

CompTIA Security+:

SY0-601 Certification

CompTIA Security+

- **More choose Security+ -** chosen by more corporations and defense organizations than any other certification on the market to validate baseline security skills and for fulfilling the DoD 8570 compliance.
- **Security+ proves hands-on skills –** the only baseline cybersecurity certification emphasizing hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
- **More job roles turn to Security+ to supplement skills –** baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
- **Security+ is aligned to the latest trends and techniques –** covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

CompTIA Security+

CompTIA Security+ is the first security certification a candidate should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

- **Assess** the security posture of an enterprise environment and recommend and implement appropriate security solutions
- **Monitor and secure** hybrid environments, including cloud, mobile, and IoT
- **Operate** with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- **Identify, analyze, and respond** to security events and incidents

What Skills Will You Learn?

Attacks, Threats and Vulnerabilities

- Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

Architecture and Design

- Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

Implementation

- Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.

What Skills Will You Learn?

Operations and Incident Response

- Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.

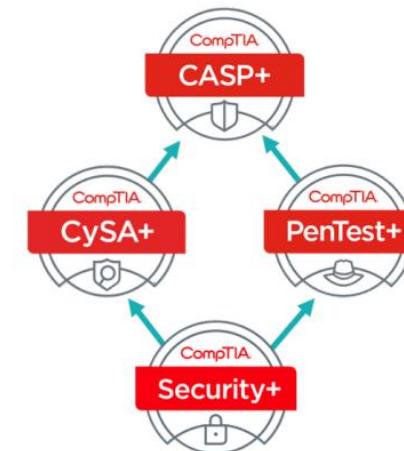
Governance, Risk and Compliance

- Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

CompTIA Security+

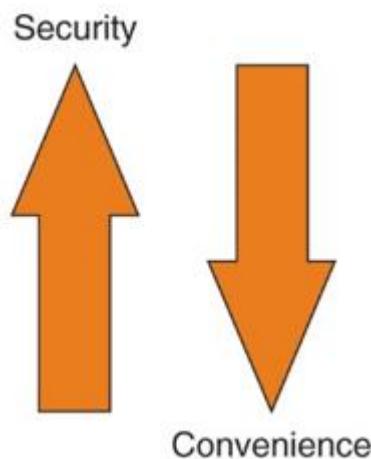
- Domains (SYO-601)
 - Attacks, Threats, and Vulnerabilities (24%)
 - Architecture and Design (21%)
 - Implementation (25%)
 - Operations and Incident Response (16%)
 - Governance, Risk, and Compliance (14%)

- **Exam Tricks**
 - 1. Use a Cheat Sheet
 - 2. Skip the Simulations
 - 3. Take a Guess
 - 4. Pick the Best Time
 - 5. Be Confident

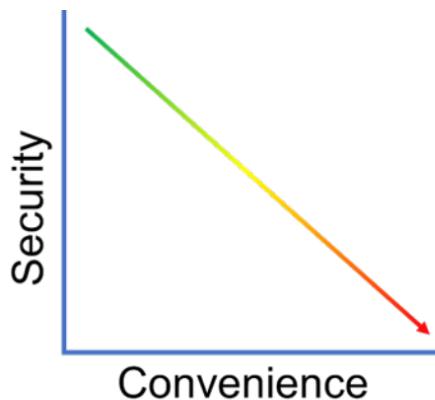


UNDERSTANDING SECURITY

- Security is:
 - To be free from danger is the goal
 - The process that achieves that freedom
- As security is increased, convenience is often decreased
 - The more secure something is, the less convenient it may become to use



Overview of Security



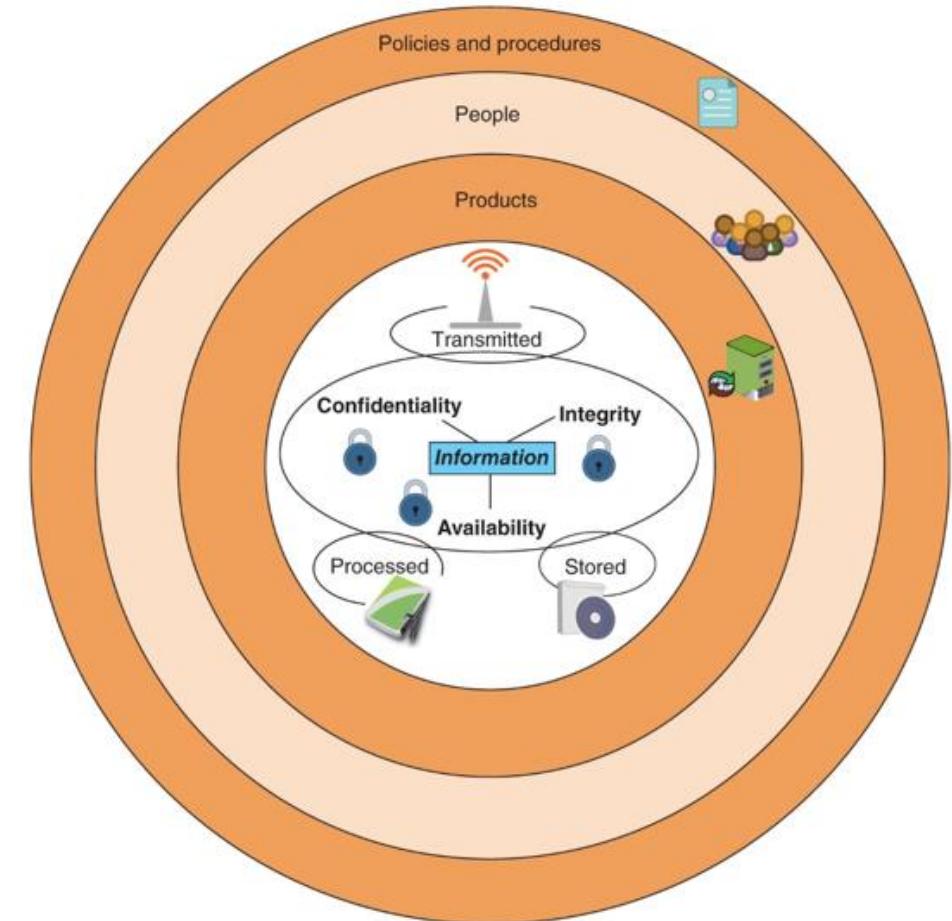
- **Information Security**
 - Act of protecting data and information from unauthorized access, unlawful modification and disruption, disclosure, corruption, and destruction
- **Information Systems Security**
 - Act of protecting the systems that hold and process our critical data
- **Basics and Fundamentals**



- **Confidentiality**
 - Information has not been disclosed to unauthorized people
- **Integrity**
 - Information has not been modified or altered without proper authorization
- **Availability**
 - Information is able to be stored, accessed, or protected at all times

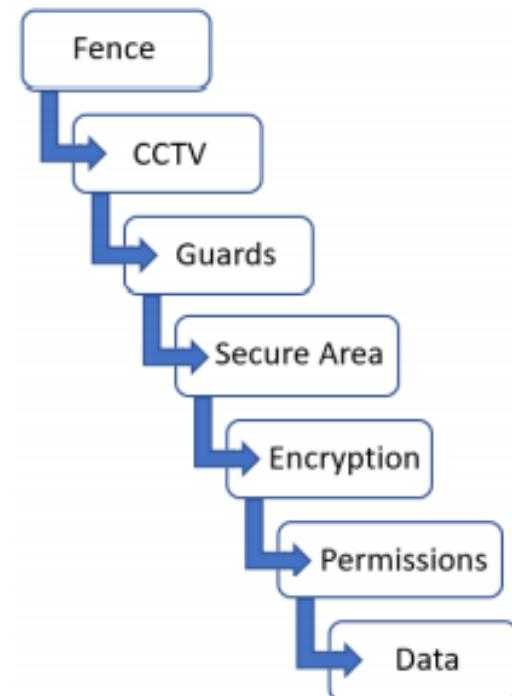
DEFINING INFORMATION SECURITY

Layer	Description
Products	Form the security around the data. May be as basic as door locks or as complicated as network security equipment.
People	Those who implement and properly use security products to protect data.
Policies and procedures	Plans and policies established by an enterprise to ensure that people correctly use the products.



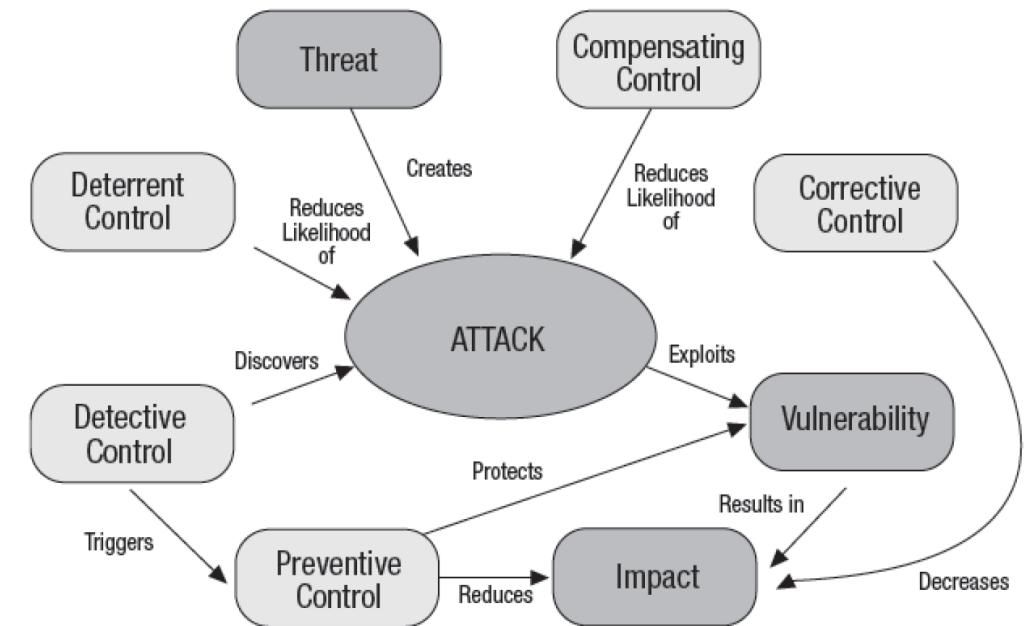
Defense in Depth

- Defense in Depth Model Defense in Depth is the concept of protecting a company's data with a series of protective layers so that if one layer fails, another layer will already be in place to thwart an attack. We start with our data, then we encrypt it to protect it:
 - The data is stored on a server.
 - The data has file permissions.
 - The data is encrypted.
 - The data is in a secure area of the building.
 - There is a security guard at the building entrance checking identification.
 - There is CCTV around the perimeter.
 - There is a high fence around the perimeter



CONTROL TYPES AND CATEGORIES

- **Preventative:** Reduces or eliminates specific instances of vulnerability by making the behavior impossible.
- **Corrective:** Reduce impact by offsetting the impact of consequences after the fact.
- **Detective:** Warn of violations or attempted violations.
- **Compensating:** Reduce the risk of a control weakness through layering.
- **Deterrent:** Reduce threat through warnings and notices that influence behavior.



CONTROLS IMPLEMENTATION METHODS

- Managerial (administrative)
 - Apply to processes and behaviors
- Technical (logical)
 - Apply to information systems, software and networks
- Physical
 - Apply to facilities and areas within them

Controls of any effect category can be implemented using any of the three implementation methods.

- Automated controls are generally preferred to manual controls.
 - Analysis is needed to confirm if this is the case.
- High volume of data may require automation.
- SIEM software can help to create useful reports out of automation.



Comparing Control Types

- **Managerial Controls** are written by managers to create organizational policies and procedures to reduce risk within companies. They incorporate regulatory frameworks so that the companies are legally compliant.
- The following are examples of management controls:
 - Annual Risk Assessment: A company will have a risk register where the financial director will look at all of the risks associated with money and the IT manager will look at all of the risks posed by the IT infrastructure. As technology changes and hackers get more sophisticated, the risks can become greater. Each department will identify their risks and the risk treatments, and place them in the risk register. These should be reviewed annually.
 - Penetration Testing/Vulnerability Scanning: A vulnerability scan is not intrusive as it merely checks for vulnerabilities, whereas a penetration test is more intrusive and can exploit vulnerabilities.

Comparing Control Types

- **Operational controls** are executed by company personnel during their day-to-day operations. Examples of these are the following:
 - **Annual Security Awareness Training:** This is an annual event where you are reminded about what you should be doing on a daily basis to keep the company safe:
 - Example 1 – When you are finished for the day, you clear your desk and lock all documents away; another employee would remind you that your identity badge should be worn at all times and you should challenge anyone not wearing a badge.
 - Example 2 – Companies need their employees to complete annual cybersecurity training as the risk is getting greater each day.
 - **Change Management:** This is a process that a company adopts so that changes made don't cause any security risks to the company. A change to one department could impact another department. The Change Advisory Board (CAB) assists with the prioritization of changes; they also look at the financial benefits of the change and they may accept or reject the changes proposed for the benefit of the company. IT evolves rapidly and our processes will need to change to cope with the potential security risks associated with newer technology.
 - **Business Continuity Plan:** This is contingency planning to keep the business up and running when a disaster occurs by identifying any single point of failure that would prevent the company from remaining operational.

Comparing Control Types

- **Technical Controls** are those implemented by the IT team to reduce the risk to the business.
- These could include the following:
 - **Firewall Rules:** Firewalls prevent unauthorized access to the network by IP address, application, or protocol. These are covered in depth later in this book.
 - **Antivirus/Antimalware:** This is the most common threat to a business, and we must ensure that all servers and desktops are protected and up to date.
 - **Screen Savers:** These log computers off when they are idle, preventing access.
 - **Screen Filters:** These prevent people that are walking past from reading the data on your screen.
 - **Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS):** An IDS monitors the network for any changes and an IPS stops the attacks. If you do not have an IDS, the IPS has the ability to fulfill the role of the IDS.

Comparing Control Types

- **Deterrent Controls** could be CCTV and motion sensors. When someone is walking past a building and the motion sensors detect them, it turns the lights on to deter them. A building with a sign saying that it is being filmed with CCTV prevents someone from breaking into your premises, even though there may not be film inside the camera—but they don't know that!
- **Detective Controls** are used to investigate an incident that has happened and needs to be investigated; these could include the following:
 - CCTV records events as they happen and from that, you can see who has entered a particular room or has climbed through a window at the rear of a building. CCTV can capture motion and provide non-repudiation.
 - Log Files are text files that record events and the times that they occurred; they can log trends and patterns over a period of time. For example, servers, desktops, and firewalls all have event logs that detail actions that happen. Once you know the time and date of an event, you can gather information from various log files. These can be stored in Write-Once Read-Many (WORM) drives so that they can be read but not tampered with.

Comparing Control Types

- Corrective Controls are the actions you take to recover from an incident. You may lose a hard drive that contained data; in that case, you would replace the data from a backup you had previously taken.
- Fire Suppression Systems are another form of corrective control. There may have been a fire in your data center that destroyed many servers, therefore when you purchase a replacement, you may install an oxygen suppressant system that will starve a fire of the oxygen needed. This method uses argon/nitrogen and carbon dioxide to displace the oxygen in the server room.

Comparing Control Types

- **Compensating Controls** can also be called Alternative or Secondary Controls and can be used instead of a primary control that has failed or is not available. Once a primary control has failed, we need a secondary control. This is similar to when you go shopping and you have \$100 in cash—once you have spent your cash, you will have to use a credit card as a compensating control.
- Example: When a new employee arrives, they should log in using a smart card and PIN. It may take 3–5 days to get a new smart card, so during the waiting period, they may log in using a username and password.

Comparing Control Types

- **Preventative Controls** are in place to deter any attack; this could be having a security guard with a large dog walking around the perimeter of your building. This would make someone trying to break in think twice about doing so.
- Some of the preventive measures that can be taken are as follows:
 - Disable User Accounts: When someone leaves a company, the first thing that happens is that their account is disabled, as we don't want to lose information that they have access to, and then we change the password so that they cannot access it. We may also disable an account while people are on secondment or maternity leave.
 - Operating System Hardening: This makes a computer more secure, where we ensure that the operating system is fully patched and turn off unused features and services. This will ensure that there will be no vulnerabilities.

Understanding Digital Forensics

- **Collection:** Here, the data is examined, then extracted from the media that it is on, and then converted into a format that can be examined by forensic tools.
- **Examination:** Prior to examination, the data will be hashed, and then an investigation will be carried out with the relevant forensic tool. When the examination has concluded, the data is once again hashed to ensure that the examiner or the tools have not tampered with it. We could use a USB write blocker that allows only read access to storage media.
- **Analysis:** When all of the forensic data has been collected, it is analyzed and then transformed into information that can be used as evidence.
- **Reporting:** A report is compiled that can be used as evidence for conviction.



NIST Four different phases

Understanding Identity and Access Management Concepts

- There are four key elements to Identify and Access Management (IAM), and these are identity, authentication, authorization, and accounting. Let's look at each of these in the order that they should be presented:
- **Identify:** Each person needs some form of identification so that they can prove who they are; this could be anything, ranging from a username to a smart card. It needs to be unique so that the person using that identity is accountable for its use.
- **Authentication:** The second part after proving your identity is to provide authentication for that identity. This can be done in many ways; for example, inserting a password or if you have a smart card, it would be a Personal Identification Number (PIN).
- **Authorization:** Once the individual has been authenticated, they are given an access level based on their job role. This could also be known as their permission level to the system to which they have access.
- **Accounting:** Computer systems maintain a log of when users log in and log out, and accounting is the process of maintaining these log files. This could be the security log in a Windows desktop in Event Viewer or it could be a database on a AAA server that is responsible for authentication, authorization, and accounting. Examples of these are RADIUS and DIAMETER from Microsoft or TACACS+ from CISCO.

Understanding Identity and Access Management Concepts

- An identity provider (IdP) is an entity that can validate that the credentials that are presented are valid. The identity could be a certificate, token, or details such as a username or password. IdP is used by cloud providers who use federation services to validate the identity of a user.
 - An example of this is that they would use SAML to pass credentials to the IdP to validate their identity. Example: A user authenticates using a token from a provider such as OKTA. The cloud provider uses SAML to pass the credentials back to OKTA to verify the user's identity.

Understanding Identity and Access Management Concepts

The following can be used when assessing a person's identity as it needs to be unique to them:

- **Username:** This is the account identity given to the user.
- **Attribute:** This is a unique variable that the user has in their account details, for example, an employee ID.
- **Smart Card:** A credit card token with a certificate embedded on a chip; it is used in conjunction with a pin.
- **Certification:** This is a digital certificate where two keys are generated, a public key and a private key. The private key is used for identity.
- **Token:** This is a digital token that can either be a SAML token used for federation services or a token used by **Open Authentication (OAuth)**.
- **SSH Keys:** These are typically used by an administrator using a secure remote connection to the server. First of all, a key pair, private and public keys, is generated. The public key is stored on the server, with the private key remaining on the administrator's desktop. **Example:** Using a tool such as OpenSSH, the `ssh-keygen -t RSA` command is used to generate a RSA public and private key pair on the administrator's desktop. The next step is to use `ssh-copy-id` to log in to the server and copy the public key across. This is added to the list of authorized keys on the server. While copying, the administrator may be asked to provide their process whereby the key is generated and copied across. An administrator will use the `ssh-root@server` and a user will use `username@server` to test the SSH keys.

Role-Based Access Control

This is a subset of duties within a department. An example would be two people within the finance department who only handle the petty cash. In IT terms, it could be that only two of the IT team administer the email server.

Rule-Based Access Control

In **Rule-Based Access Control (RBAC)**, a rule is applied to all of the people within a department, for example, contractors will only have access between 8 a.m. and 5 p.m., and the help desk people will only be able to access Building 1, where their place of work is. It can be time-based or have some sort of restriction, but it applies to the whole department.

Attribute-Based Access Control

In **Attribute-Based Access Control (ABAC)**, access is restricted based on an attribute in the account. John could be an executive and some data could be restricted to only those with the executive attribute. This is a user attribute from the directory services, such as a department or a location. You may wish to give different levels of control to different departments.

