employing, as long as your **keys remain secure**
- **Frequency analysis** - the practice of studying the frequency with which letters appear in a ciphertext
- **Steganography** - the practice of hiding information from observers, but not encoding it

Symmetric Encryption

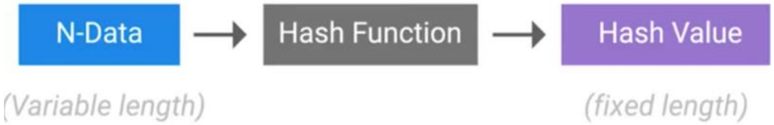
- Same key is used to encrypt & decrypt
- **Substitution cipher**- encryption mechanism that replaces parts of your plaintext with ciphertext, i.e. caesar cipher, ROT13 cipher
- **Stream cipher** - takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time
- **Block ciphers** - the cipher takes data in, place it into a bucket or block of data that's a fixed size, then encodes that entire block as one unit
- Symmetric Encryption Algorithms
    - **DES** - symmetric block cipher, was a **FIPS** when first invented by IBM: (federal information processing standard) | 56-bit key size (64-bit, 8 used for parity)
    - **AES** (2001) - symmetric block cipher, 128-bit size. Because of the large key size, brute-force attacks on AES are only **theoretical** right now, because the computing power required (or time required using modern tech) exceeds anything feasible today
    - An important thing to keep in mind when considering various encryption algorithms is **speed** and **ease of implementation**
    - **RC4 (Rivest Cipher 4)** - a symmetric stream cipher that gained widespread adoption because of its simplicity and speed , replaced by GCM
- Symmetric is good for fast and low power communication, cons are sharing the key

Public Key or Asymmetric Encryption

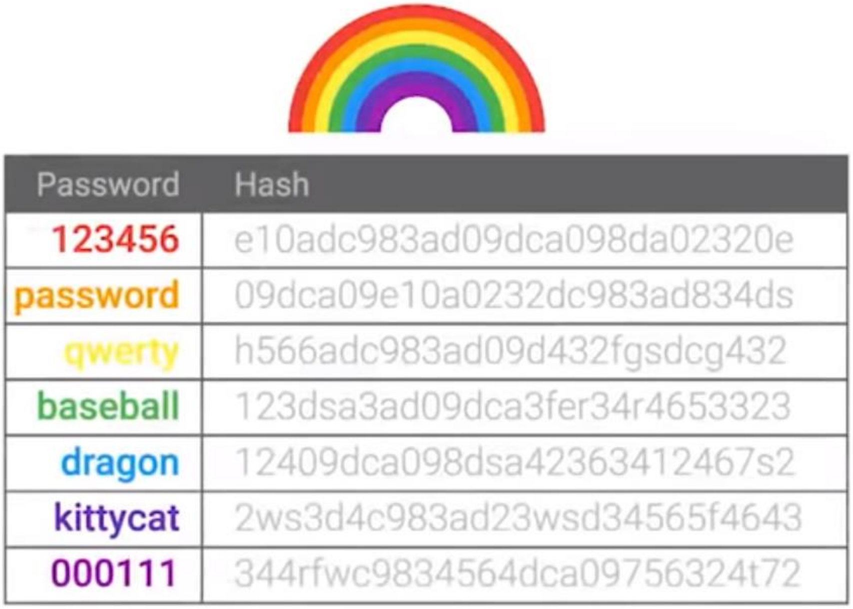
- Different keys are used to encrypt & decrypt
- Public key signatures (**digital signatures**)
- Asymmetric encryption used to ensure confidentiality, authenticity, non-repudiation
- **MAC (message authentication code)** - a bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party
    - **HMAC** - keyed-hash message authentication code
    - **CMACs** cipher-based message authentication codes
- Asymmetric encryption algorithms
    - **RSA**
    - **DSA** - digital signature algorithm, part of FIPS
    - **DH - Diffie-Hellman**
    - **ECC** (**elliptic curve cryptography**) - a public-key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys
    - Both DH & DSA have elliptic curve variants, referred to as **ECDH** and **ECDSA**, respectively

Hashing

- **Hashing** (or a hash function) - a type of function or operation that takes in an arbitrary data input and maps it to an output of fixed size, called a hash or digest