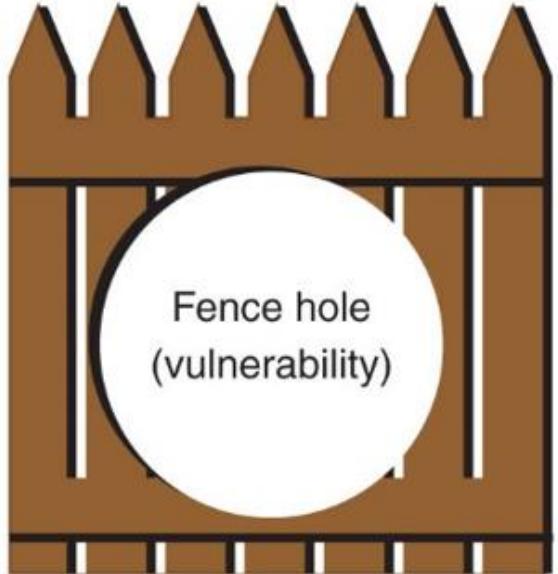
Group-Based Access

To control access to data, people may be put into groups to simplify access. An example would be if there were two people who worked in **Information Technology (IT)** who needed access to older IT data. These people are called Bill and Ben:

INFORMATION SECURITY TERMINOLOGY

- **Asset**
 - Item that has value
- **Threat**
 - Type of action that has the potential to cause harm
- **Threat actor**
 - A person or element with power to carry out a threat
- **Vulnerability**
 - Flaw or weakness that allows a threat agent to bypass security
- **Threat vector**
 - The means by which an attack can occur
- **Risk**
 - A situation that involves exposure to some type of danger
- **Risk response techniques:**
 - **Accept** – risk is acknowledged but no steps are taken to address it
 - **Transfer** – transfer risk to a third party
 - **Avoid** – identifying risk but making the decision to not engage in the activity
 - **Mitigate** – attempt to address risk by making the risk less serious

Attack vector
(go through
fence hole)



Fence hole
(vulnerability)

Theft of scooter
(threat)



Thief (threat actor)

Stolen scooter (risk)

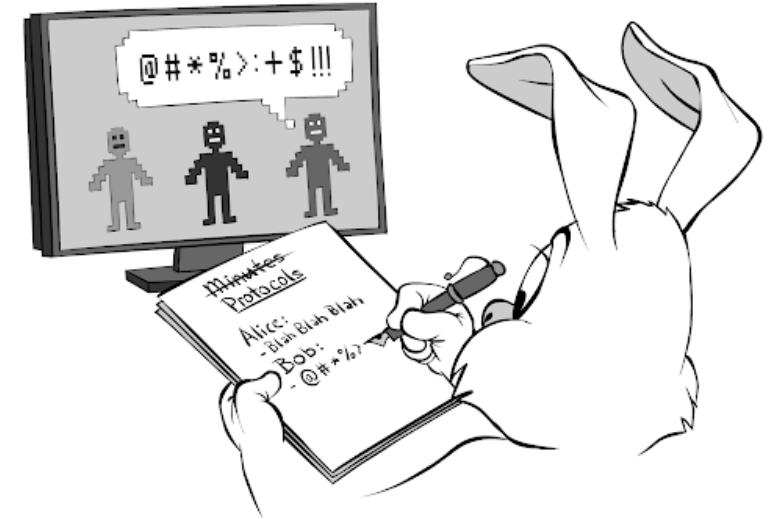


Scooter (asset)

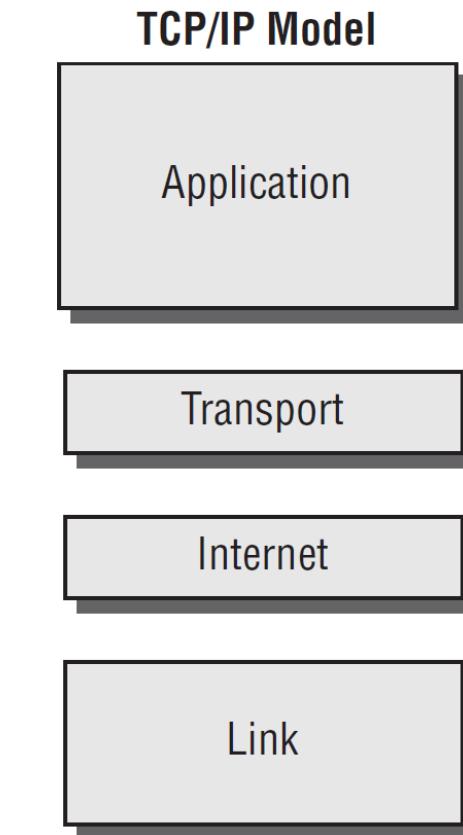
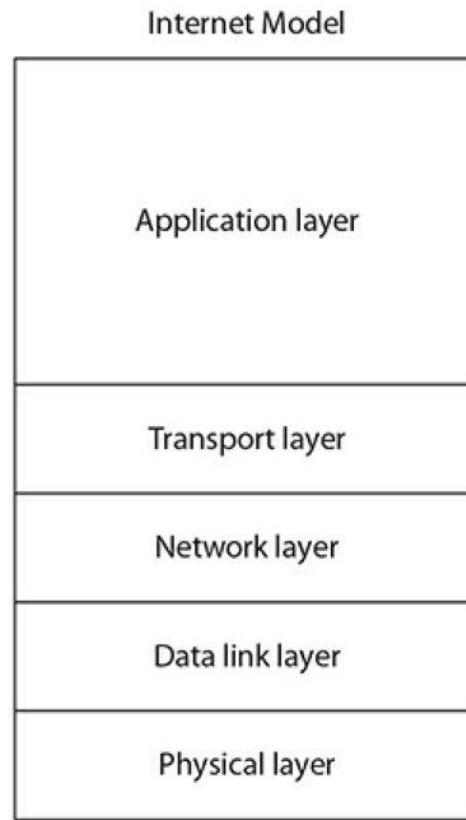
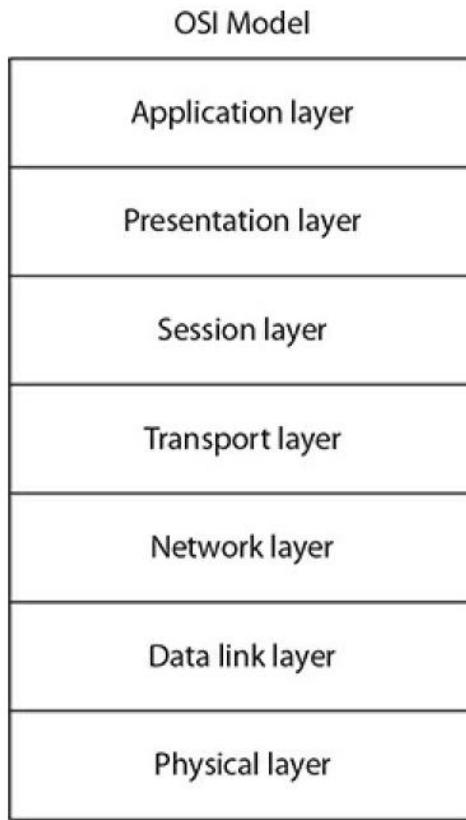
Term	Example in Scooter scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat actor	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Attack vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Stolen scooter	Virus infection or stolen data

NETWORK COMMUNICATION

- Protocols
 - Rules for communication
 - Essential for proper communication between network devices
 - Open Systems Interconnection (OSI) Reference Model
- Transmission Control Protocol/Internet Protocol (TCP/IP)
 - Most common protocol suite used for local area networks and the Internet
 - Comprises several protocols that all function together



OSI AND INTERNET NETWORK MODELS

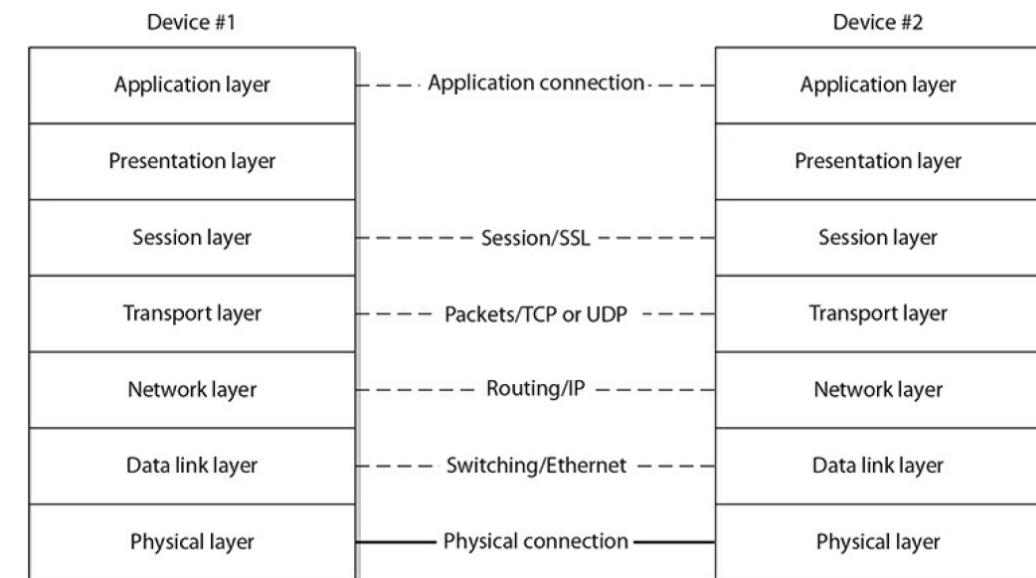


Mnemonic for seven layers of the OSI model

OSI memory aid

Away	= (Application)	Layer 7
Pizza	= (Presentation)	Layer 6
Sausage	= (Session)	Layer 5
Throw	= (Transport)	Layer 4
Not	= (Network)	Layer 3
Do	= (Data-Link)	Layer 2
Please	= (Physical)	Layer 1

Representation of the OSI model peer layer logical channels



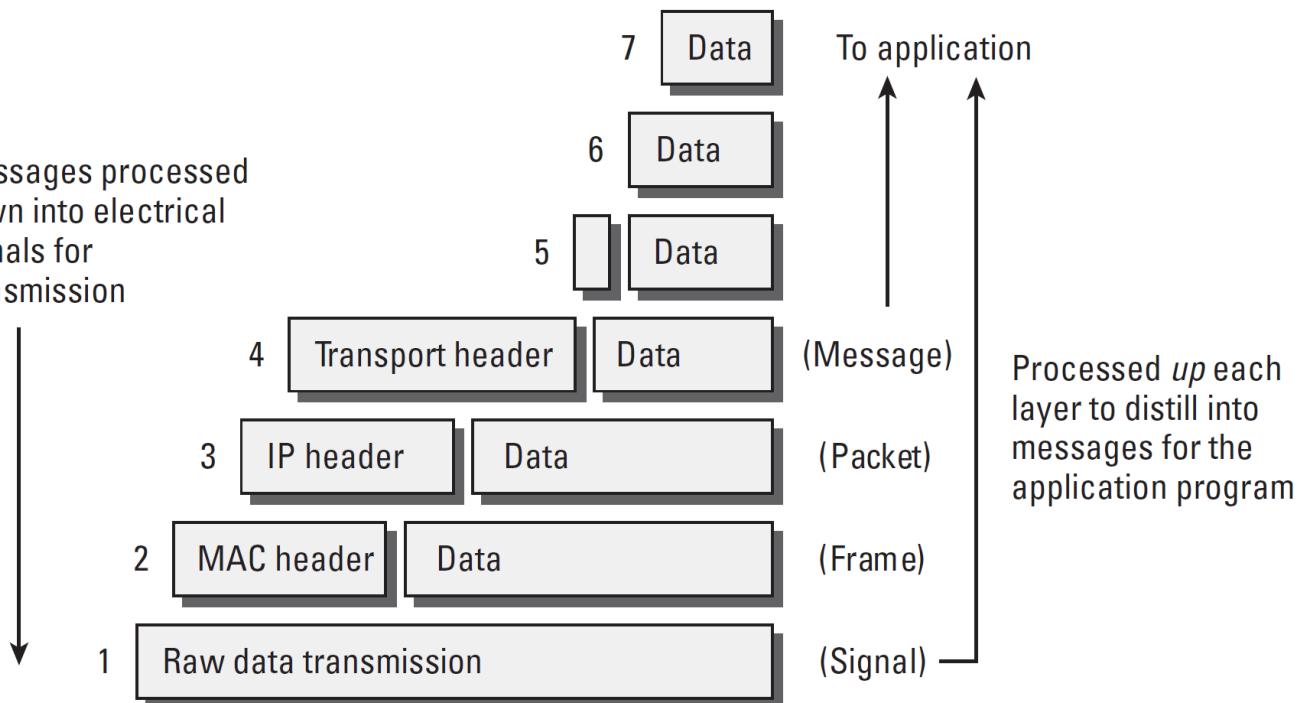
OSI model data names

Application
Presentation
Session
Transport
Network
Data Link
Physical

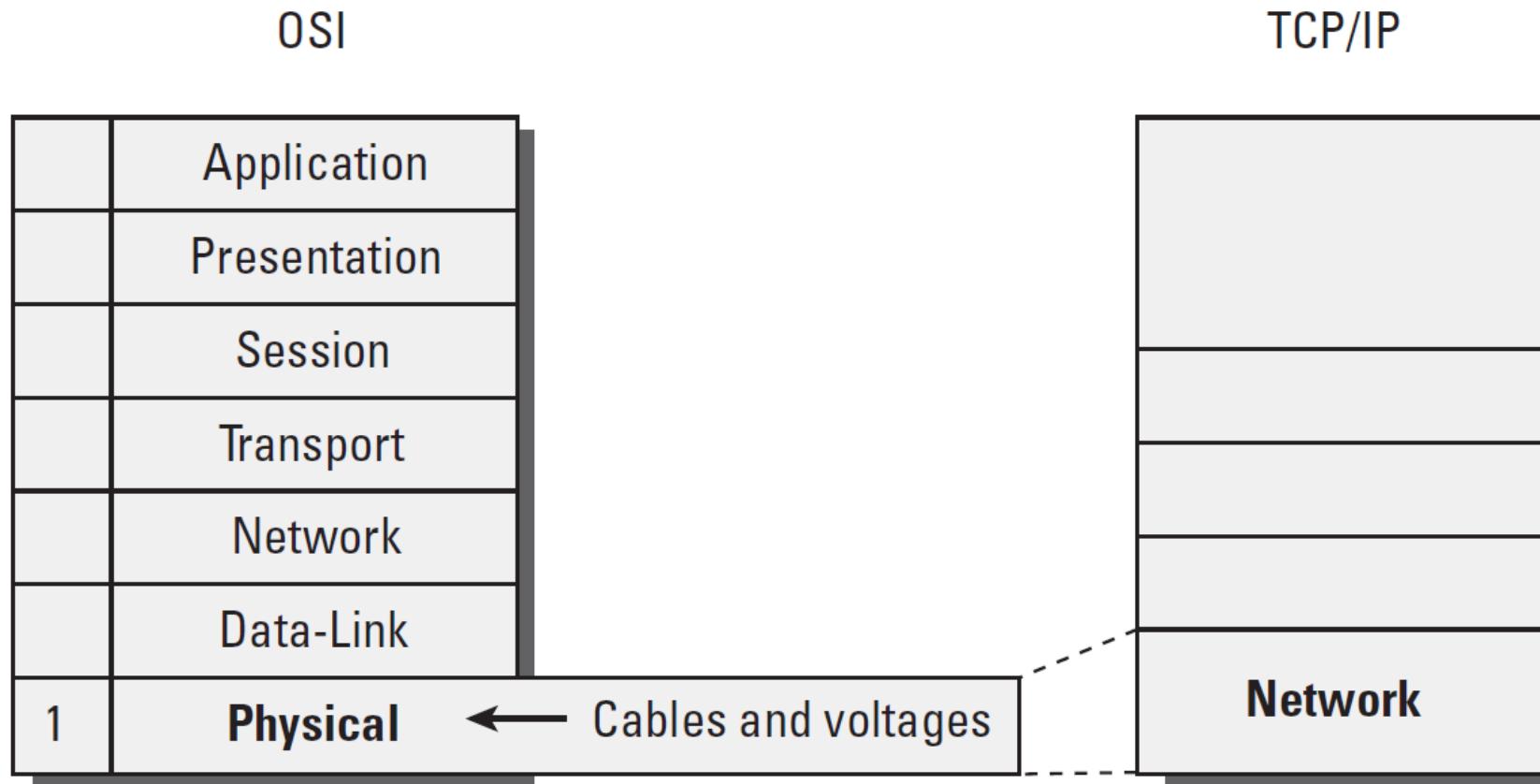
Data stream
Data stream
Data stream
Segment (TCP)/Datagram (UDP)

Packet
Frame
Bits

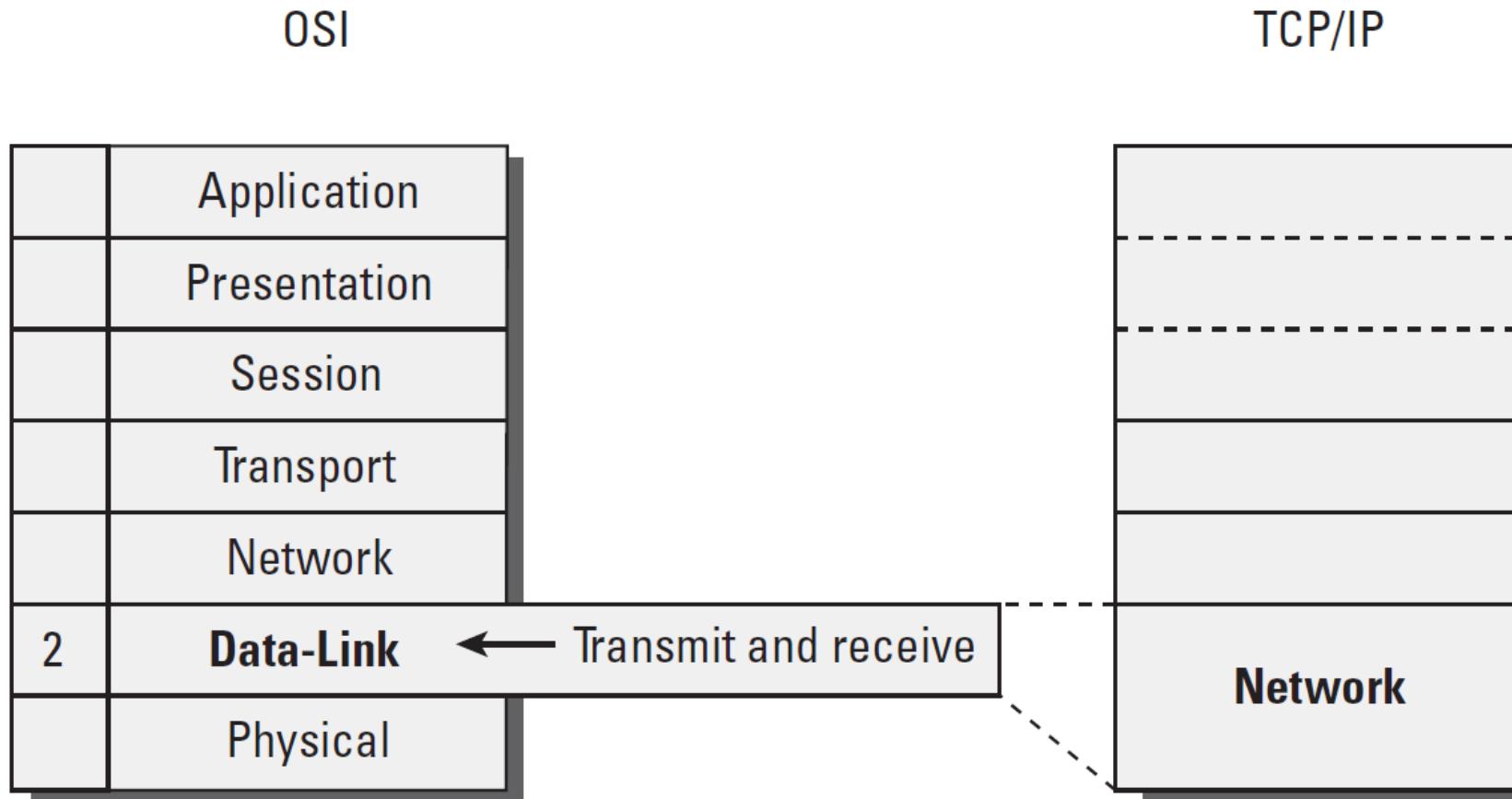
Messages processed
down into electrical
signals for
transmission



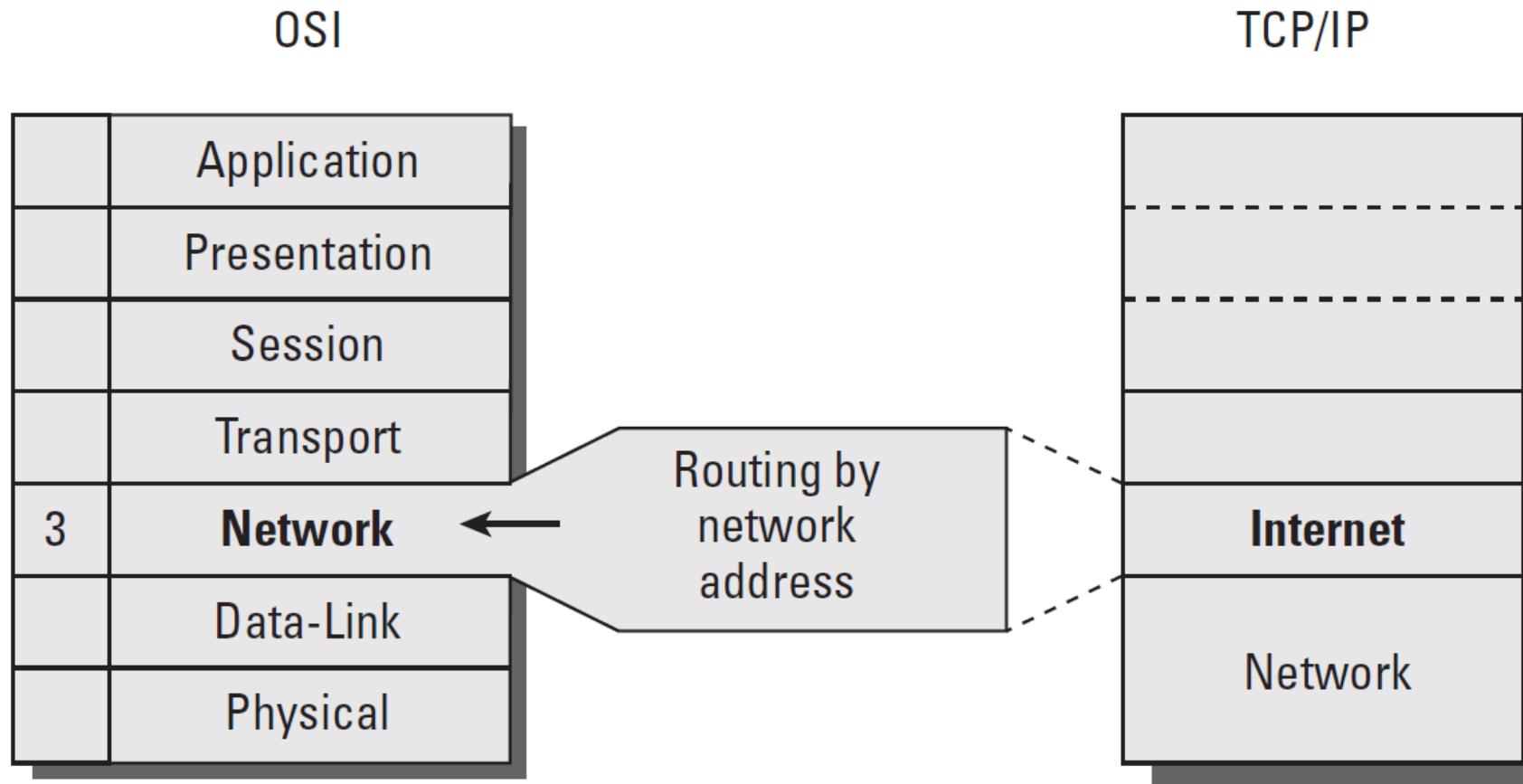
PHYSICAL LAYER



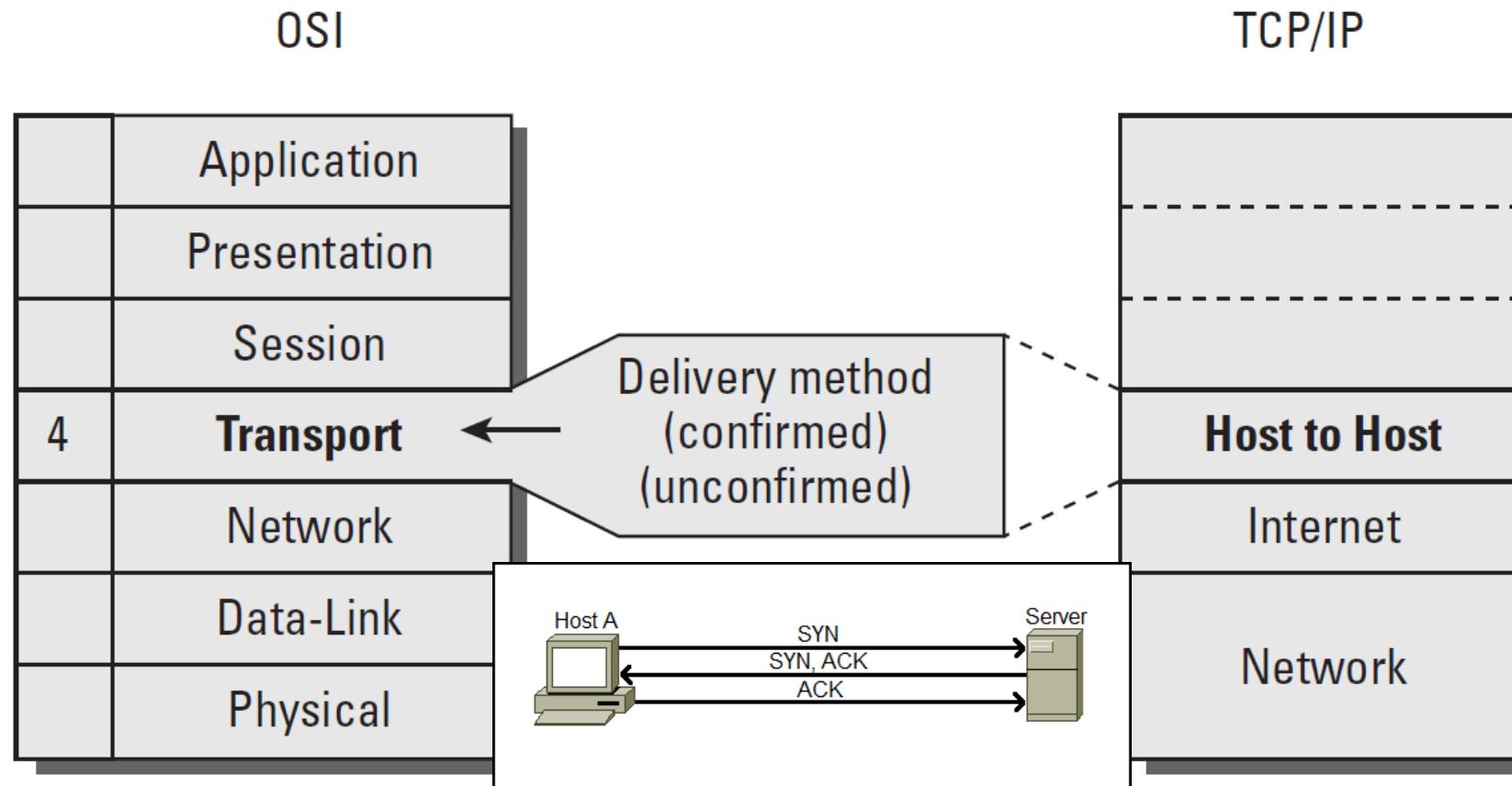
DATA-LINK LAYER



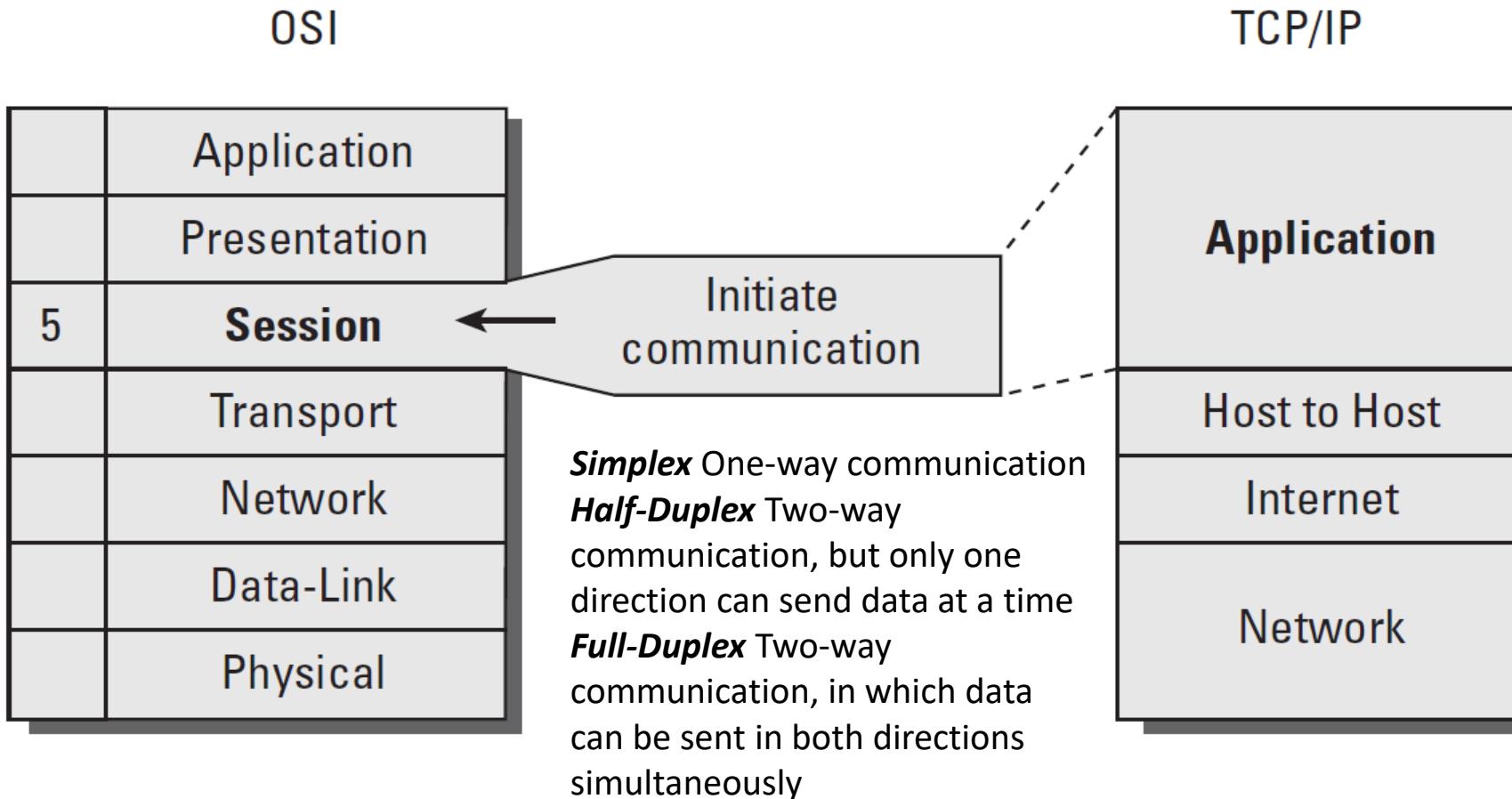
NETWORK LAYER



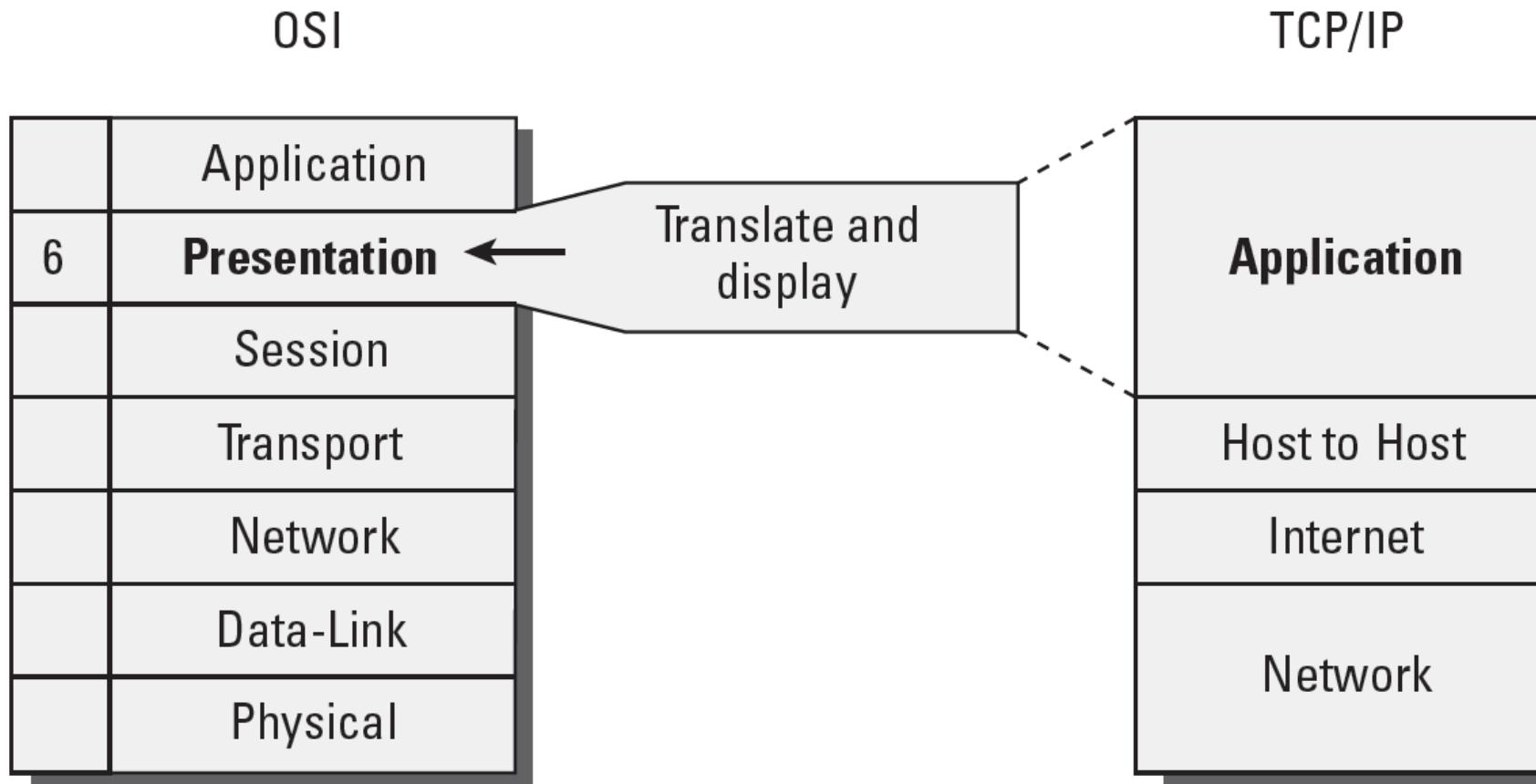
TRANSPORT LAYER



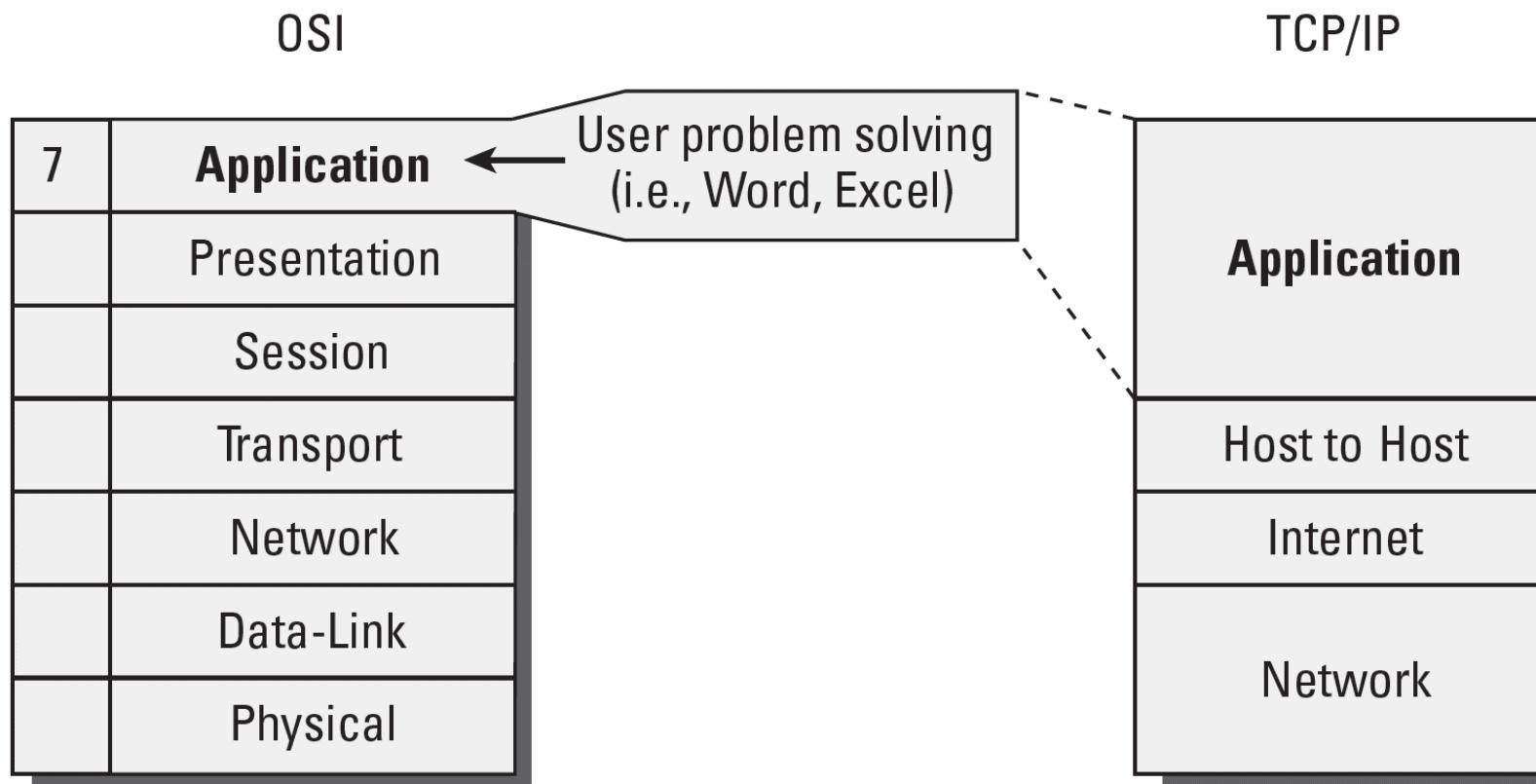
SESSION LAYER



PRESENTATION LAYER



APPLICATION LAYER



ARCHITECTURE AND DESIGN

24%

ARCHITECTURE AND DESIGN

- **Baseline configuration** is the process of identifying and documenting all aspects of an asset's configurations to create a secure template against which all subsequent configurations are measured.
 - **Change control**—monitoring for changes and comparing changes against the established baseline.
- A **naming convention** is a convention for naming things.
- **Internet protocol (IP) schema** is a requirement for communications in a computer network. With an addressing scheme, packets are forwarded from one location to another.
- The **configuration template** is a fictitious configuration management implementation

ARCHITECTURE AND DESIGN

- **Authentication, Authorization and Accounting** is the term for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.
 - As the first process, **authentication** provides a way of identifying a user, typically by having the user enter a valid username and valid password before access is granted.
 - Following authentication, a user must gain **authorization** for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands.
 - The final plank in the AAA framework is **accounting**, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session.