  - You feed in any amount of data into a hash function and the resulting output will always be the same size, but the output should be **unique to the input**, such that two different inputs should never yield the same output
  - Hashing can also be used to identify duplicate data sets in databases or archives to speed up searching of tables or to remove duplicate data to save space
  - Cryptographic hashing is distinctly different from encryption because cryptographic hash functions should be one directional
  - The ideal cryptographic hash function should be **deterministic**, meaning that the same input value should always return the same hash value
  - The function should not allow for **hash collisions** - two different inputs mapping to the same output
- Hashing algorithms
  - **MD5 -** deprecated 2010, recommended SHA after
  - **SHA1** - part of the Secure Hash Algorithm suite of functions, designed by the NSA, published in 1995
    - Used in TLS/SSL, PGP SSH, IPsec
    - Recommended SHA2 or SHA3 after 2010
  - **MIC** - message integrity check
- **Rainbow tables** - precomputed table of all possible password values and their corresponding hashes, trade computational power for disk space , mitigated by salting



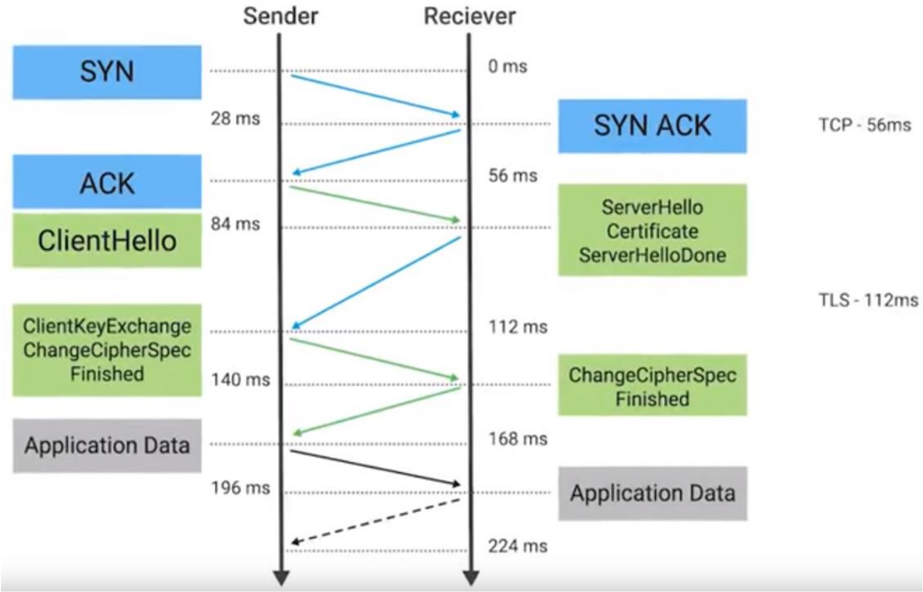
Password	Hash
123456	e10adc983ad09dca098da02320e
password	09dca09e10a0232dc983ad834ds
qwerty	h566adc983ad09d432fgsdcg432
baseball	123dsa3ad09dca3fer34r4653323
dragon	12409dca098dsa42363412467s2
kittycat	2ws3d4c983ad23wsd34565f4643
000111	344rfwc9834564dca09756324t72

- **Password Salt / Salting** - additional randomized data that's added into the hashing function to generate a hash that's unique to the password and salt combination

Cryptography Applications

- **Public Key Infrastructure (PKI)**

    - PKI - a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption
    - A certificate contains info on public key, registered owner, and digital signature
    - **CA**: certificate authority - an entity that issues digital certificates
    - **RA**: registration authority - verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it
    - A central repository is needed to securely store and index keys, and a certificate management system of some sort makes managing access to stored certificates and issuance of certificates easier
    - **Root certificate authority** - starts the chain of trust
    - A certificate that has no authority as a CA is referred to an **end-entity** or **leaf certificate**
    - The **X.509** standard is what defines the format of digital certificates
        - Version
        - Serial Number - a unique identifier for the certificate assigned by the CA which allows the CA to manage and identify individual certificates
        - Certificate signature algorithm - this field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate
        - Issuer name - this field contains information about the authority that signed the certificate
        - Validity - this contains two subfields - “Not Before” and “Not After” - which define the dates when the certificate is valid for
        - Subject - this field contains identifying information about the entity the certificate was issued to
        - Subject public key info - these two subfields define the algorithm of public key, along with the public key itself
        - Certificate signature algorithm - same as the Subject Public Key Info field; these two fields must match
        - Certificate signature value - the digital signature data itself
    - **Web of trust** - a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner
- Cryptography in action
    - **HTTPS** - is the secure version of HTTP, the HyperText Transfer Protocol
        - SSL 3.0 deprecated in 2015, **TLS** 1.3 is standard now
    - TLS Handshake