ARCHITECTURE AND DESIGN

- A **honeypot** is essentially bait (passwords, vulnerabilities, fake sensitive data) that's intentionally made very tempting and accessible. The goal is to deceive and attract a hacker who attempts to gain unauthorized access to your network. The honeypot is in turn being monitored by IT security. Anyone caught dipping their paws into the honeypot is often assumed to be an intruder
- **Serverless architecture** is a way to build and run applications and services without having to manage infrastructure. Your application still runs on servers, but all the server management is done by AWS. You no longer have to provision, scale, and maintain servers to run your applications, databases, and storage systems.

ARCHITECTURE AND DESIGN

- **Public clouds** are the most common way of deploying cloud computing. The cloud resources like servers and storage are owned and operated by a third-party cloud service provider and delivered over the Internet. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider
- A **private cloud** consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization.

ARCHITECTURE AND DESIGN

Advantages of public clouds:

1. Lower costs—no need to purchase hardware or software, and you pay only for the service you use.
2. No maintenance—your service provider provides the maintenance.
3. Near-unlimited scalability—on-demand resources are available to meet your business needs.
4. High reliability—a vast network of servers ensures against failure.

Disadvantages of public clouds:

1. Loss of Control-When you outsource your technology to the public cloud, it's out of your hands.
2. Insecure Data-When you entrust your data and applications to the public cloud, you have no real assurances that they will be safe.

ARCHITECTURE AND DESIGN

- **Hybrid clouds** combine on-premises infrastructure, or private clouds, with public clouds so organizations can reap the advantages of both. In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options.
- **Platform as a Service (PaaS)**, provides cloud components to certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain the management of the applications. PaaS is primarily used by developers who are building software or applications and provides the platform for developers to create unique, customizable software. This means developers don't need to start from scratch when creating applications, saving them a lot of time (and money) on writing extensive code.

ARCHITECTURE AND DESIGN

- **Software as a Service (SaaS)** utilizes the internet to deliver applications, which are managed by a thirdparty vendor, to its users. With SaaS, you don't need to install and run software applications on your computer (or any computer). Everything is available over the internet when you log in to your account online. You can usually access the software from any device, anytime (as long as there is an internet connection).
- **Infrastructure as a Service (IaaS)** gives users cloud-based alternatives to on-premise infrastructure, so businesses can avoid investing in expensive on-site resources. IaaS delivers cloud computing infrastructure, including servers, network, operating systems, and storage, through virtualization technology. These cloud servers are typically provided to the organization through a dashboard or an API, giving IaaS clients complete control over the entire infrastructure.

ARCHITECTURE AND DESIGN

- **Anything as a service (XaaS)** describes a general category of services related to cloud computing and remote access. It recognizes the vast number of products, tools, and technologies that are now delivered to users as a service over the internet. Essentially, any IT function can be transformed into a service for enterprise consumption. The service is paid for in a flexible consumption model rather than as an upfront purchase or license.

ARCHITECTURE AND DESIGN

- A **time-based one-time password (TOTP)** is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors. Time-based one-time passwords are commonly used for two-factor authentication and have seen growing adoption by cloud application providers. In two-factor authentication scenarios, a user must enter a traditional, static password as well as a time-based one-time password to gain access to digital information or a computing system. Typically, the temporary passcode expires after 30, 60, 120, or 240 seconds.
- **Event-based OTP** (also called HOTP meaning HMAC-based One-Time Password) is the original One-Time Password algorithm and relies on two pieces of information. The first is the secret key, called the “seed”, which is known only by the token and the server that validates submitted OTP codes. The second piece of information is the moving factor which, in event-based OTP, is a counter. The counter is stored in the token and on the server. The counter in the token increments when the button on the token is pressed, while the counter on the server is incremented only when an OTP is successfully validated.

ARCHITECTURE AND DESIGN

- **SMS Authentication** is a kind of identity proof often used for two-factor authentication (2FA) or multifactor authentication (MFA). In SMS authentication, the user provides a code that has been sent to their phone via SMS as proof of their identity. In theory, SMS authentication provides a second identity factor. While usernames and passwords represent something that only the right user knows, an SMS code delivered to a particular mobile device is evidence of the possession of something (a particular mobile phone) that only the right user should have.
- **Push notifications** is not an authenticated method but is a way of alerting users to information that they have opted-in to from apps and services. Notifications encompass nearly every possible use case and type of service, including other communications mediums like email, SMS, and VoIP.

ARCHITECTURE AND DESIGN

- Biometric authentication is the security process that relies on the unique traits such as retinas, irises, voices, facial characteristics, and fingerprints of an individual to verify that he is who says he is.

Types of biometric authentication technologies:

1. Retina scans produce an image of the blood vessel pattern in the light-sensitive surface lining the individual's inner eye.
2. Iris recognition is used to identify individuals based on unique patterns within the ring-shaped region surrounding the pupil of the eye.
3. Finger scanning, the digital version of the ink-and-paper fingerprinting process, works with details in the pattern of raised areas and branches in a human finger image.
4. Finger vein ID is based on the unique vascular pattern in an individual's finger.
5. Facial recognition systems work with numeric codes called faceprints, which identify 80 nodal points on a human face.

ARCHITECTURE AND DESIGN

- **SDN** is a network architecture approach that enables the network to be intelligently and centrally controlled, or ‘programmed,’ using software applications. This helps operators manage the entire network consistently and holistically, regardless of the underlying network technology
- **Software-Defined Visibility** is a framework that allows users to control and program Gigamon’s Visibility Fabric via REST-based Application Program Interfaces (APIs).

ARCHITECTURE AND DESIGN

- **Version control** systems are a category of software tools that help a software team manage changes to source code over time. Version control software keeps track of every modification to the code in a special kind of database. If a mistake is made, developers can turn back the clock and compare earlier versions of the code to help fix the mistake while minimizing disruption to all team members.
- **Elasticity** is the ability of an IT infrastructure to quickly expand or cut back capacity and services without hindering or jeopardizing the infrastructure's stability, performance, or security.

ARCHITECTURE AND DESIGN

- **Scalability** is the ability of a computer application or product to continue to function well when it is changed in size or volume in order to meet a user's need.
- A **compiler** is a software program that transforms high-level source code that is written by a developer in a high-level programming language into a low-level object code (binary code) in machine language, which can be understood by the processor. The process of converting high-level programming into machine language is known as compilation.

ARCHITECTURE AND DESIGN

- The **staging** server is where you deploy your work for folks to look at – before it goes to production. Think of it as the place you show your client your work. You don't want to show them your dev machine as they may not have time to look at your work right when you know things are stable. By pushing your updates to staging, the client can look it over in a stable format before it gets pushed to production.
- **Development (Dev)** - This is the environment that's on your computer. Here is where you'll do all of your code updates. It's where all of your commits and branches live along with those of your co-workers. The development environment is usually configured differently from the environment that users work in. Nothing you do in the development environment affects what users currently see when they pull up the website. This is just for you and the other web devs to see how new features will work and to try out improvements.

ARCHITECTURE AND DESIGN

- **Quality assurance (QA)** environment is where you test your upgrade procedure against data, hardware, and software that closely simulate the production environment and where you allow intended users to test the resulting application.
- The **production** environment is where users access the final code after all of the updates and testing. Of all the environments, this one is the most important. This is where companies make their money so you can't have any crippling mistakes here. That's why you have to go through the other two environments with all of the testings first.

ARCHITECTURE AND DESIGN

- **Containers** are a solution to the problem of how to get the software to run reliably when moved from one computing environment to another. A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.
- **Thin clients** function as regular PCs, but lack hard drives and typically do not have extra I/O ports or other unnecessary features. Since they do not have hard drives, thin clients do not have any software installed on them. Instead, they run programs and access data from a server. Thin clients can be a cost-effective solution for businesses or organizations that need several computers that all do the same thing.

ARCHITECTURE AND DESIGN

- An **API**, or Application Programming Interface, allows your application to interact with an external service using a simple set of commands. Rather than having to create complex processes yourself, you can use APIs to access the underlying services of another application which can save you time and resources. Many applications that you use every day rely on APIs in some capacity to function, since there are APIs for almost every category imaginable.
- A **microservice** architectural pattern is a modular application development technique that organizes loosely coupled services. Microservice architecture is like an assembly line, where every service has a specialized role. Together, the services create a complete application. These services can be independently deployed and tend to serve a specific purpose. For example, an eCommerce website might have a service for customer information, a service for payments, and a service for shipping logistics.

ARCHITECTURE AND DESIGN

- **Continuous deployment** is a software development method that releases or deploys software automatically into the production environment. In this model, no one manually checks the code and pushes it into your app.
- **Continuous Integration (CI)** is a development practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration can then be verified by an automated build and automated tests. While automated testing is not strictly part of CI it is typically implied. Continuous integration is designed to trigger automatic code integration in the main code base instead of developing in isolation and then integrating them at the end of the development cycle.

ARCHITECTURE AND DESIGN

- **Continuous monitoring** provides security and operations analysts with real-time feedback on the overall health of IT infrastructure, including networks and applications deployed in the cloud. The goal of continuous monitoring is to increase the visibility and transparency of network activity, especially suspicious network activity that could indicate a security breach, and to mitigate the risk of cyber attacks with a timely alert system that triggers a rapid incident response.
- **Continuous delivery** is an ongoing DevOps practice of building, testing, and delivering improvements to software code and user environments with the help of automated tools. The key outcome of the continuous delivery (CD) paradigm is code that is always in a deployable state.

ARCHITECTURE AND DESIGN

- A **decentralized computing** infrastructure in which data, compute, storage, and applications are located between the data source and the cloud is called Fog computing. In this environment, intelligence is at the local area network (LAN) and data is transmitted from endpoints only.
- **Edge computing** is a distributed information technology (IT) architecture in which client data is processed at the periphery of the network, as close to the originating source as possible. One simple way to understand the basic concept of edge computing is by comparing it to cloud computing. In cloud computing, data from a variety of dissimilar sources is sent to a large centralized data center that is often geographically far away from the source of the data.

ARCHITECTURE AND DESIGN

- **Cloud computing** is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.
- **Cluster computing** refers that many of the computers connected on a network and they perform like a single entity. Each computer that is connected to the network is called a node. Cluster computing offers solutions to solve complicated problems by providing faster computational speed, and enhanced data integrity.

ARCHITECTURE AND DESIGN

- A **cold site** is a backup facility with little or no hardware equipment installed. A cold site is essentially an office space with basic utilities such as power, cooling system, air conditioning, and communication equipment. A cold site is the most cost-effective option among the three disaster recovery sites. However, due to the fact that a cold site doesn't have any pre-installed equipment, it takes a lot of time to properly set it up so as to fully resume business operations.
- A **Hot Site** can be defined as a backup site, which is up and running continuously. A Hot Site allows a company to continue normal business operations, within a very short period of time after a disaster. Hot Site must be online and must be available immediately. The hot site must be equipped with all the necessary hardware, software, network, and Internet connectivity. Data is regularly backed up or replicated to the hot site so that it can be made fully operational in a minimal amount of time in the event of a disaster at the original site.

ARCHITECTURE AND DESIGN

- A **warm site** is considered the middle ground between the cold site and the hot site. A warm site is a backup facility that has the network connectivity and the necessary hardware equipment already pre-installed. However, a warm site cannot perform on the same level as the production center because they are not equipped in the same way. Therefore, a warm site has less operational capacity than the primary site.
- The **normal site** is a fictitious type of disaster recovery site.

ARCHITECTURE AND DESIGN

- Data masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.
 - Overall, the primary function of masking data is to protect sensitive, private information in situations where it might be visible to someone without clearance to the information.

ARCHITECTURE AND DESIGN

- **Tokenization** is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. Tokens serve as a reference to the original data, but cannot be used to guess those values. That's because, unlike encryption, tokenization does not use a mathematical process to transform sensitive information into the token.
 - There is no key or algorithm, that can be used to derive the original data for a token. Instead, tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured, often via encryption.

ARCHITECTURE AND DESIGN

- **Encryption** is the process of using an algorithm to transform plain text information into a non-readable form called ciphertext. An algorithm and an encryption key are required to decrypt the information and return it to its original plain text format. Today, SSL encryption is commonly used to protect information as it's transmitted on the Internet.
- **Data at rest** is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/ stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion.

ARCHITECTURE AND DESIGN

- **Symmetric encryption** uses a single key that needs to be shared among the people who need to receive the message. It's a simple technique, and because of this, the encryption process can be carried out quickly. It's mostly used when large chunks of data need to be transferred. The secret key is shared. Consequently, the risk of compromise is higher.
- **Asymmetrical encryption** uses a pair of a public key and a private key to encrypt and decrypt messages when communicating. It's a much more complicated process than symmetric key encryption, and the process is slower. It's used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer. The private key is not shared, and the overall process is more secure as compared to symmetric encryption.

ARCHITECTURE AND DESIGN

- **Lightweight cryptography** is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards and health-care devices.
 - It is very difficult for a resource-limited environment to implement the standard cryptographic algorithms due to the implementation size, speed, or throughput and energy consumption. The lightweight cryptography trade-offs implementation cost, speed, security, performance, and energy consumption on resource-limited devices. The motivation of lightweight cryptography is to use less memory, less computing resource, and less power supply to provide security solutions that can work over resource-limited devices.

ARCHITECTURE AND DESIGN

- The purpose of **homomorphic encryption** is to allow computation on encrypted data. Thus data can remain confidential while it is processed, enabling useful tasks to be accomplished with data residing in untrusted environments. In a world of distributed computation and heterogeneous networking, this is a hugely valuable capability. A homomorphic cryptosystem is like other forms of public encryption in that it uses a public key to encrypt data and allows only the individual with the matching private key to access its unencrypted data. However, what sets it apart from other forms of encryption is that it uses an algebraic system to allow you or others to perform a variety of computations (or operations) on the encrypted data.

ARCHITECTURE AND DESIGN

- **Elliptical curve cryptography (ECC)** is a public key encryption technique based on the elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public-key encryption methods, such as RSA, and Diffie-Hellman.

ARCHITECTURE AND DESIGN

- **Steganography** is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content.

ARCHITECTURE AND DESIGN

- **Hashing** is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. In addition to faster data retrieval, hashing is also used to encrypt and decrypt digital signatures (used to authenticate message senders and receivers)
- **SSL/TLS Inspection** is a man-in-the-middle attack executed to filter out malicious content. SSL Inspection or TLS Interception is done by means of an interception device. This interceptor sits in between the client and server, with all the traffic passing through it. When the connection is made over HTTPS, the inspector intercepts all traffic, decrypts it and scans it. First, the interceptor establishes an SSL connection with the web server. Here, it decrypts and examines the data. Once the scanning is done, it creates another SSL connection—this time with the client (browser). This way, the data gets to the client in an encrypted format—the way it was intended originally.

ARCHITECTURE AND DESIGN

- A **cloud access security broker (CASB)** is an on-premises or cloud-based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies. A CASB can offer a variety of services such as monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware.
- **Managed service provider (MSP)** is a company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.
 - MSSP (managed security service provider)

ARCHITECTURE AND DESIGN

- A **storage area network (SAN)** is a dedicated high-speed network or subnetwork that interconnects and presents shared pools of storage devices to multiple servers. A SAN moves storage resources off the common user network and reorganizes them into an independent, high-performance network. This enables each server to access shared storage as if it were a drive directly attached to the server. When a host wants to access a storage device on the SAN, it sends out a block-based access request for the storage device.
- **Tape storage** is a system in which magnetic tape is used as a recording media to store data. With data volumes growing rapidly worldwide, tape storage is the most suitable system for data storage requiring large capacity. Tape storage is not used only for backup in case of system failure, but also for archiving data for long-term storage.

ARCHITECTURE AND DESIGN

- **Disk storage** is a general category of storage mechanisms where data are recorded by various electronic, magnetic, optical, or mechanical changes to a surface layer of one or more rotating disks. A disk drive is a device implementing such a storage mechanism.
- A **Network-attached storage (NAS)** device is a storage device connected to a network that allows storage and retrieval of data from a central location for authorized network users and varied clients. NAS devices are flexible and scale-out, meaning that as you need additional storage, you can add to what you have. NAS is like having a private cloud in the office. It's faster, less expensive, and provides all the benefits of a public cloud on-site, giving you complete control.

ARCHITECTURE AND DESIGN

- **Network interface card teaming**, also known as Load Balancing/ Failover (LBFO) in the Microsoft world, is a mechanism that enables multiple physical network adapter cards in the same physical host/server to be bound together and placed into a “team” in the form of a single logical NIC. The connected network adapters, shown as one or more virtual adapters. These virtual network adapters provide fast performance and fault tolerance in the event of a network adapter failure.
- **Load balancing** is defined as the methodical and efficient distribution of network or application traffic across multiple servers in a server farm. Each load balancer sits between client devices and backend servers, receiving and then distributing incoming requests to any available server capable of fulfilling them.
 - A load balancer acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance.

ARCHITECTURE AND DESIGN

- **Multipathing** also called SAN multipathing or I/O multipathing is the establishment of multiple physical routes between a server and the storage device that supports it. In storage networking, the physical path between a server and the storage device that supports it can sometimes fail. When there's only one physical path between the two devices, there is a single point of failure (SPoF), which can be a problem if a cable breaks or someone accidentally unplugs the wrong cable. Because SAN multipathing establishes multiple routes between the hardware, however, if someone accidentally unplugged the wrong cable and one path failed, I/O would simply be routed through another path.
- A **redundant array of independent disks (RAID)** is a method of storing duplicate data on two or more hard drives. It is used for data backup, fault tolerance, to improve throughput, increase storage functions, and to enhance performance.

ARCHITECTURE AND DESIGN

- An **uninterruptible power supply (UPS)** is a device that allows a computer to keep running for at least a short time when the primary power source is lost. UPS devices also provide protection from power surges.
- **Power Distribution Unit (PDU)**, is a device used in data centers to control and distribute electric power. The most basic form of a PDU is a large power strip without surge protection. This is designed to provide standard electrical outlets for use within a variety of settings that don't require monitoring or remote access capabilities.

ARCHITECTURE AND DESIGN

- A **digital signature** is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.
- **Key stretching** algorithms take a relatively insecure value, such as a password, and manipulates it in a way that makes it stronger and more resilient to threats like dictionary attacks.

ARCHITECTURE AND DESIGN

- **Salting** is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system.

ARCHITECTURE AND DESIGN

- **Incremental backups** were introduced as a way to decrease the amount of time and storage space that it takes to do a full backup. Incremental backups only back up the data that has changed since the previous backup.
- A **full backup** is exactly what the name implies, it is a full copy of your entire data set.
- A **differential backup** is similar to an incremental backup in that it starts with a full backup and subsequent backups only contain data that has changed. The difference in incremental vs. differential backup is that, while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup.
- A **snapshot backup** is a type of backup copy used to create the entire architectural instance/ copy of an application, disk or system. It is used in backup processes to restore the system or disk of a particular device at a specific time. A snapshot backup can also be referred to as image backup.

ATTACKS, THREATS, AND VULNERABILITIES

21%

ATTACKS, THREATS, AND VULNERABILITIES

- **SQL injection** is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.
- **DLL injection** is another privilege escalation method that attackers are using. It involves the compromising of legitimate processes and services of the Windows operating system. DLL injection is used to run malicious code using the context of a legitimate process. By using the context of a process recognized to be legitimate, an attacker gains several advantages, especially the ability to access the processes memory and permissions.

ATTACKS, THREATS, AND VULNERABILITIES

- **LDAP Injection** is an attack used to exploit web-based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree.
 - What is LDAP? LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication. LDAP provides the communication language that applications use to communicate with other directory services servers.
- **XML Injection** manipulates or compromises the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intended logic of an application, and XML Injection can cause the insertion of malicious content into resulting messages/documents.
 - Extensible Markup Language is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. The design goals of XML emphasize simplicity, generality, and usability across the Internet.
 - With a successful XML Injection attack, the attacker can steal the entire database, or can even log in as the administrator of the website. Other security issues such as XSS and DOS attack can be leveraged with malicious XML Injections.

ATTACKS, THREATS, AND VULNERABILITIES

- A **replay attack** occurs when a cybercriminal eavesdrops on secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.
- **Improper Input Handling** is the term used to describe functions such as validation, sanitization, filtering, or encoding and/or decoding of input data. Improper Input Handling is a leading cause of critical vulnerabilities that exist in today's systems and applications.
 - The root cause of Improper Input Handling is the application trusting, rather than validating, data inputs. One of the key aspects of input handling is validating that the input satisfies certain criteria. All inputs should be considered untrusted as they can come from a variety of mechanisms and be transferred in various formats.

ATTACKS, THREATS, AND VULNERABILITIES

- A **Pass-the-Hash (PtH)** attack is a technique whereby an attacker captures a password hash (as opposed to the password characters) and then simply passes it through for authentication and potentially lateral access to other networked systems. The threat actor doesn't need to decrypt the hash to obtain a plain text password. PtH attacks exploit the authentication protocol, as the password's hash remains static for every session until the password is rotated. Attackers commonly obtain hashes by scraping a system's active memory and other techniques.

ATTACKS, THREATS, AND VULNERABILITIES

- **SSL Stripping or an SSL Downgrade Attack** is an attack used to circumvent the security enforced by SSL certificates on HTTPS-enabled websites. In other words, SSL stripping is a technique that downgrades your connection from secure HTTPS to insecure HTTP and exposes you to eavesdropping and data manipulation.

ATTACKS, THREATS, AND VULNERABILITIES

- **Phishing** is where an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- **Vishing** is when individuals are tricked into revealing critical financial or personal information to unauthorized entities through voice email or VoIP (voice over IP).
- **Spear phishing** is an email or electronic communications scam targeted towards a specific individual, organization or business.

ATTACKS, THREATS, AND VULNERABILITIES

- A **Trojan horse**, or **Trojan**, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network.
 - A Trojan acts as a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.
 - RAT is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program — such as a game — or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet.
- **Computer worm** is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
- **Ransom malware**, or **ransomware** is a type of malware that prevents users from accessing their system or personal files and demands a ransom payment in order to regain access. There are several different ways that ransomware can infect your computer. One of the most common methods today is through malicious spam, which is an unsolicited email that is used to deliver malware. The email might include boobytrapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.
- **Spyware** is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware — malicious software designed to gain access to or damage your computer, often without your knowledge. Spyware gathers your personal information and relays it to advertisers, data firms, or external users. Spyware is used for many purposes. Usually, it aims to track and sell your internet usage data, capture your credit card or bank account information, or steal your personal identity.

ATTACKS, THREATS, AND VULNERABILITIES

- **Malware command and control** (also called C&C or C2) refers to how attackers communicate and exhibit control of the infected system. Upon infecting the system, most malware communicates with the attacker-controlled server (C2 server) either to take commands, download additional components, or to exfiltrate information.
- **Watering hole attack** is a method in which the attacker seeks to compromise a specific group of end-users by infecting websites that members of that group are known to visit. The goal is to infect a victim's computer and gain access to the network within the victims' place of employment. Many conclude that these attacks are an alternative to Spear Phishing but are quite different. Watering Hole attacks are still targeted attacks, but they cast a wider net and trap more victims than the attacker's original objective.

ATTACKS, THREATS, AND VULNERABILITIES

- a **backdoor** refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high-level user access (root access) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.
- **Botnet** is a collection of internetconnected devices infected by malware that allow hackers to control them. Cybercriminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft, and DDoS attacks.

ATTACKS, THREATS, AND VULNERABILITIES

- **Crypto-malware** is one of the latest malware threats, and it's particularly insidious because, unlike ransomware, it can go about doing its work completely undetected. The goal of a crypto-malware isn't to steal data – it is to remain in place for as long as possible, quietly mining in the background.
- A **Logic Bomb** is a malicious program that is triggered when a logical condition is met, such as after a number of transactions have been processed, or on a specific date (also called a time bomb).

ATTACKS, THREATS, AND VULNERABILITIES

- The Keylogger is a malicious program for recording computer user keystrokes to steal passwords and other sensitive information.
- The Rootkit is malicious software that allows an unauthorized user to have privileged access to a computer. A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks. This software remains hidden in the computer and allows the attacker remote access to the computer.

ATTACKS, THREATS, AND VULNERABILITIES

- **Jamming attacks** are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks.
- **Disassociation attacks** exploit the unauthenticated nature of 802.11 management frames. When a station wants to connect to an AP, it first exchanges authentication frames and then association frames. It can participate in the network after it is authenticated and associated. However, any station can spoof a disassociate message, pretending to be another station. The AP disassociates the targeted station, which cannot send traffic until it is associated again. By repeatedly sending these frames, an attacker can keep one or more stations off a network indefinitely. This attack is documented in a paper by John Bellardo and Stephan Savage. The following are several implementations of this attack.

ATTACKS, THREATS, AND VULNERABILITIES

- **Bluesnarfing** is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information — such as the user's calendar, contact list, and e-mail and text messages — without leaving any evidence of the attack.

ATTACKS, THREATS, AND VULNERABILITIES

- **Bluejacking** is the sending of either a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. Bluejacking does not involve the removal or alteration of any data from the device. It can also involve taking control of a mobile device wirelessly.
- A **brute force attack** uses trial-and-error to guess login info, encryption keys, or find a hidden web page. An attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

ATTACKS, THREATS, AND VULNERABILITIES

- **Password Spraying** is a variant of what is known as a brute force attack. In a traditional brute force attack, the perpetrator attempts to gain unauthorized access to a single account by guessing the password repeatedly in a very short period of time.
 - Most organizations have employed countermeasures, commonly a lock-out after three to five attempts. In a Password Spraying attack, the attacker circumvents common countermeasures (e.g., account lockout) by “spraying” the same password across many accounts before trying another password.

ATTACKS, THREATS, AND VULNERABILITIES

- A **rainbow table attack** is a type of hacking wherein the perpetrator tries to use a rainbow hash table to crack the passwords stored in a database system. A rainbow table is a hash function used in cryptography for storing important data such as passwords in a database. Sensitive data are hashed twice (or more times) with the same or with different keys in order to avoid rainbow table attacks.
- A **dictionary attack** is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

ATTACKS, THREATS, AND VULNERABILITIES

- **Dumpster diving** refers to the exploration of a system's trash bin for the purpose of finding details in order for a hacker to have a successful online assault. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network.
- **Shoulder surfing** is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine

ATTACKS, THREATS, AND VULNERABILITIES

- **Credential Harvesting** is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username/ password combinations) for reuse. Attackers use a variety of these tools to aggregate vast quantities of credentials and make them available for sale on the dark web and through other clandestine channels.
- 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 attacker snoops on Internet traffic using a bogus wireless access point. Unwitting web users may be invited to log into the attacker's server, prompting them to enter sensitive information such as usernames and passwords. Often, users are unaware they have been duped until well after the incident has occurred. When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it is sent through their equipment. The attacker is also able to connect to other networks associated with the users' credentials.

ATTACKS, THREATS, AND VULNERABILITIES

- **Rouge AP** is any wireless access point that has been installed on a network's wired infrastructure without the consent of the network's administrator or owner, thereby providing unauthorized wireless access to the network's wired infrastructure.
- An **initialization vector (IV) attack** is an attack on wireless networks. It modifies the initialization vector of an encrypted wireless packet during transmission. Once an attacker learns the plaintext of one packet, the attacker can compute the RC4 keystream generated by the IV used. This keystream can then be used to decrypt all other packets that use the same IV.

ATTACKS, THREATS, AND VULNERABILITIES

- Near-Field-Communication (NFC) is a set of communication protocols for communication between two electronic devices in close proximity.
 - In an eavesdropping scenario, the attacker uses an antenna to record communication between NFC devices. Despite the fact that NFC communication occurs between devices in close proximity, this type of attack is feasible. The interception of an NFC exchange doesn't always translate into the theft of information. In some cases, the attack is meant to corrupt the information being exchanged, making it useless.

ATTACKS, THREATS, AND VULNERABILITIES

- **Spam or spamming** is the use of messaging systems to send an unsolicited message to large numbers of recipients for the purpose of commercial advertising or for the purpose of noncommercial proselytizing.
- **Tailgating attack**, also known as “**piggybacking**,” involves an attacker seeking entry to a restricted area that lacks the proper authentication. The attacker can simply walk in behind a person who is authorized to access the area. In a typical attack scenario, a person impersonates a delivery driver or a caretaker who is packed with parcels and waits when an employee opens their door. The attacker asks that the employee hold the door, bypassing the security measures in place.

ATTACKS, THREATS, AND VULNERABILITIES

- **Pharming** is a cyberattack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in the DNS server.
- **Whaling attack** is a method used by cybercriminals to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes. Also known as CEO fraud, whaling is similar to phishing in that it uses methods such as email and website spoofing to trick a target into performing specific actions, such as revealing sensitive data or transferring money.

ATTACKS, THREATS, AND VULNERABILITIES

- **Typosquatting**, also known as URL hijacking, is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets Internet users who incorrectly type a website address into their web browser (e.g., “Gooogle.com” instead of “Google.com”).
 - When users make such a typographical error, they may be led to an alternative website owned by a hacker that is usually designed for malicious purposes.
 - Hackers often create fake websites that imitate the look and feel of your intended destination so you may not realize you're at a different site.
 - Sometimes these sites exist to sell products and services that are in direct competition with those sold at the website you had intended to visit, but most often they are intended to steal your personal identifiable information, including credit cards or passwords.

ATTACKS, THREATS, AND VULNERABILITIES

- **Impersonation attack** uses social engineering and personalization to trick an employee into unwittingly transferring money to a fraudulent account or sharing sensitive data with cybercriminals.
 - A computer virus hoax is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.
 - Hoaxes can involve a wide range of subjects – warnings about computer viruses or supposed health risks, horror stories, conspiracy theories, calls for donations for the seriously ill and many more. All of these stories are designed to be spectacular but are not based on facts – they are simply being used as bait.

ATTACKS, THREATS, AND VULNERABILITIES

- **Identity fraud** occurs when someone uses your personal identifying information and pretends to be you in order to commit fraud or to gain other financial benefits.
 - Your personal identifying information could include your full name, home address, email address, online login and passwords, Social Security number, driver's license number, passport number, or bank number. Once thieves access this information, they may use it to commit identity theft or sell it on the dark web.
- **Adversarial machine learning** is a machine learning technique that attempts to fool models by supplying deceptive input.
 - Adversarial examples are inputs to machine learning models that an attacker has intentionally designed to cause the model to make a mistake.

ATTACKS, THREATS, AND VULNERABILITIES

- **Privilege escalation** is a type of attack where an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular user account on a network and attempts to gain administrative permissions.
- A **zero-day attack** is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. The software developer must rush to resolve the weakness as soon as it is discovered in order to limit the threat to software users.

ATTACKS, THREATS, AND VULNERABILITIES

- **Cross-site Scripting (XSS)** is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.
 - The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser.
- **Directory traversal (also known as file path traversal)** is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files.
 - In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

ATTACKS, THREATS, AND VULNERABILITIES

- A **buffer overflow** occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information.
 - For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

ATTACKS, THREATS, AND VULNERABILITIES

- **Pretexting** is a form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and steal their victims' personal information. In these types of attacks, the scammer usually says they need certain bits of information from their target to confirm their identity. In actuality, they steal that data and use it to commit identity theft or stage secondary attacks
- **Smishing attack**, the user is tricked into downloading a Trojan horse, virus, or other malware onto his cellular phone or other mobile devices.

ATTACKS, THREATS, AND VULNERABILITIES

- **API Man in the Middle** attack, the attacker intercepts communications between an API endpoint and a client. The attacker steals and/or alters the confidential data that is passed between them.
- **Authentication Hijacking** is when an attackers attempt to bypass or break the authentication methods that a web application is using.
- **Unencrypted Communications** is when attackers take advantage of organizations that don't use Transport Layer Security (TLS) to secure APIs. This gives hackers free reign over the API and the data that passes through it.
- **Injection Attacks** occur when malicious code is embedded into unsecured software. SQLi (SQL injection) and XSS (cross-site scripting) are the most prominent examples, but there are others. Injection attacks are a long-standing threat against web applications; today, they are also a growing threat for APIs.

ATTACKS, THREATS, AND VULNERABILITIES

- **Server-side request forgery** (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing.
 - In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services within the organization's infrastructure, or to external third-party systems.
 - A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

ATTACKS, THREATS, AND VULNERABILITIES

- The purpose of **Cross-site request forgery** (also known as CSRF) attacks is to force a user to take undesired actions on their online account. Accomplishing this involves taking advantage of state-changing requests, where a web server will take some action based upon an authenticated user browsing to a particular page.
 - Examples may include changing an account password or making a transaction via an online banking portal.
- **DNS poisoning** also referred to as DNS spoofing, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address.
 - This results in traffic being diverted to the attacker's computer (or any other computer) or to the wrong websites.

ATTACKS, THREATS, AND VULNERABILITIES

- The MAC Flooding is an attacking method intended to compromise the security of the network switches. In a typical MAC flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses.
 - The intention of the attacker is to consume the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So a considerable number of incoming frames will be flooded at all ports.

ATTACKS, THREATS, AND VULNERABILITIES

- An **ARP spoofing**, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.
- The attack works as follows:
 1. The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router. The attacker uses a spoofing tool, such as Arpspoof or Driftnet, to send out forged ARP responses.
 2. The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
 3. The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
 4. The attacker is now secretly in the middle of all communications.

ATTACKS, THREATS, AND VULNERABILITIES

- **MAC address cloning** is the process of setting the MAC address of the device WAN port to be the same MAC address as your PC or some other MAC address. For example, some ISPs register your computer card MAC address when the service is first installed. When you place a router behind the cable modem or DSL modem, the MAC address from the device WAN port is not recognized by the ISP.
- A **man-in-the-browser** attack uses a Trojan horse (typically spread through email) to install malware as an extension or Browser Helper Object (BHO). The malware initiates a man-in-the-browser attack by intercepting all communication between a user's browser and a destination Web server, changing the messages or transactions as they occur in real-time.

ATTACKS, THREATS, AND VULNERABILITIES

- **Downgrade attacks** are network attacks that force victims to use older, more vulnerable versions of software in order to exploit known vulnerabilities against them. An example of a downgrade attack might be redirecting a visitor from an HTTPS version of a resource to an HTTP copy.
- A **birthday attack** is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes).
 - In probability theory, the birthday paradox or birthday problem considers the probability that some paired people in a set of n randomly chosen of them, will have the same birthday.

ATTACKS, THREATS, AND VULNERABILITIES

- A **collision attack** finds two identical values among elements that are chosen according to some distribution on a finite set.
 - In cryptography, one typically assumes that the objects are chosen according to a uniform distribution. In most cases, a repeating value or collision results in an attack on the cryptographic scheme.
- **Reconnaissance** is an important step in exploring an area to steal confidential information. It also plays a key role in penetration testing. A proper recon would provide detailed information and open doors to attackers for scanning and attacking all the way. By using a recon, an attacker can directly interact with potential open ports, services running, or attempt to gain information without actively engaging with the network.

ATTACKS, THREATS, AND VULNERABILITIES

- **Footprinting** is a part of the reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active.
 - Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.
 - During this phase, a hacker can collect the following information.
 1. Domain name
 2. IP Addresses
 3. Namespaces
 4. Employee information
 5. Phone numbers
 6. E-mails
 7. Job Information

ATTACKS, THREATS, AND VULNERABILITIES

- **URL redirection** attack redirects victims from the current page to a new URL which is usually a phishing page that impersonates a legitimate site and steals credentials from the victims. Such techniques are a common practice and a widely used method for attackers to trick victims.
- **Domain hijacking** is the act of changing the registration of a domain name without the permission of the original owner, or by abuse of privileges on domain hosting and domain registrar systems.

ATTACKS, THREATS, AND VULNERABILITIES

- The **Rules of Engagement**, or ROE, are meant to list out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being tested when it's being tested, and how it's being tested. Lateral movements is incorrect.
- **Lateral movements** are used by cybercriminals to move throughout a network systematically to search for sensitive data or assets to perform data exfiltration. PowerShell is the number one mechanism by which to implement lateral movement techniques. PowerShell uses objectoriented scripting that makes stealing credentials, system configuration modification, and automation of movement from system to system as easy as it is legal to own.
- **Pivoting** is a powerful technique in the arsenal of a web application penetration tester (pen tester). Once a host has been compromised, the pen tester looks for information to plunder. Common artifacts of interest include such things as user accounts, password hashes, and knowledge of other systems or networks that might be accessible from the host. The pen tester might be able to use the compromised host as a bridge to pivot to another network or system that is not directly accessible from the attacking system.
- A **Bug Bounty** is a reward offered for security vulnerabilities discovered within a set scope. Bug Bounty programs utilize a pay for results model, leveraging the crowdsourced model. One of the biggest benefits of a Bug Bounty Program is that companies pay for valid results, versus paying for time and effort spent.
 - Bug Bounty programs can be public or private, meaning they can be open to anyone in the researcher community, or they can be invite-only offering organizations the opportunity to utilize the power of the crowd – volume of testers, diversity of skill and perspective and competitive environment – in a more controlled and stringent environment

ATTACKS, THREATS, AND VULNERABILITIES

- **DNS amplification** is a Network layer **DDoS attack**. This DDoS attack is a reflection-based volumetric distributed denial of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.

ATTACKS, THREATS, AND VULNERABILITIES

- A false positive state is when the IDS identifies an activity as an attack but the activity is acceptable behavior. A false positive is a false alarm.
- A False negative state is the most serious and dangerous state. This is when the IDS identifies an activity as acceptable when the activity is actually an attack. That is, a false negative is when the IDS fails to catch an attack.

ATTACKS, THREATS, AND VULNERABILITIES

- **Non-credentialed scans** - Non-credentialed as the name suggests, do not require credentials and do not get trusted access to the systems they are scanning. While they provide an outsider's eye view of an environment, they tend to miss most vulnerabilities within a target environment. Non-credentialed scans give a very incomplete picture of vulnerability exposure.
- **Credentialed scans** - Credentialed require logging in with a given set of credentials. These authenticated scans are conducted with a trusted user's eye view of the environment. Credentialed scans uncover many vulnerabilities that traditional (non-credentialed) scans might overlook. Because credentialed scans require privileged credentials to gain access for scanning, organizations should look to integrate an automated privileged password management tool with the vulnerability scanning tool, to ensure this process is streamlined and secure.

ATTACKS, THREATS, AND VULNERABILITIES

- **War driving** also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna that can be mounted on top of or positioned inside the car.
- **Open Source Intelligence (OSINT)** is the collection and analysis of information that is gathered from the public, or open, sources. OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence. OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD), as “produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement”.
- **Cleanup** is the final stage in every penetration test is cleaning up all that has been done during the testing process. For this reason, during a penetration test, you must keep track of all the payloads you may have dropped to disk and which modules you may need to clean up after you have run them.

ATTACKS, THREATS, AND VULNERABILITIES

- **Common Vulnerabilities and Exposures (CVE)** is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE Entries are comprised of an identification number, a description, and at least one public reference.
- **Log aggregation** is a software function that consolidates log data from throughout the IT infrastructure into a single centralized platform where it can be reviewed and analyzed. Log aggregation is just one aspect of an overall log management process that produces real-time insights into application security and performance.
- **Sentiment analysis** helps data analysts within large enterprises gauge public opinion, conduct nuanced market research, monitor brand and product reputation, and understand customer experiences.
- **Security Orchestration, Automation and Response (SOAR)** is a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance. The goal of using a SOAR stack is to improve the efficiency of physical and digital security operations.