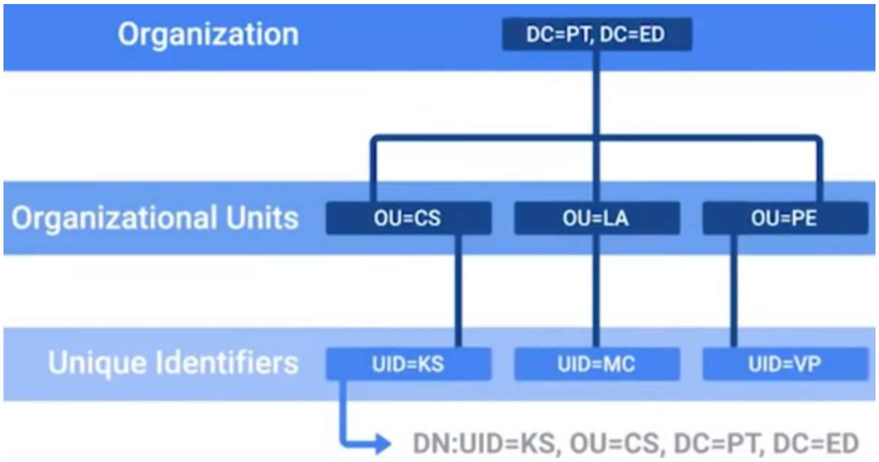
- **SSH** (secure shell) - a secure network protocol that uses encryption to allow access to a network service over unsecured networks , port 22
- **PGP** (pretty good privacy) - an encryption application that allows authentication of data, along with privacy from third parties, relying upon asymmetric encryption to achieve this
- Securing network traffic
  - **VPN** - a mechanism that allows you to remotely connect a host or network to an internal, private network, passing the data over a public channel, like the internet
    - **IPsec**, can use transport or tunnel mode
    - **L2TP**
    - SSL/TLS is used in VPNs as well - **OpenVPN** - can operate over either TCP or UDP, typically over port 1194
- Cryptographic hardware
  - **TPM** (trusted platform module) an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.
  - **FDE** (full disk encryption)
    - **PGP**
    - **Bitlocker** (Microsoft)
    - **Filevault 2** (Apple)
    - **dm-crypt** (open source)

AAA Security

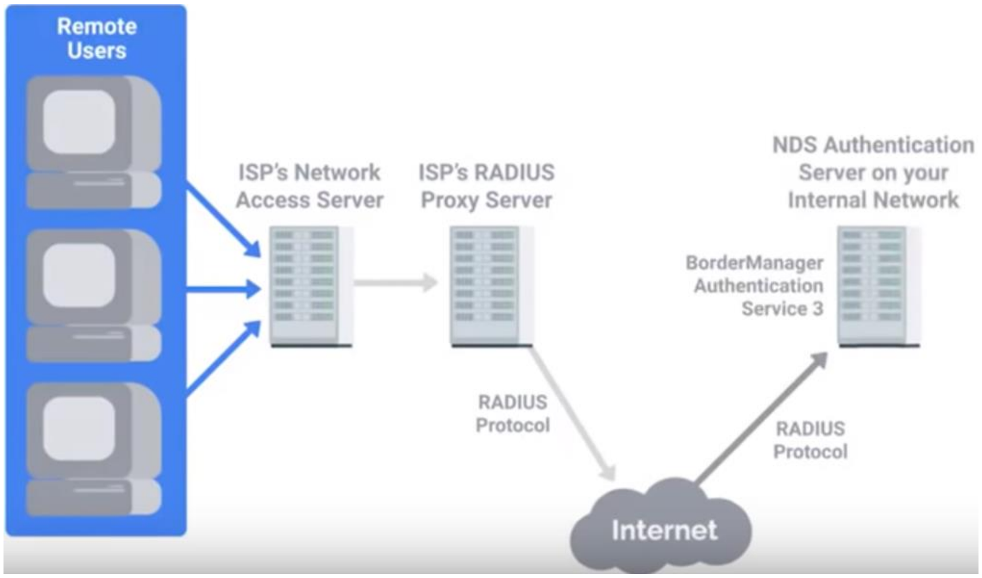
Authentication

- **Identification** - the idea of describing an entity uniquely
- “**authn**”
- **Authentication** ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
- Incorporating **good password policies** into an organization is key to ensuring that employees are securing their accounts with **strong passwords**
- **Multi Factor Authentication** - a system where users are authenticated by presenting multiple pieces of information or objects
  - **Something you know** = password/pin