ATTACKS, THREATS, AND VULNERABILITIES

- **Black-Hat Hackers** violate computer security for personal gain without permission (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness (such as creating a botnet and using that botnet to perform DDoS attacks against websites they don't like.)
- **White-hat hackers** are the opposite of black-hat hackers. They're the "ethical hackers," experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes.
- A **Gray-hat hacker** falls somewhere between a black hat and a white hat. A gray hat doesn't work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things.
- **Red hats hackers** are the most sophisticated hackers of them all. Red hats are motivated by a desire to end black hat hackers but do not want to play by society's rules.

ATTACKS, THREATS, AND VULNERABILITIES

- In a **black-box testing** assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available. A black-box penetration test determines the vulnerabilities in a system that are exploitable from outside the network. The limited knowledge provided to the penetration tester makes black-box penetration tests the quickest to run since the duration of the assignment largely depends on the tester's ability to locate and exploit vulnerabilities in the target's outwardfacing services.
- A **gray-box tester** has the access and knowledge levels of a user, potentially with elevated privileges on a system. Gray-box pen-testers typically have some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network. The purpose of gray-box pen testing is to provide a more focused and efficient assessment of a network's security than a black-box assessment. Using the design documentation for a network, pentesters can focus their assessment efforts on the systems with the greatest risk and value from the start, rather than spending time determining this information on their own.
- **White-box** and **Open-box**, fall on the opposite end of the spectrum from black-box testing. Penetration testers are given full access to source code, architecture documentation and so forth. The main challenge with white-box testing is sifting through the massive amount of data available to identify potential points of weakness, making it the most time-consuming type of penetration testing.

ATTACKS, THREATS, AND VULNERABILITIES

- The goal of most **Advanced persistent threat attacks** is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible. Because a great deal of effort and resources usually go into carrying out APT attacks, hackers typically target high-value targets, such as nation-states and large corporations, with the ultimate goal of stealing information over a long period of time.
- **Insider threat** is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.
- **Nation-State actors** aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.
- **Hacktivism** uses cyber-attacks based on political motivations who use cyber sabotage to promote a specific cause. As opposed to the hacking industry intent on data theft, hacktivism is not motivated by money and high visibility is key. Hacktivisms are motivated by revenge, politics, ideology, protest and a desire to humiliate victims. Profit is not a factor.
- **Script kiddies** are actors who lack skills to write their own malicious code, so they rely on scripts they can get from other sources.

ATTACKS, THREATS, AND VULNERABILITIES

- **Misconfigured Cloud Storage** - Cloud storage is a rich source of stolen data for cybercriminals. Despite the high stakes, organizations continue to make the mistake of misconfiguration of cloud storage which has cost many companies greatly.
- **Poor Access Control** - Another prevalent cyberattack in the cloud has to do with vulnerabilities around access control. Often this is due to weak authentication or authorization methods or is linked to vulnerabilities that bypass these methods.
- **Shared Tenancy** - Another rare security vulnerability in the cloud that takes a high level of skill to exploit; it's called shared tenancy. As you are probably aware, cloud platforms involve a number of software and hardware components. Adversaries who are able to determine the software or hardware used in a cloud architecture could take advantage of known vulnerabilities and elevate privileges in the cloud.

ATTACKS, THREATS, AND VULNERABILITIES

- **Shadow IT** is a term that refers to Information Technology (IT) applications and infrastructure that are managed and utilized without the knowledge of the enterprise's IT department. Shadow IT can include hardware, software, web services or cloud applications that employees turn to without IT authorization to accomplish their tasks and projects.
- **Indicators of compromise (IOCs)** are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity.
- **Open-source intelligence** means collecting information from public sources, analyzing it, and using it for intelligence purposes. The information sources can be anything from television and print newspapers to blogs and websites, social media, research papers, business and sales documents, and anything you can find online or offline.

ATTACKS, THREATS, AND VULNERABILITIES

- **Red Teams** are the attackers. While not strictly required, Red Teams are usually outside contractors – since the best testing is done by a team with a lot of knowledge of how to break in, but no knowledge of what security is already in place. Knowing what security is being used can lead to some attacks being automatically avoided because there is security in place – which can lead to vulnerabilities being missed if that security isn't properly configured.
- **Blue teams** are the defenders. Blue Teams have two major areas of operations. They continually attempt to harden security around and within the company's data systems and networks – even when no testing is going on. They can also act as an active part of the defensive systems when the Red Team is attacking.
- **White team** oversees the cyber defense competition and adjudicates the event. They are also responsible for recording scores for the Blue Teams given by the Red Team on usability and security, respectively. The White Team also reads the security reports and scores them for accuracy and countermeasures.
- **Purple Teams** are a single group of people who do both Red and Blue testing and securing of a company. They may be a consulting group brought in for an audit, or employees of the company directly, but they do not focus exclusively on attacking or defending – they do both. Purple Teams are effective for spot-checking systems in larger organizations as well, but it is generally best to have opposing and independent teams whenever possible.

ATTACKS, THREATS, AND VULNERABILITIES

- **URL redirection attack** redirects victims from the current page to a new URL which is usually a phishing page that impersonates a legitimate site and steals credentials from the victims. Such techniques are a common practice and a widely used method for attackers to trick victims.
- **DNS spoofing** is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer) or to the wrong websites.
- **Domain hijacking** is the act of changing the registration of a domain name without the permission of the original owner, or by abuse of privileges on domain hosting and domain registrar systems.

ATTACKS, THREATS, AND VULNERABILITIES

- The **known-plaintext attack (KPA)** is an attack model for cryptanalysis where the attacker has access to both the plaintext and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and codebooks.
- A **supply chain attack** also called a value-chain or third-party attack occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.
- **Skimming** is a method used by identity thieves to capture payment and personal information from a credit cardholder. Several approaches can be used by fraudsters to procure card information with the most advanced approach involving a small device called a skimmer that reads the information stored in a card's magnetic strip or microchip.

ATTACKS, THREATS, AND VULNERABILITIES

- **Refactoring** is the process of changing a computer program's internal structure without modifying its external functional behavior or existing functionality.
- **Shimming** is a small library that transparently intercepts API calls and changes the arguments passed. They also can be used for running programs on different software platforms than they were developed for.

IMPLEMENTATION

25%

IMPLEMENTATION

- **Remote wipe** is a security feature for mobile device management that allows you to remotely clear data from a lost or stolen mobile device.
- **Geofencing** is a location-based service that businesses use to engage their audience by sending relevant messages to smartphone users who enter a pre-defined location or geographic area. Companies send product offers or specific promotions to consumers' smartphones when they trigger a search in a particular geographic location, enter a mall, neighborhood, or store.
- **Geolocation** refers to the use of location technologies such as GPS or IP addresses to identify and track the whereabouts of connected electronic devices. Because these devices are often carried on an individual's person, geolocation is often used to track the movements and location of people and surveillance.
- **Push notifications** are clickable pop-up messages that appear on your users' browsers irrespective of which device they use or which browser they are on. Subscribers can be anywhere on the browser and still receive these messages as long as they are online or have their browsers running on their devices.
 - Browser push notifications are different from in-app notifications because in-app notifications appear only when triggered by an existing application on your mobile device, while browser push notifications can be triggered through browsers on any device as long as the user subscribes to receive your notifications. It is an instant mode of automated, direct communication between a website and its end users.

IMPLEMENTATION

- **SSH**, also known as **Secure Shell** or **Secure Socket Shell**, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.
 - Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet. In addition to providing strong encryption, SSH is widely used by network administrators for managing systems and applications remotely, enabling them to log in to another computer over a network, execute commands and move files from one computer to another. SRTP is incorrect.
- **SRTP** also known as **Secure Real-Time Transport Protocol**, is an extension profile of RTP (Real-Time Transport Protocol) which adds further security features, such as message authentication, confidentiality and replay protection mostly intended for VoIP communications.
- The **Lightweight Directory Access Protocol (LDAP)** is a vendor-neutral application protocol used to maintain distributed directory info in an organized, easy-to-query manner. That means it allows you to keep a directory of items and information about them.
- **Hypertext transfer protocol secure (HTTPS)** is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.

IMPLEMENTATION

- **DHCP snooping** is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes. However, the most common DoS scenario is that of an end-user plugging in a consumer-grade router at their desk, ignorant that the device they plugged in is a DHCP server by default.
- **MAC filtering** is a security method based on access control. In this, each address is assigned a 48-bit address which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address.
- **Jump server** is a system on a network used to access and manage devices in a separate security zone. A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. The most common example is managing a host in a DMZ from trusted networks or computers. The jump server acts as a single audit point for traffic and also a single place where user accounts can be managed. A prospective administrator must log into the jump server in order to gain access to the DMZ assets and all access can be logged for later audit.

IMPLEMENTATION

- **Next-generation firewall (NGFW)** filters network traffic to protect an organization from external threats. Maintaining features of stateful firewalls such as packet filtering, VPN support, network monitoring, and IP mapping features, NGFWs also possess deeper inspection capabilities that give them a superior ability to identify attacks, malware, and other threats.
 - Next-generation firewalls provide organizations with application control, intrusion prevention, and advanced visibility across the network. As the threat landscape continues to develop rapidly, traditional firewalls fall further behind and put your organization at risk. NGFWs not only block malware, but also include paths for future updates, giving them the flexibility to evolve with the landscape and keep the network secure as new threats arise.
- **Endpoint detection and response (EDR)** is an emerging technology that addresses the need for continuous monitoring and response to advanced threats. Endpoint detection and response tools work by monitoring endpoint and network events and recording the information in a central database where further analysis, detection, investigation, reporting, and alerting take place. A software agent installed on the host system provides the foundation for event monitoring and reporting.
- **Anti-malware** tools may employ scanning, strategies, freeware, or licensed tools to detect rootkits, worms, Trojans, and other types of potentially damaging software. Each type of malware resource carries its own interface and system requirements, which impact user solutions for a given device or system.
- **Antivirus software** helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware as quickly as possible.

IMPLEMENTATION

- **Simple Network Management Protocol (SNMP)** is a way for different devices on a network to share information with one another. It allows devices to communicate even if the devices are different hardware and run different software. Without a protocol like SNMP, there would be no way for network management tools to identify devices, monitor network performance, keep track of changes to the network, or determine the status of network devices in real-time.
 - Simple Network Management Protocol (SNMP) provides a message format for communication between what are termed, managers, and agents. An SNMP manager is a network management application running on a PC or server, with that host typically being called a Network Management Station (NMS).
 - As for the SNMP protocol messages, all versions of SNMP support a basic clear-text password mechanism, although none of those versions refer to the mechanism as using a password. SNMP Version 3 (SNMPv3) adds more modern security as well.
 - The following are SNMPv3 features:
 1. **Message integrity:** This mechanism, applied to all SNMPv3 messages, confirms whether or not each message has been changed during transit.
 2. **Authentication:** This optional feature adds authentication with both a username and password, with the password never sent as clear text. Instead, it uses a hashing method like many other modern authentication processes.
 3. **Encryption (privacy):** This optional feature encrypts the contents of SNMPv3 messages so that attackers who intercept the messages cannot read their contents.

IMPLEMENTATION

- **DMZ (demilitarized zone)**, also sometimes known as a perimeter network or a screened subnet, is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks — usually the public internet. External-facing servers, resources, and services are located in the DMZ. Therefore, they are accessible from the internet, but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data through the internet.
- **VLAN (virtual LAN)** is a subnetwork that can group together collections of devices on separate physical local area networks (LANs).
 - A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area. A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch.

IMPLEMENTATION

Here are the main reasons why VLANs are used:

1. VLANs increase the number of broadcast domains while decreasing their size.
2. VLANs reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.
3. You can keep hosts that hold sensitive data on a separate VLAN to improve security.
4. You can create more flexible network designs that group users by department instead of by physical location.
5. Network changes are achieved with ease by just configuring a port into the appropriate VLAN.

IMPLEMENTATION

- A **Virtual Private Network (VPN)** is a service that allows you to connect to the Internet via an encrypted tunnel to ensure your online privacy and protect your sensitive data. A VPN is commonly used to secure connection to a public Wi-Fi hotspot, hide IP address, and make your browsing private.
- **DNS** stands for **Domain Name System**. It's a system that lets you connect to websites by matching human readable domain names (like examsdigest.com) with the unique ID of the server where a website is stored.
 - Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers.

IMPLEMENTATION

- **Application blacklisting** prevents undesirable programs from executing, while application whitelisting is more restrictive and allows only programs that have been explicitly permitted to run.
 - Application blacklisting, sometimes just referred to as blacklisting, is a network administration practice used to prevent the execution of undesirable programs. Such programs include not only those known to contain security threats or vulnerabilities but also those that are deemed inappropriate within a given organization. Blacklisting is the method used by most antivirus programs, intrusion prevention/detection systems and spam filters.
- **Application whitelisting** is the practice of specifying an index of approved software applications or executable files that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

IMPLEMENTATION

- In **Active/active** mode two or more servers aggregate the network traffic load and work as a team distributes it to the network servers. The load balancers can also remember information requests from users and keep this information in the cache.
- **Active/passive** configuration offers many advantages so you should consider buying a pair of load balancers and configure them in H/A (High Availability) mode.
 - This done the primary load balancer distributes the network traffic to the most suitable server while the second load balancer operates in listening mode to constantly monitor the performance of the primary load balancer, ready at any time to step in and take over the load balancing duties should the primary load balancer be in difficulty and failing.

IMPLEMENTATION

- A **Unified threat management (UTM)** system is a type of network hardware appliance, virtual appliance or cloud service that protects businesses from security threats in a simplified way by combining and integrating multiple security services and features. UTM devices are often packaged as network security appliances that can help protect networks against combined security threats, including malware and attacks that simultaneously target separate parts of the network.
- **Network Address Translation (NAT)** is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.
- **Web application firewall (WAF)** - A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools that together create a holistic defense against a range of attack vectors.
- **Content/URL filter** - URL filtering is a type of technology that helps businesses control their users' and guests' ability to access certain content on the web.

IMPLEMENTATION

- **Port mirroring** copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring or to a VLAN for remote monitoring. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.
 - Port mirroring is needed for traffic analysis on a switch because a switch normally sends packets only to the port to which the destination device is connected. You configure port mirroring on the switch to send copies of unicast traffic to a local interface or a VLAN and run an analyzer application on a device connected to the interface or VLAN.
- **Access Control Lists (ACLs)** are network traffic filters that can control incoming or outgoing traffic. ACLs work on a set of rules that define how to forward or block a packet at the router's interface. An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination. When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it.
- **Quality of service (QoS)** refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network. Quality of service also involves controlling and managing network resources by setting priorities for specific types of data (video, audio, files) on the network. QoS is exclusively applied to network traffic generated for video on demand, IPTV, VoIP, streaming media, videoconferencing, and online gaming.
- **File integrity monitoring (FIM)** refers to an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted.

IMPLEMENTATION

- SFTP, also known as SSH FTP, encrypts both commands and data while in transmission. This means all your data and credentials are encrypted as they pass through the internet. SFTP authenticates your connection using a user ID and password or SSH Keys.
- FTPS, also known as FTP Secure or FTP-SSL, is a more secure form of FTP. FTPS is basic FTP with security added to the data transfer. Special security protocols TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are cryptographic and provide encryption of data to protect your information as it moves from point A to point B, including username/password. FTPS authenticates your connection using a user ID and password, a certificate, or both.
 - SFTP, also known as SSH FTP, encrypts both commands and data while in transmission.
 - FTPS, also known as FTP Secure or FTP-SSL.
 - SFTP protocol is packet-based as opposed to text-based making file and data transfers faster.

IMPLEMENTATION

- A broadcast storm is an abnormally high number of broadcast packets within a short period of time. A broadcast storm can overwhelm switches and endpoints as they struggle to keep up with processing the flood of packets. When this happens, network performance degrades.
- How to reduce broadcast storms:
 1. Storm control and equivalent protocols allow you to ratelimit broadcast packets. If your switch has such a mechanism, turn it on.
 2. Ensure IP-directed broadcasts are disabled on your Layer 3 devices. There's little to no reason why you'd want broadcast packets coming in from the internet going to a private address space. If a storm is originating from the WAN, disabling IP-directed broadcasts will shut it down.
 3. Split up your broadcast domain. Creating a new VLAN and migrating hosts into it will load balance the broadcast traffic to a more acceptable level. Broadcast traffic is necessary and useful, but too much of it eventually leads to a poor network experience.
 4. Check how often ARP tables are emptied. The more frequently they're emptied, the more often ARP broadcast requests occur.
 5. Sometimes, when switches have a hardware failure, their switchports begin to spew out broadcast traffic onto the network. If you have a spare switch of the same or similar model, clone the config of the active switch onto the spare and swap the hardware and cables during a maintenance window. Does the storm subside? If it does, it was a hardware issue. If not, then you've gotta keep digging.
 6. Check for loops in switches. Say there was an unmanaged Layer 2 switch connected upstream to an unmanaged switch, and someone's connected a cable between two ports on the same unmanaged switch (let's say ports 1 and 2). The unmanaged switch will respond to all broadcasts multiple times and flood the broadcast domain with packets, causing a denial of service attack on the network.

IMPLEMENTATION

- A **WiFi heatmap** is a map of wireless signal coverage and strength. Typically, a WiFi heatmap shows a real map of a room, floor, or even a city overlaid by a graphical representation of a wireless signal.
 - The purpose of creating a WiFi heatmap is to obtain accurate information about the quality of coverage of a WiFi network. As you may know, WiFi coverage is affected by many different factors, including:
 - 1. Your WiFi router
 - 2. Other WiFi networks
 - 3. Physical obstacles
 - 4. RF interference
- **WiFi Protected Setup** is a wireless network security standard that tries to make connections between a router and wireless devices faster and easier. WPS works only for wireless networks that use a password that is encrypted with the WPA Personal or WPA2 Personal security protocols.
- **Captive portal** is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources. You can't avoid channel interference is incorrect because there are many tools to avoid channel interference such as Heatmaps, Site surveys & Wifi Analyzers.

IMPLEMENTATION

- **WPA2** - Short for Wi-Fi Protected Access 2, WPA2 is the security method added to WPA for wireless networks that provide stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.
- **WPA3** is the latest version of WiFi Protected Access, a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. The primary enhancement to WPA3 Personal is in the authentication process, where WPA3 makes brute-force dictionary attacks much more difficult and time-consuming for an attacker.
- **CCMP** - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANS), particularly those using WiMax technology. CCMP offers enhanced security compared with similar technologies such as Temporal Key Integrity Protocol (TKIP). CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.
- **SAE** - In cryptography, **Simultaneous Authentication of Equals (SAE)** is a secure password-based authentication and password-authenticated key agreement method. SAE is resistant to passive attack, active attack, and dictionary attack. It provides a secure alternative to using certificates or when a centralized authority is not available. It is a peer-to-peer protocol, has no asymmetry, and supports simultaneous initiation. It is therefore well-suited for use in mesh networks.
- **EAP** - The **Extensible Authentication Protocol (EAP)** is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. In EAP, a user requests a connection to a wireless network through an access point. The access point requests identification (ID) data from the user and transmits that data to an authentication server. The authentication server asks the access point for proof of the validity of the ID. After the access point obtains that verification from the user and sends it back to the authentication server, the user is connected to the network as requested.
- **PEAP (Protected Extensible Authentication Protocol)** is a version of EAP. PEAP is designed to provide more secure authentication for 802.11 WLANS (wireless local area networks) that support 802.1X port access control. PEAP authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS) session, over which the WLAN user, WLAN stations and the authentication server can authenticate themselves.

IMPLEMENTATION

- The main goal of performing a **wireless site survey** is to reveal areas of channel interference and dead zones, helping you avoid problems as you build the network and prevent obstacles for network users. A wireless site survey is used to determine two things. First, you want to determine the feasibility of building a wireless network on your site. Once you have established it's feasible, you'll need to determine the best place for access points and other equipment such as antennas and cables.
 - A site survey also helps you to determine what type of equipment you will need, where it will go, and how it needs to be installed.

IMPLEMENTATION

- Full-disk encryption (FDE) and self-encrypting drives (SED) encrypt data as it is written to the disk and decrypt data as it is read off the disk. FDE makes sense for laptops, which are highly susceptible to loss or theft. But FDE isn't suitable for the most common risks faced in data center and cloud environments.
 - The advantages of full-disk encryption/self-encrypting drives (FDE/SED) include:
 1. Simplest method of deploying encryption
 2. Transparent to applications, databases, and users.
 3. High-performance, hardware-based encryption
 - The limitations of full-disk encryption/self-encrypting drives (FDE/SED) include:
 1. Addresses a very limited set of threats (protects only from physical loss of storage media)
 2. Lacks safeguards against advanced persistent threats (APTs), malicious insiders, or external attackers
 3. Meets minimal compliance requirements
 4. Doesn't offer granular access audit logs

IMPLEMENTATION

- The **Root of Trust** is a concept that starts a chain of trust needed to ensure computers boot with legitimate code. If the first piece of code executed has been verified as legitimate, those credentials are trusted by the execution of each subsequent piece of code.
- **TPM (Trusted Platform Module)** is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.
- **Sandboxing** is a technique in which you create an isolated test environment, a sandbox, in which to execute or detonate a suspicious file or URL that is attached to an email or otherwise reaches your network and then observe what happens. If the file or URL displays malicious behavior, then you've discovered a new threat. The sandbox must be a secure, virtual environment that accurately emulates the CPU of your production servers.

IMPLEMENTATION

- The **Site to Site VPN**, known as point to point VPN, is used to connect two local area networks (LANs). Site to site VPNs are usually utilized by businesses large and small that want to provide their employees or business partners secure access to network resources. Usually, these network resources are files or access to programs that need to be protected.
- **Remote Access** - Remote Access (Personal) VPN is used to connect a personal user device to a remote server on a private network. Once a remote access VPN is connected, a user's internet activity will go through the encrypted VPN tunnel to the remote server and access the internet from that remote server. That means that the internet website or application sees the remote server's IP address instead of your personal device's IP address – which provides a layer of privacy.
- **Split tunnel** - VPN split tunneling lets you route some of your device or app traffic through the encrypted VPN tunnel while other devices or apps access the internet directly. Use split tunneling to protect the traffic you choose, without losing access to local network devices.
- **Proxy server** - A proxy server is not a VPN solution, the proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests.

IMPLEMENTATION

- The **Extensible Authentication Protocol (EAP)** is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. In EAP, a user requests a connection to a wireless network through an access point. The access point requests identification (ID) data from the user and transmits that data to an authentication server. The authentication server asks the access point for proof of the validity of the ID. After the access point obtains that verification from the user and sends it back to the authentication server, the user is connected to the network as requested.
- **PEAP** (Protected Extensible Authentication Protocol) is a version of EAP. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. PEAP authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS) session, over which the WLAN user, WLAN stations and the authentication server can authenticate themselves.
- **RADIUS** - Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point.

IMPLEMENTATION

- **Code signing certificates** are used by software developers to digitally sign apps, drivers, and software programs as a way for end-users to verify that the code they receive has not been altered or compromised by a third party. They include your signature, your company's name, and if desired, a timestamp.
- A **Wildcard SSL Certificate** allows you to secure an unlimited number of first-level sub-domains on a single domain name.
 - That means you can get an SSL Certificate with the common name as *.yourcompany.com and you can use it on all of the following without errors:
 - www.yourcompany.com
 - mail.yourcompany.com
 - intranet.yourcompany.com
 - secure.yourcompany.com
 - me.yourcompany.com
- **Subject alternative name** - A SAN cert allows for multiple domain names to be protected with a single certificate. For example, you could get a certificate for yourcompany.com, and then add more SAN values to have the same certificate protect yourcompany.org, yourcompany.net and even examsdigest.com while the wildcard certificate allows for unlimited subdomains to be protected with a single certificate.
- A **self-signed certificate** is a digital certificate that's not signed by a publicly trusted certificate authority (CA). This can include SSL/TLS certificates, code signing certificates, and S/MIME certificates. The reason why they're considered different from traditional certificate-authority signed certificates is that they've created, issued, and signed by the company or developer who is responsible for the website or software being signed. This is why self-signed certificates are considered unsafe for public-facing websites and applications.

IMPLEMENTATION

- The **OpenID** allows you to use an existing account to sign in to multiple websites, without needing to create new passwords. With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit.
- **Kerberos** is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet.
- **Terminal Access Controller AccessControl System Plus (TACACS+)** is an Authentication, Authorization, and Accounting (AAA) protocol that is used to authenticate access to network devices.
- **OAuth** is an authentication protocol that allows you to approve one application interacting with another on your behalf without giving away your password.
 - For example, you can tell Facebook that it's OK for BBC.com to access your profile or post updates to your timeline without having to give BBC your Facebook password. This minimizes risk in a major way: In the event, BBC suffers a breach, your Facebook password remains safe.

IMPLEMENTATION

- In **Rule-Based Access Control (RBAC)**, you're focusing on the rules associated with the data's access or restrictions. These rules may be parameters, such as allowing access only from certain IP addresses, denying access from certain IP addresses, or something more specific. In a more specific instance, access from a specific IP address may be allowed unless it comes through a certain port (such as the port used for FTP access).
 - When dealing with Role-based access controls, data is protected in exactly the way it sounds like it is: by user roles. Users are sorted into groups or categories based on their job functions or departments, and those categories determine the data that they're able to access. Human Resources team members, for example, might be permitted to access employee information while no other role-based group is permitted to do so.

IMPLEMENTATION

- A **Certificate authority (CA)** also sometimes referred to as a certification authority, is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.
- A **digital certificate** provides:
 1. Authentication, by serving as a credential to validate the identity of the entity that it is issued to.
 2. Encryption, for secure communication over insecure networks such as the Internet.
 3. Integrity of documents signed with the certificate so that they cannot be altered by a third party in transit.
- **Registration Authority** is a company or organization that is responsible for receiving and validating requests for digital certificates and public/private key pairs. A registration authority (RA) is part of the public key infrastructure (PKI).
- **Online Certificate Status Protocol (OCSP)** - When establishing an SSL/TLS session, clients can use Online Certificate Status Protocol (OCSP) to check the revocation status of the authentication certificate. The authenticating client sends a request containing the serial number of the certificate to the OCSP responder (server).
 - The responder searches the database of the certificate authority (CA) that issued the certificate and returns a response containing the status (good, revoked, or unknown) to the client. The advantage of the OCSP method is that it can verify status in real-time, instead of depending on the issue frequency (hourly, daily, or weekly) of CRLs.
- **Certificate signing request (CSR)** is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key.

IMPLEMENTATION

- **Dynamic resource allocation** is the ability to scale up and down resources based on the user's needs.
- **A virtual private cloud (VPC)** is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider. VPCs combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.
- **Network segmentation** in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. The advantages of such splitting are primarily for boosting performance and improving security.
- **A public subnet** is a subnet that's associated with a route table that has a route to an Internet gateway.

IMPLEMENTATION

- **Security Assertions Markup Language** is an important component of many SSO systems that allow users to access multiple applications, services, or websites from a single login process. It is used to share security credentials across one or more networked systems.
- **MAC filtering** is a security method based on access control. In this, each address is assigned a 48-bit address which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address.

IMPLEMENTATION

- **DHCP snooping** is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.
 - The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.
 - Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes. However, the most common DoS scenario is that of an end-user plugging in a consumer-grade router at their desk, ignorant that the device they plugged in is a DHCP server by default.
- **BPDU** - PortFast BPDU guard prevents loops by moving a non trunking port into an errdisable state when a BPDU is received on that port. When you enable BPDU guard on the switch, spanning tree shuts down PortFast-configured interfaces that receive BPDUs instead of putting them into the spanning-tree blocking state.

Practice Questions

Question 1. You have been hired by a company to identify and document all aspects of an asset's configurations in order to create a secure template against which all subsequent configurations will be measured. What type of configuration management will you implement?

- (A) Standard naming conventions
- (B) Internet protocol (IP) schema
- (C) Configuration template
- (D) Baseline configurations

Question 2. Which of the following process is designed to trigger automatic code integration in the main code base instead of developing in isolation and then integrating them at the end of the development cycle?

- (A) Continuous integration
- (B) Continuous delivery
- (C) Continuous monitoring
- (D) Continuous deployment

Question 3. Authentication, _____, and Accounting is the term for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

- (A) Controlling
- (B) Authorization
- (C) Auditing
- (D) Enforcing

Question 4. A company hired you as a security expert. You have been tasked to implement a solution to deceive and attract hackers who attempt to gain unauthorized access to their network in order to gain information about how they operate. Which of the following technique will you implement to meet this requirement as cost-effective as possible?

- (A) Honeyfile
- (B) Honeypots
- (C) DNS Sinkholing
- (D) Honeynet

Question 5. What type of architecture developers use to build and run applications and services without having to manage infrastructure?

- (A) Software-Defined Networking
- (B) Serverless
- (C) Software-Defined visibility
- (D) Transit gateway

Question 6. Your company due to a strict budget migrating to the cloud. The primary reason is to avoid spending money on purchasing hardware and time on maintaining it. The company needs to pay only for the cloud computing resources it uses. Which of the following cloud computing architecture your company will use to deploy the cloud services?

- (A) Public Cloud
- (B) Private Cloud
- (C) Hybrid Cloud
- (D) Community Cloud

Question 7. The developers of your company thinking to switch the development process to the cloud, so they don't need to start from scratch when creating applications with the purpose of saving a lot of time and money on writing code. Which of the following cloud service models developers will use to create unique, customizable software on the Cloud?

- (A) PaaS
- (B) IaaS
- (C) XaaS
- (D) SaaS

Question 8. Which of the following companies is not a cloud service provider?

- (A) Amazon Web Services
- (B) Microsoft Azure
- (C) Examsdigest
- (D) Google Cloud Platform

Question 9. You are developing a new system that requires users to be authenticated using temporary passcode which is generated by an algorithm that uses the current time of day. Which of the following authentication methods will you use to authenticate the users?

- (A) HOTP
- (B) SMS
- (C) Push notifications
- (D) TOTP

Question 10. Version _____ keeps track of every modification to the code in a special kind of database. If a mistake is made, you can turn back the clock and compare earlier versions of the code to help fix the mistake.

- (A) Scalability
- (B) Elasticity
- (C) Control
- (D) Compiler

Question 11. You are working for a client as a web developer and your client asked you to check the new update of the app without making the updates live for the users. In which environment will you push the update so your client can look it over in a stable format before it gets pushed to the users?

- (A) Development
- (B) Quality Assurance
- (C) Production
- (D) Staging

Question 12. The solution to the problem of how to get the software to run reliably when moved from one computing environment to another is known as:

- (A) Containers
- (B) Microservice
- (C) API
- (D) Thin Client

Question 13. A decentralized computing infrastructure in which data, compute, storage, and applications are located between the data source and the cloud is called _____ computing. In this environment, intelligence is at the local area network (LAN) and data is transmitted from endpoints only.

- (A) Fog
- (B) Edge
- (C) Distributed
- (D) Cloud

Question 14. Which of the following types of disaster recovery sites doesn't have any pre-installed equipment and it takes a lot of time to properly set it up so as to fully resume business operations?

- (A) Cold Site
- (B) Hot Site
- (C) Normal Site
- (D) Warm Site

Question 15. The security process that relies on the unique traits such as retinas, irises, voices, facial characteristics, and fingerprints of an individual to verify that he is who says he is, is called:

- (A) Trait authentication
- (B) Characteristics authentication
- (C) Personalized authentication
- (D) Biometric authentication

Question 16. Which of the following options is a network architecture approach that enables the network to be intelligently and centrally controlled, or programmed using software applications and helps operators manage the entire network consistently, regardless of the underlying network technology?

- (A) Serverless
- (B) Transit gateway
- (C) SDN
- (D) SDV

Question 17. Your organization is working with a contractor to build a database. You need to find a way to hide the actual data from being exposed to the contractor. Which of the following technique will you use in order to allow the contractor to test the database environment without having access to actual sensitive customer information?

- (A) Data Masking
- (B) Tokenization
- (C) Encryption
- (D) Data at rest

Question 18. The software that monitoring user activity and automatically preventing malware between cloud service users and cloud applications is known as:

- (A) Cloud access security broker
- (B) Hashing
- (C) Hardware security modules
- (D) SSL/TLS inspection

Question 19. A managed service provider (MSP) is a company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.

- (A) TRUE
- (B) FALSE

Question 20. Which of the following types of disaster recovery sites allows a company to continue normal business operations, within a very short period of time after a disaster?

- (A) Warm Site
- (B) Hot Site
- (C) Cold Site
- (D) Normal Site

Question 21. Recently the physical network adapter card from your company's server broke. As a result, your co-workers couldn't access important resources for hours. You have been instructed to implement a solution to eliminate this from happening again in the event of a network adapter failure. Which of the following solutions will you implement to meet the requirement?

- (A) NIC teaming
- (B) UPS
- (C) PDU
- (D) Power generator

Question 22. Which of the following cryptographic technique will you use to validate the authenticity and integrity of a message or digital document?

- (A) Key stretching
- (B) Digital signatures
- (C) Salting
- (D) Hashing

Question 23. Which of the following products using Software as a Service cloud model? (Choose all that apply.)

- (A) Google Apps
- (B) Dropbox
- (C) Google Compute Engine
- (D) Mailchimp
- (E) AWS EC2
- (F) Slack

Question 24. You are working for a startup and recently the application you are developing experienced a large amount of traffic. As a result, the performance of the application was decreased. You have been instructed to implement a solution to efficiently distributing incoming network traffic across a group of backend servers to increase the performance of the APP.

Which of the following solutions will you implement to meet the requirement?

- (A) Load balancers
- (B) Network interface card teaming
- (C) Multipath
- (D) Redundant array of inexpensive disks

Question 25. You have been instructed to connect a storage device that allows storage and retrieval of data from a central location for authorized network users and varied clients. Which of the following storage type will you use to meet the requirement?

- (A) Storage area network
- (B) Tape storage
- (C) Network-attached storage
- (D) Disk storage

Question 26. Continuous _____ is a software development method that releases or deploys software automatically into the production environment. In this model, no one manually checks the code and pushes it into your app.

- (A) Integration
- (B) Deployment
- (C) Monitoring
- (D) Delivery

Question 27. Which of the following options allows your application to interact with an external service using a simple set of commands rather than having to create complex processes yourself?

- (A) Thin Client
- (B) API
- (C) Microservice
- (D) Containers

Question 28. Cloud backup is a strategy for sending a copy of files or database to a secondary server which is usually hosted by a third-party service provider, for preservation in case of equipment failure or catastrophe. (True/False)

- (A) TRUE**
- (B) FALSE**

Question 29. Asymmetrical encryption uses a single key that needs to be shared among the people who need to receive the message while symmetric encryption uses a pair of a public key and a private key to encrypt and decrypt messages when communicating. (True/False)

- (A) TRUE
- (B) FALSE

Question 30. Which of the following technique will you use to hide secret data within a non-secret file or message with the purpose of avoiding data detection?

- (A) Elliptical curve cryptography
- (B) Homomorphic encryption
- (C) Lightweight cryptography
- (D) Steganography

Question 31. You have been tasked to find a way to transform a plain text sensitive file into a non-readable form and send it through the web. Which of the following technique will you use to send the file through the web and only authorized parties can understand the information?

- (A) Encryption
- (B) Data masking
- (C) Tokenization
- (D) Data at rest

Question 32. Which of the following backup types only back up the data that has changed since the previous backup?

- (A) Full backup
- (B) Incremental backup
- (C) Differential backup
- (D) Snapshot backup

Question 33. Which of the following part(s) of the Authentication, Authorization, and Accounting (AAA) is responsible for measuring the resources a user consumes during access to a system?

- (A) Accounting
- (B) Authorization
- (C) Authentication
- (D) Authentication & Authorization

Question 34. Which of the following actions should be taken to increase the security of SCADA networks? (Choose all that apply)

- (A) Identify all connections to SCADA networks
- (B) Disconnect unnecessary connections to the SCADA network
- (C) Enable unnecessary services
- (D) Implement internal and external intrusion detection systems
- (E) Conduct physical security surveys and assess all remote sites connected to the SCADA network

Question 35. Your company migrates its infrastructure to the public cloud because of the advantages the cloud offers. Which of the following options are considered advantages for using public cloud services? (Choose all that apply.)

- (A) Lower costs
- (B) No maintenance
- (C) Full-control
- (D) Near-unlimited scalability
- (E) High reliability
- (F) Secure data

Question 36. Given the following injection attacks, which one allows an attacker to interfere with the queries that an application makes to its database?

- (A) SQL injection
- (B) DLL Injection
- (C) LDAP Injection
- (D) XML Injection

Question 37. A member of the company asks for a financial transfer by sending an encrypted message to the financial administrator. An attacker eavesdrops on this message, captures it, and is now in a position to resend it. Because it's an authentic message that has simply been resent, the message is already correctly encrypted and looks legitimate to the financial administrator. Then the financial administrator is likely to respond to this new request, that response could include sending a large sum of money to the attacker's bank account. Which of the following type of attack does the scenario describe?

- (A) Improper Input Handling
- (B) Pass the hash attack
- (C) Replay attack
- (D) SSL Stripping

Question 38. The type of malicious code or software that looks legitimate but can take control of your computer is known as _____ . It is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network.

- (A) Worm
- (B) Spyware
- (C) Ransomware
- (D) Trojan

Question 39. _____ attacks are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks.

- (A) Disassociation
- (B) Bluesnarfing
- (C) Bluejacking
- (D) Jamming

Question 40. There are two main techniques for driver manipulating: Shimming and Refactoring. Shiming is the process of changing a computer program's internal structure without modifying its external functional behavior or existing functionality.

- (A) TRUE
- (B) FALSE

Question 41. In which of the following attacks the attacker submitting many passwords or passphrases with the hope of eventually guessing correctly?

- (A) Brute force attack
- (B) Rainbow table attack
- (C) Dictionary attack
- (D) Plaintext Attack

Question 42. Which of the following attacks is a type of hacking wherein the perpetrator tries to crack the passwords stored in a database system?

- (A) Brute force attack
- (B) Rainbow table attack
- (C) Dictionary attack
- (D) Plaintext Attack

Question 43. Which of the following attack occurs when someone infiltrates a system through an outside partner or provider with access to the systems and data?

- (A) Supply-chain attack
- (B) Skimming
- (C) Remote Access Trojan
- (D) Command and control

Question 44. Which of the following types of social engineering is a method in which the attacker seeks to compromise a specific group of end-users by infecting websites that members of that group are known to visit?

- (A) Credential Harvesting
- (B) Shoulder surfing
- (C) Watering hole attack
- (D) Dumpster diving

Question 45. In which of the following wireless network attacks the attacker set up a fraudulent Wi-Fi access point that appears to be legitimate but it is used to eavesdrop wireless communications?

- (A) Rogue Access Point
- (B) Evil Twin
- (C) Initialization Vector
- (D) Near-field Communication

Question 46. Which of the following types of social engineering techniques is the use of messaging systems to send an unsolicited message to large numbers of recipients for the purpose of commercial advertising, or for the purpose of non-commercial proselytizing?

- (A) Tailgating
- (B) Whaling
- (C) Pharming
- (D) Spamming

Question 47. Which of the following attacks is known as URL hijacking?

- (A) Impersonation attack
- (B) Hoax
- (C) Identity fraud
- (D) Typosquatting attack

Question 48. Adversarial machine learning is a machine learning technique that attempts to fool models by supplying deceptive input.

- (A) TRUE
- (B) FALSE

Question 49. What type of attack is when an attacker takes over a regular user account on a network and attempts to gain administrative permissions?

- (A) Cross-site scripting
- (B) Directory traversal
- (C) Privilege escalation
- (D) Buffer overflow

Question 50. A method by which authorized and unauthorized users are able to get around normal security measures and gain high-level user access (root access) on a computer system, network, or software application is known as:

- (A) Backdoor
- (B) Botnet
- (C) Spraying
- (D) Pretexting

Question 51. In which of the following social engineering techniques the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile devices?

- (A) Smishing
- (B) Phising
- (C) Spear phishing
- (D) Vishing

Question 52. The attacker connects to a switch port and start sending a very large number of Ethernet frames with a different fake source MAC address. The switch's MAC address table becomes full and now it's not able to save more MAC address, which means it enters into a fail-open mode and starts behaving like a network Hub. Frames are flooded to all ports, similar to a broadcast type of communication. The attacker's machine will be delivered with all the frames between the victim and other machines. The attacker will be able to capture sensitive data from the network. Given the above scenario, identify the Layer 2 type of attack.