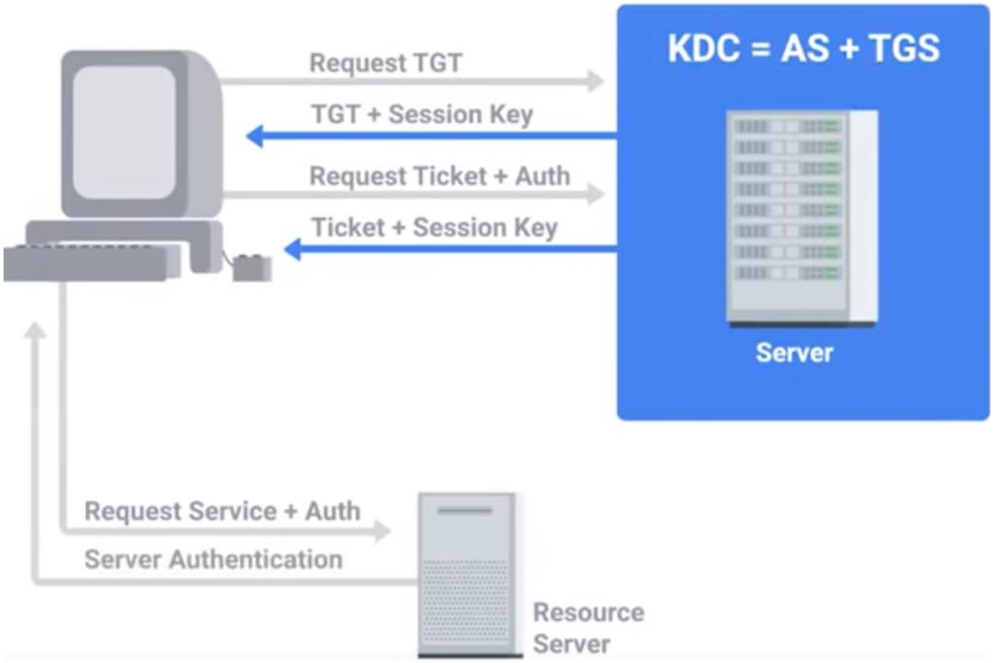
        - Physical Tokens
            - OTP - one time password
            - TOTP - time based OTP
    - **Something you have** = ATM/Bank card
    - **Something you are** = Biometric ID
        - **Biometric authentication**- the process of using nique physiological characteristics of an individual to identify them
- Client Certificates, Certificate-based authentication
    - I order to issue client certificates, an organization must setup and maintain CA infrastructure to issue and sign certificates
    - **CRL** (certificate revocation list) - a signed list published by the CA which defines certificates that have been explicitly revoked
- **LDAP** - an open, industry-standard protocol for accessing and maintaining directory services



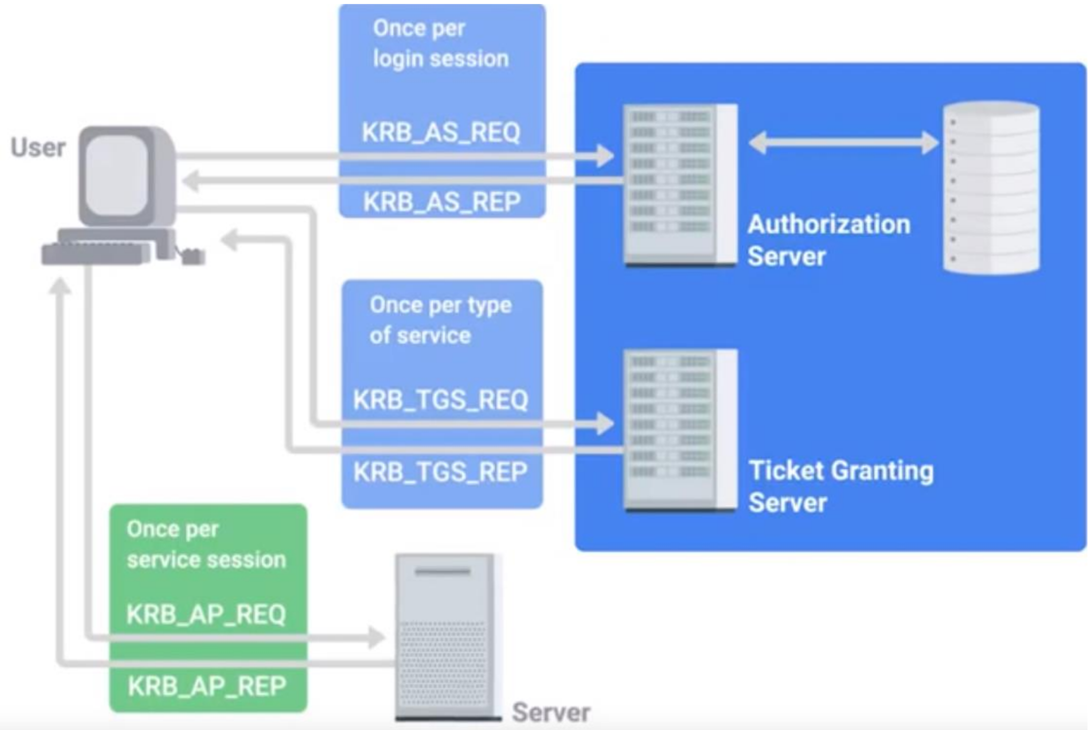
- **RADIUS** (remote authentication dial-in user service) - a protocol that provides AAA services for users on a network, network access
    - **EAP** - extensible authentication protocol - an authentication framework frequently used in wireless networks and point-to-point connections


Remote Users
ISP's Network Access Server
ISP's RADIUS Proxy Server
NDS Authentication Server on your Internal Network
BorderManager Authentication Service 3
RADIUS Protocol
RADIUS Protocol
Internet

- **Kerberos** - a network authentication protocol that uses “tickets” to allow entities to prove their identity over potentially insecure channels to provide mutual authentication
    - Utilizes symmetric encryption



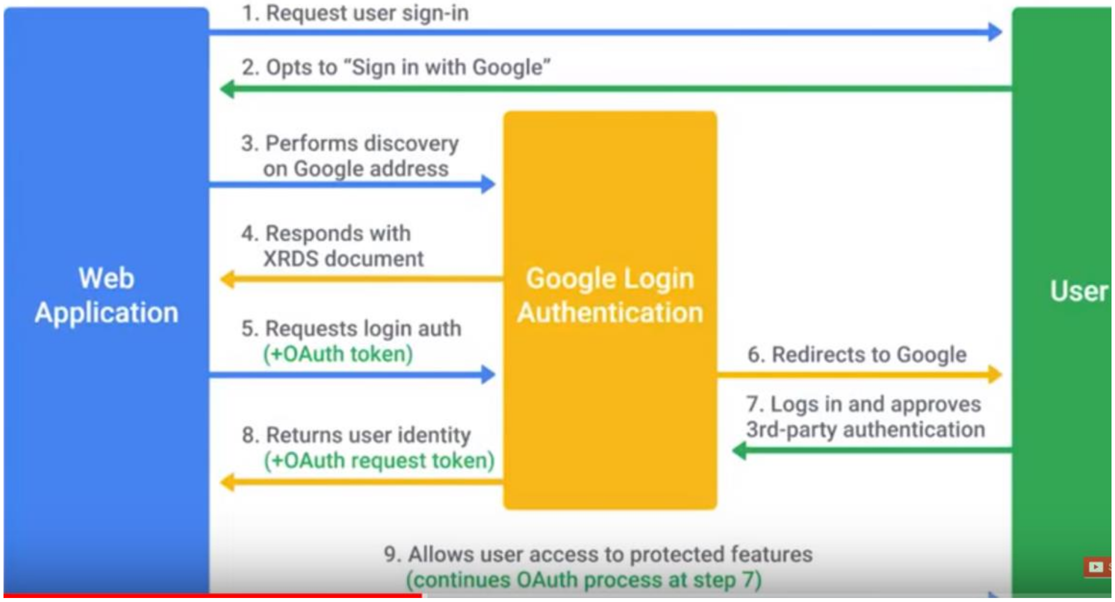
- Single point of failure - the kerberos server
- **TACACS+** = terminal access controller access-control system plus, Cisco developed AAA protocol; primarily used for device administration and AAA
  - Mainly used for network infrastructure devices
- **SSO** (single sign-on) - an authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications
  - Kerberos is a good example:



  - Usually paired with MFA
  - **OpenID**

Authorization

- “**authz**”
- **Authorization** - pertains to describing what the user account has access to, or doesn’t have access to
- Access Control
    - **OAuth** - an open standard that allows users to grant third-party websites and applications access to their information without sharing account credentials
    - OAuth permissions can be used in phishing-style attacks to gain access to accounts, **without requiring credentials** to be compromised



1. Request user sign-in
2. Opts to “Sign in with Google”
3. Performs discovery on Google address
4. Responds with XRDS document
5. Requests login auth (+OAuth token)
6. Redirects to Google
7. Logs in and approves 3rd-party authentication
8. Returns user identity (+OAuth request token)
9. Allows user access to protected features (continues OAuth process at step 7)

Accounting

- Tracking usage and access
    - **Accounting** - keeping records of what resources and services your users accessed, or what they did when they were using your systems
    - **TACACS+** is a device access AAA system that manages who has access to your network devices and what they do on them

Securing Your Networks

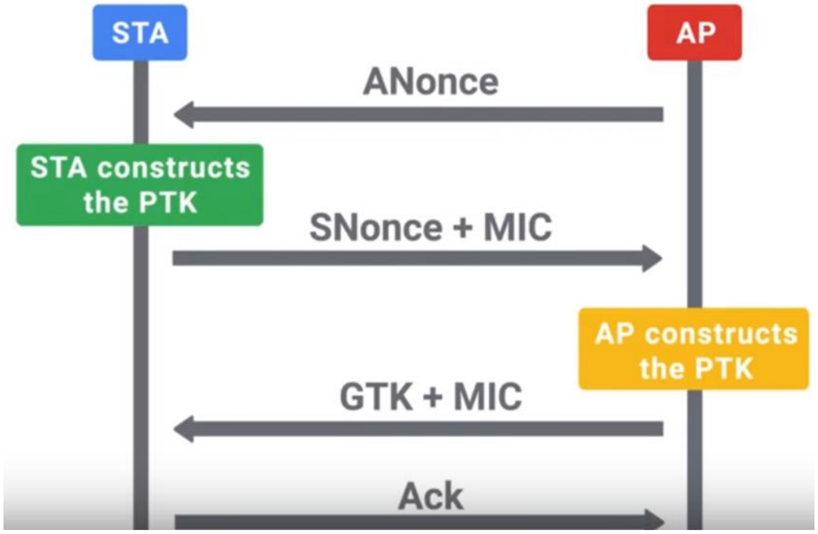
Secure network architecture

- Network hardening best practices
    - **Network hardening** - the process of securing a network by reducing its potential vulnerabilities through configuration changes and taking specific steps
    - **Implicit deny** - a network security concept where anything not explicitly permitted or allowed should be denied
    - **Analyzing logs** - the practice of collecting logs from different network and sometimes client devices on your network, then performing an automated analysis on them
    - **Logs analysis systems** are configured using user-defined rules to match interesting or atypical log entries
    - **Normalizing log data** is an important step, since logs from different devices and systems may not be formatted in a common way
    - **Correlation analysis** - the process of taking log data from different systems and matching events across the systems
    - **Flood guards** - provide protection against DoS attacks

- Network hardware hardening
    - **DHCP Snooping** - implement to protect against DHCP spoofing attacks
    - **Dynamic ARP inspection (DAI)** - Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors.
    - **IP Source Guard (IPSG)**
    - **802.1X,** IEEE standard for encapsulating EAP (extensible authentication protocol)
        - AKA EAPOL (EAP over lan)
        - **EAP-TLS** - an authentication type supported by EAP that uses TLS to provide mutual authentication of both the client and the authenticating server
- Network software hardening

Wireless security

- **WEP**
    - No one should be using WEP anymore
    - Utilized RC4 stream cipher
- **WPA/WPA2**
    - Replaces WEP
    - WPA was designed as a short-term replacement that would be compatible with older WEP-enabled hardware with a simple firmware update
    - **TKIP** - temporal key integrity protocol
    - Under WPA, the **pre-shared key (PSK)** is the Wifi password you share with people when they come over and want to use your wireless network
    - **WPA2** introduced **CCMP** - counter mode CBC-MAC protocol
        - Utilizes AES cipher, no more RC4
        - **4 way handshake**

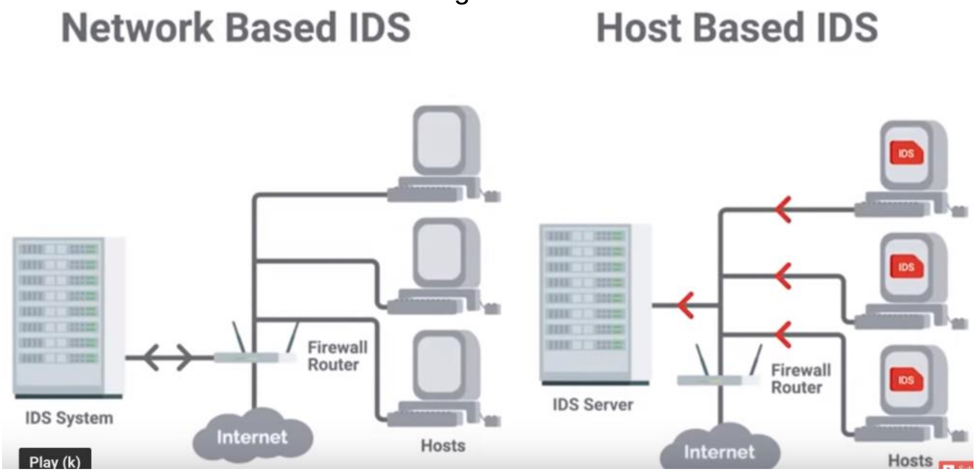


        - **802.1X - WPA2 Enterprise**
    - **WPS**
- Wireless Hardening
    - Strongest is WPA2-Enterprise with EAP-TLS, but requires a ton of complexity and overhead - needs Radius server and authentication server at a minimum, and needs a proper PKI
    - If 802.1X is too complicated for a company, the next best alternative would be WPA2 with AES/CCMP mode

-
  - If your company values security over convenience, you should make sure that WPS isn't enabled on your APs

Network monitoring

- Sniffing the network
  - **Packet Sniffing (packet capture)** - the process of intercepting network packets in their entirety for analysis
  - **Promiscuous mode** - a type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode
  - **Port mirroring** - allows the switch to take all packets from a specified port, port range, or entire VLAN and mirror the packets to a specific switch port
  - **Monitor mode** - allows us to scan across channels to see all wireless traffic being sent by APs and clients
- Wireshark and Tcpdump
  - **Tcpdump** - a super popular, lightweight, command-line based utility that you can use to capture and analyze packets
  - **Wireshark** - more powerful, GUI
- Intrusion detection/prevention systems
  - **IDS/IPS** - IDS or IPS systems operate by monitoring network traffic and analyzing it; IDS is only detection and alerting, IPS can apply firewall rules for blocking
  - **Network IDS (NIDS)** - the detection system would be deployed somewhere on a network where it can **monitor traffic** for a network segment or subnet

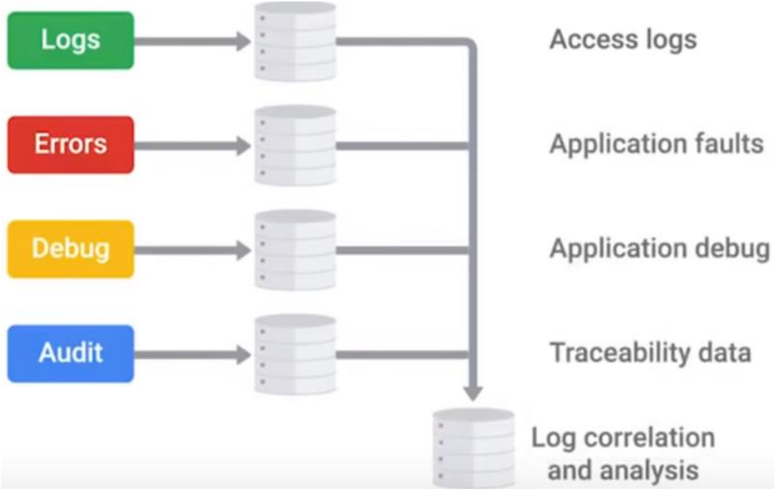


Defense in Depth

System hardening

- Intro to Defense in Depth
  - **Defense in Depth** - the concept of having multiple, overlapping systems of defense to protect IT systems
- Disabling unnecessary components
  - **Attack vector** - the method or mechanism by which an attacker or malware gains access to a network or system
  - **Attack surface** - the sum of all the different attack vectors in a given system
  - The less complex something is, the less likely there will be undetected flaws
  - Another way to keep things simple is to reduce your software deployments
  - Telnet access for a managed switch has no business being enabled in a real-world environment

  -
- **Host-based firewall** - protect individual hosts from being compromised when they're used in untrusted, potentially malicious environments
  - A host-based firewall plays a big part in reducing what's accessible to an outside attacker
  - If the users of the system have administrator rights, then they have the ability to **change firewall rules and configurations**
- Logging and auditing
  - **SIEM** - In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM).



  - Once logs are centralized and standardized, you can write automated alerting based on **rules**
- Antimalware protection
  - **Antivirus** - signature based : AV software will monitor and analyze things, like new files being created or being modified on the system, in order to watch for any behavior that matches a known malware signature
    - Recommended because it protects against the most common attacks on the internet
- Disk Encryption
  - **Full-disk encryption (FDE)** - works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversation
  - When you implement a full disk encryption solution at scale, it's super important to think about how to handle cases where passwords are forgotten
  - Many enterprise solutions have a Key Escrow functionality
    - **Key Escrow** - allows the encryption key to be securely stored for later retrieval by an authorized party
  - **Home directory** or **file-based encryption** only guarantees confidentiality and integrity of files protected by encryption

Application hardening

- Software patch management
  - It's critical that you make sure that you install software updates and security patches in a timely way, in order to **defend your company's systems and networks**
  - The best protection is to have a **good system and policy** in place for your company
  - Tools for constant patching: SCCM, Puppet

    - Critical infrastructure devices should be approached **carefully** when you apply updates. There's always the risk that a software update will introduce a new bug that might affect the **functionality** of the device
- Application policies
    - A common recommendation, or even a requirement, is to only support or require the **latest version** of a piece of software
    - It's generally a good idea to **disallow risky classes** of software by policy. Things like file sharing software and piracy-related software tend to be closely associated with malware infections.
    - Understanding **what your users need** to do their jobs will help shape your approach to software policies and guidelines
    - Helping your users accomplish tasks by recommending or supporting specific software meks for a more **secure environment**

Creating a Company Culture for Security

Risk in the Workplace

- Security goals (example)
    - If your company handles credit card payments, then you have to follow **PCI DSS - payment card industry data security standard**
        1. Build & maintain a secure network and systems
        2. Protect cardholder data
        3. Maintain a vulnerability management program
        4. Implement strong access control measures
        5. Regularly monitor and test networks
        6. Maintain an information security policy
- Measuring & Assessing risk
    - Security is all about determining **risks** or exposure; understanding the likelihood of **attacks**; and designing **defenses** around these risks to **minimize** the impact of an attack
    - High-value data usually includes account information, like usernames and passwords. Typically, **any kind of user data is considered high value**, especially if payment processing is involved
    - **Vulnerability scanner** - a computer program designed to assess computers, computer systems, networks or applications for weaknesses
    - **Penetration testing** - the practice of attempting to break into a system or network to verify the systems in place
- Privacy policy
    - **Privacy policies** oversee the access and use of sensitive data
    - It's good practice to apply principle of **least privilege** here, by not allowing access to this type of data by default
    - Any access that doesn't have a corresponding request should be flagged as a **high-priority potential breach** that needs to be investigated as soon as possible
    - **Data-handling policies** should cover the details of how different data is classified
    - Once different data classes are defined, you should create **guidelines** around how to handle these different types of data

Users

- User habits

    - You can build the world’s best security systems, but they won’t protect you if the users are going to be practicing **unsafe security**
    - You should **never upload confidential information** onto a third-party service that hasn’t been evaluated by your company
    - It’s important to **make sure employees use new and unique passwords**, and don’t reuse them from other services
    - A much greater risk in the workplace that users should be educated on is **credential theft** from phishing emails.
    - If someone entered their password into a phishing site, or even suspects they did, it’s important to **change their password** as soon as possible
- Third-party security
    - Utilize vendor security assessment questionnaire
        - Google’s for free: https://vsaq-demo.withgoogle.com/
    - If you can, ask for a third-party security assessment report

Incident Handling

- Incident reporting & analysis
    - The very first step of handling an incident is to **detect it** in the first place
    - The next step is to **analyze it** and **determine the effects** and scope of damage
    - Once the scope of the incident is determined, the next step is **containment**
    - If an account was compromised, change the password **immediately**. If the owner is unable to **change the password** right away, then **lock the account**.
    - **Severity** includes factors like what and how many systems were compromised, and how the branch affects business functions
    - The **impact** of an incident is also an important issue to consider
    - **Data exfiltration** - the unauthorized transfer of data from a computer
    - **Recoverability** - how complicated and time - consuming the recovery effort will be
- Incident response and recovery
    - Update firewall rules and ACLs if an exposure was discovered in the course of the investigation
    - Create new definitions and rules for intrusion detection systems that can watch for the signs of the same attack again