- (A) ARP poisoning
- (B) MAC flooding
- (C) MAC cloning
- (D) Man-in-the-browser

Question 53. Which of the following Cryptographic attacks force victims to use older, more vulnerable versions of software in order to exploit known vulnerabilities against them?

- (A) Birthday
- (B) Collision
- (C) Downgrade
- (D) Reconnaissance

Question 54. Which of the following attacks isn't intended to steal data but to remain in place for as long as possible, quietly mining in the background?

- (A) Logic bomb
- (B) Keylogger
- (C) Rootkit
- (D) Crypto-malware

Question 55. In which of the following API attacks, the attacker intercepts communications between an API endpoint and a client in order to steals and/or alters the confidential data that is passed between them?

- (A) Man in the Middle
- (B) Authentication Hijacking
- (C) Unencrypted Communications
- (D) Injection Attacks

Question 56. Which of the following options are considered as request forgery attacks? (Choose all that apply)

- (A) Server-side
- (B) Cross-site
- (C) Forge-site
- (D) Request-side
- (E) Forge-side

Question 57. A hacker introduced corrupt Domain Name System (DNS) data into a DNS resolver's cache with the aim of redirecting users either to the wrong websites or to his own computer. What type of DNS attack, hacker implement in this scenario?

- (A) DNS Poisoning
- (B) URL redirection
- (C) Domain Hijacking
- (D) DNS Corruption

Question 58. The document that lists out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being tested when it's being tested, and how it's being tested is known as:

- (A) Lateral Movements
- (B) Rules of Engagement
- (C) Pivoting
- (D) Bug Bounty

Question 59. Which of the following attacks is a Network Layer DDoS attack?

- (A)** BGP Hijacking
- (B)** DNS amplification
- (C)** HTTP Flood
- (D)** Slow Read

Question 60. You have set up an Intrusion detection system (IDS) and suddenly the IDS identifies an activity as an attack but the activity is acceptable behavior. The state, in this case, is known as:

- (A) False-positive
- (B) False-negative
- (C) Non-credentialed scans
- (D) Credentialed scans

Question 61. A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. (True/False)

- (A) TRUE
- (B) FALSE

Question 62. _____ is the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

- (A) War Driving
- (B) OSINT
- (C) Footprinting
- (D) Cleanup

Question 63. Which of the following options is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures?

- (A) Log aggregation
- (B) Common Vulnerabilities and Exposures
- (C) Sentiment analysis
- (D) Security Orchestration, Automation, and Response

Question 64. The type of hackers that violates computer security systems without permission, stealing the data inside for their own personal gain or vandalizing the system is commonly known as:

- (A) Black-Hat hackers
- (B) White-Hat hackers
- (C) Red-Hat hackers
- (D) Gray-Hat hackers

Question 65. A hacker attacks a network with the aim of maintaining ongoing access to the targeted network rather than to get in and out as quickly as possible with the ultimate goal of stealing information over a long period of time. Which type of attack a hacker used in this case?

- (A) Insider threat
- (B) State actors
- (C) Hacktivism
- (D) Advanced persistent threat (APT)

Question 66. Which of the following statements are true regarding Cloud-based security vulnerabilities? (Choose all that apply)

- (A) Misconfigured Cloud Storage
- (B) Poor Access Control
- (C) Shared Tenancy
- (D) Secure APIs

Question 67. You have been hired as a penetration tester for a company to locate and exploit vulnerabilities in its target's outward-facing services. You are not provided with any architecture diagrams or source code. This means that you are relying on dynamic analysis of currently running programs and systems within the target network. Which of the following pentesting assignments are you currently on?

- (A) Gray-Box Testing
- (B) White-Box Testing
- (C) Black-Box Testing
- (D) Open-Box Testing

Question 68. Which of the following terms refers to Information Technology (IT) applications and infrastructure that are managed and utilized without the knowledge of the enterprise's IT department?

- (A) Script Kiddies
- (B) Indicators of compromise
- (C) Shadow IT
- (D) Open-source intelligence

Question 69. Which of the following cybersecurity testing exercise team do not focus exclusively on attacking or defending, but they do both?

- (A) Red team
- (B) Blue team
- (C) White team
- (D) Purple team

Question 70. The technique of redirecting victims from a current page to a new URL which is usually a phishing page that impersonates a legitimate site and steals credentials from the victims is known as:

- (A)** URL redirection
- (B)** DNS spoofing
- (C)** Domain hijacking
- (D)** Domain redirection

Question 71. The type of hackers that are experts in compromising computer security systems and use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes is commonly known as:

- (A) White-Hat hackers
- (B) Black-Hat hackers
- (C) Red-Hat hackers
- (D) Gray-Hat hackers

Question 72. Which of the following features will you use to remotely clear your phones' data in the event of losing your phone?

- (A) Geofencing
- (B) Remote wipe
- (C) Geolocation
- (D) Push notifications

Question 73. You have been tasked to access a remote computer for handling some administrative tasks over an unsecured network in a secure way. Which of the following protocols will you use to access the remote computer to handle the administrative tasks?

- (A) SRTP
- (B) LDAPS
- (C) SSH
- (D) HTTPS

Question 74. As a security expert of your company you are responsible for preventing unauthorized (rogue) Dynamic Host Configuration Protocols servers offering IP addresses to the clients. Which of the following security technology will you implement to meet the requirement?

- (A) DHCP snooping
- (B) BPDU guard
- (C) MAC filtering
- (D) Jump server

Question 75. You have been hired as a security expert to implement a security solution to protect an organization from external threats. The solution should provide packet filtering, VPN support, network monitoring, and deeper inspection capabilities that give the organization a superior ability to identify attacks, malware, and other threats. Which of the following security solutions will you implement to meet the requirement?

- (A) Next-generation firewall (NGFW)
- (B) Endpoint detection and response (EDR)
- (C) Anti-malware
- (D) Antivirus

Question 76. One of the features of SNMPv3 is called message integrity.

- (A) TRUE
- (B) FALSE

Question 77. You have been tasked to implement a solution to increase the security of your company's local area network (LAN). All of the company's external-facing servers (Web server, Mail server, FTP server) should be placed in a separate area in order to be accessible from the internet, but the rest of the internal LAN to be unreachable. Which of the following techniques will you implement to meet the requirement?

- (A) DMZ
- (B) VLAN
- (C) VPN
- (D) DNS

Question 78. Application whitelisting prevents undesirable programs from executing, while application blacklisting is more restrictive and allows only programs that have been explicitly permitted to run.

- (A) TRUE
- (B) FALSE

Question 79. In which of the following load balancer mode, two or more servers aggregate the network traffic load and work as a team distributes it to the network servers?

- (A) Active/active
- (B) Active/passive
- (C) Passive/active
- (D) Passive/passive

Question 80. You have been tasked to implement a solution to send product offers to consumers' smartphones when they trigger a search in a particular geographic location, enter a mall, neighborhood, or store. What solution will you implement in order to achieve that?

- (A) Geolocation
- (B) Push notifications
- (C) Geofencing
- (D) Remote wipe

Question 81. The type of network hardware appliance that protects networks against security threats (malware, attacks) that simultaneously target separate parts of the network by integrating multiple security services and features is known as:

- (A) Network address translation (NAT)
- (B) Web application firewall (WAF)
- (C) Content/URL filter
- (D) Unified threat management (UTM)

Question 82. For security and monitoring purposes your company instructed you to implement a solution so that all packets entering or exiting a port should be copied and then should be sent to a local interface for monitoring. Which of the following solution will you implement in order to meet the requirement?

- (A) Access control list (ACL)
- (B) Port mirroring
- (C) Quality of service (QoS)
- (D) File Integrity Monitoring

Question 83. Your manager trying to understand the difference between SFTP and FTPS. So, he asked you to explain the difference between those. Which of the following statements are correct? (Choose all that apply.)

- (A) SFTP, also known as SSH FTP, encrypts both commands and data while in transmission
- (B) FTPS, also known as FTP Secure or FTP-SSL
- (C) SFTP protocol is packet-based as opposed to text-based making file and data transfers faster
- (D) FTPS authenticates your connection using a user ID and password or SSH Keys
- (E) SFTP authenticates your connection using a user ID and password, a certificate, or both

Question 84. The network administrator from your company notices that the network performance has been degraded due to a broadcast storm. Which of the following techniques will you recommend to the network administrator in order to reduce broadcast storms? (Choose all that apply)

- (A) Check for loops in switches
- (B) Split up your broadcast domain
- (C) Allow you to rate-limit broadcast packets
- (D) Check how often ARP tables are emptied
- (E) Split up your collision domain
- (F) Check the routing tables

Question 85. Which of the following technologies will you use in order to send instant notifications to your subscribed users each time you publish a new blog post on your website?

- (A) Push notifications
- (B) Geofencing
- (C) Geolocation
- (D) Remote wipe

Question 86. It has been noticed the Wi-Fi of your company is slow and sometimes not operational. After investigation, you noticed this caused by channel interference. Which of the following solutions will you implement to avoid problems such as channel interference when you build your WLAN?

- (A) Heat maps
- (B) WiFi Protected Setup
- (C) Captive portal
- (D) You can't avoid channel interference

Question 87. Which of the following options are cryptographic protocols? (Choose all that apply)

- (A) WPA2
- (B) WPA3
- (C) CCMP
- (D) SAE
- (E) EAP
- (F) PEAP

Question 87. Which of the following options are cryptographic protocols? (Choose all that apply)

- (A) WPA2
- (B) WPA3
- (C) CCMP
- (D) SAE
- (E) EAP
- (F) PEAP

Question 89. You have been tasked to implement a solution to encrypt data as it is written to the disk and decrypt data as it is read off the disk. Which of the following solution will you implement to meet the requirement?

- (A) Root of trust
- (B) Trusted Platform Module
- (C) Self-encrypting drive (SED) / full-disk encryption (FDE)
- (D) Sandboxing

Question 90. Which of the following VPN solutions is used to connect two local area networks (LANs) utilized by businesses large and small that want to provide their employees with secure access to network resources?

- (A) Remote access
- (B) Site-to-site
- (C) Split tunnel
- (D) Proxy server

Question 91. Which of the following options are authentication protocols? (Choose all that apply)

- (A) EAP
- (B) PEAP
- (C) WPA2
- (D) WPA3
- (E) RADIUS

Question 92. Which of the following types of certificates will you use to digitally sign your apps as a way for end-users to verify that the code they receive has not been altered or compromised by a third party?

- (A) Wildcard
- (B) Subject alternative name
- (C) Code signing certificates
- (D) Self-signed

Question 93. What technique is used for IP address conservation by making private IP addresses to connect to the Internet?

- (A) NAT
- (B) UTM
- (C) WAF
- (D) ACL

Question 94. Which of the following authentication protocols allows you to use an existing account to sign in to multiple websites, without needing to create new passwords?

- (A) OpenID
- (B) Kerberos
- (C) TACACS+
- (D) OAuth

Question 95. Assuming you have the domain yourcompany.

com with the following sub-domains:

www.yourcompany.com

mail.yourcompany.com

intranet.yourcompany.com

secure.yourcompany.com

me.yourcompany.com

Which of the following types of certificates will you choose to secure all the first-level sub-domains on a single domain name?

- (A) Subject alternative name
- (B) Code signing certificates
- (C) Wildcard
- (D) Self-signed

Question 96. A _____ certificate is a digital certificate that's not signed by a publicly trusted certificate authority (CA). These certificates are created, issued, and signed by the company or developer who is responsible for the website or software being signed.

- (A) Self-signed
- (B) Wildcard
- (C) Subject alternative name
- (D) Code signing certificates

Question 97. In the form of Rule-Based Access Control, data are accessible or not accessible based on the user's IP address.

- (A) TRUE
- (B) FALSE

Question 98. WiFi _____ Setup is a wireless network security standard that tries to make connections between a router and wireless devices faster, easier, and more secure.

- (A) Faster
- (B) Easier
- (C) Protected
- (D) Secured

Question 99. Which of the following Public key infrastructure (PKI) terms is known as an organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates?

- (A) Certificate authority (CA)
- (B) Registration authority (RA)
- (C) Online Certificate Status Protocol (OCSP)
- (D) Certificate signing request (CSR)

Question 100. You have been tasked to implement a security solution so all the network events from your company should be recorded in a central database for further analysis. Which of the following security solutions will you implement to meet the requirement?

- (A) Next-generation firewall (NGFW)
- (B) Endpoint detection and response (EDR)
- (C) Anti-malware
- (D) Antivirus

Question 101. Access _____ List is a network traffic filter that controls incoming or outgoing traffic. It works on a set of rules that define how to forward or block a packet at the router's interface.

- (A) Security
- (B) Filter
- (C) Control
- (D) Service

Question 102. Which of the following VPN solutions is used to connect a personal user device to a remote server on a private network?

- (A) Remote Access
- (B) Site-to-site
- (C) Split tunnel
- (D) Proxy server

Question 103. In the form of Role-Based Access Control, data are accessible or not accessible based on the user's IP address.

- (A) TRUE
- (B) FALSE

Question 104. In cloud computing, the ability to scale up and down resources based on the user's needs is known as:

- (A) Virtual private cloud
- (B) Network segmentation
- (C) Dynamic resource allocation
- (D) Public subnet

Question 105. _____ Assertions Markup Language is an important component of many SSO systems that allow users to access multiple applications, services, or websites from a single login process. It is used to share security credentials across one or more networked systems.

- (A) Security
- (B) Single
- (C) Sign
- (D) Service

Question 106. You have been tasked to configure the Wi-Fi of your company's LAN to allow certain computers to have access to the Internet and the rest computers need to be blocked.

Which of the following security technology will you implement to meet the requirement?

- (A) DHCP snooping
- (B) BPDU guard
- (C) MAC filtering
- (D) Jump server

RECAP

- **AAA of Security**
 - **Authentication**
 - When a person's identity is established with proof and confirmed by a system
 - Something you know
 - Something you are
 - Something you have
 - Something you do
 - Somewhere you are
 - **Authorization**
 - Occurs when a user is given access to a certain piece of data or certain areas of a building
 - **Accounting**
 - Tracking of data, computer usage, and network resources
 - Non-repudiation occurs when you have proof that someone has taken an action

- Security Threats
 - **Malware**
 - Short-hand term for malicious software
 - **Unauthorized Access**
 - Occurs when access to computer resources and data occurs without the consent of the owner
 - **System Failure**
 - Occurs when a computer crashes or an individual application fails
 - **Social Engineering**
 - Act of manipulating users into revealing confidential information or performing other detrimental actions

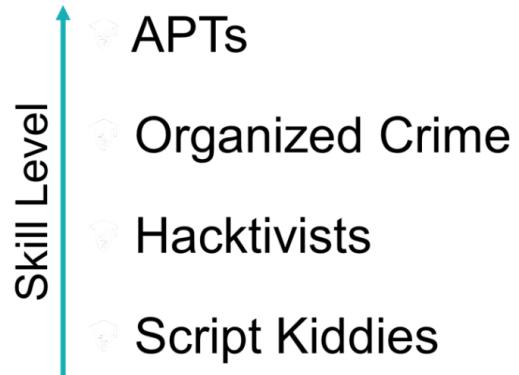
Mitigating Threats

- Physical Controls
 - Alarm systems, locks, surveillance cameras, identification cards, and security guards
- Technical Controls
 - Smart cards, encryption, access control lists (ACLs), intrusion detection systems, and network authentication
- Administrative Controls
 - Policies, procedures, security awareness training, contingency planning, and disaster recovery plans
 - User training is the most cost-effective security control to use

Hackers

- Five Types of Hackers
 - White Hats
 - Non-malicious hackers who attempt to break into a company's systems at their request
 - Black Hats
 - Malicious hackers who break into computer systems and networks without authorization or permission
 - Gray Hats
 - Hackers without any affiliation to a company who attempt to break into a company's network but risk the law by doing so
 - Blue Hats
 - Hackers who attempt to hack into a network with permission of the company but are not employed by the company
 - Elite
 - Hackers who find and exploit vulnerabilities before anyone else does
 - 1 in 10,000 are elite

- **Threat Actors**
 - **Script Kiddies**
 - Hackers with little to no skill who only use the tools and exploits written by others
 - **Hacktivists**
 - Hackers who are driven by a cause like social change, political agendas, or terrorism
 - **Organized Crime**
 - Hackers who are part of a crime group that is well-funded and highly sophisticated
 - **Advanced Persistent Threats**
 - Highly trained and funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal



Threat Intelligence and Sources

- Measuring quality of intelligence
 - Timeliness
 - Property of an intelligence source that ensures it is up-to-date
 - Relevancy
 - Property of an intelligence source that ensures it matches the use cases intended for it
 - Accuracy
 - Property of an intelligence source that ensures it produces effective results
 - Confidence Levels
 - Property of an intelligence source that ensures it produces qualified statements about reliability

- Types of intelligence
 - Proprietary
 - Threat intelligence is very widely provided as a commercial service offering, where access to updates and research is subject to a subscription fee
 - Closed-Source
 - Data that is derived from the provider's own research and analysis efforts, such as data from honeynets that they operate, plus information mined from its customers' systems, suitably anonymized
 - Open-Source
 - Data that is available to use without subscription, which may include threat feeds similar to the commercial providers and may contain reputation lists and malware signature databases
 - US-CERT
 - UK's NCSC
 - AT&T Security (OTX)
 - MISP
 - VirusTotal
 - Spamhaus
 - SANS ISC Suspicious Domains
 - Open-Source Intelligence (OSINT)
 - Methods of obtaining information about a person or organization through public records, websites, and social media

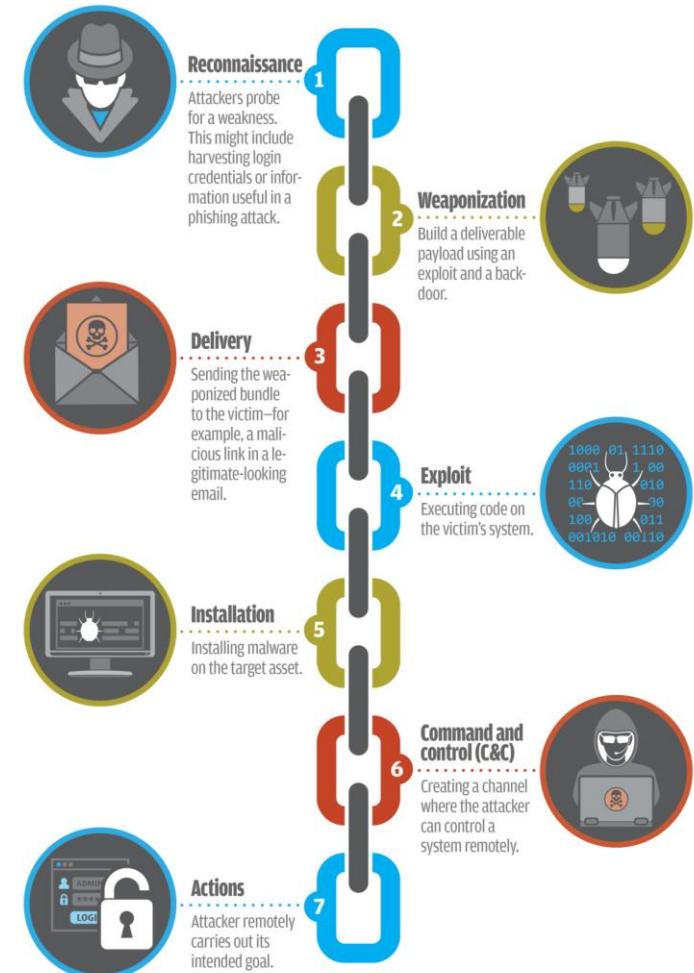
- Threat Hunting
 - A cyber security technique designed to detect presence of threat that have not been discovered by a normal security monitoring
 - Threat Hunting is potentially less disruptive than penetration testing
- Establishing a hypothesis
 - A hypothesis is derived from the threat modeling and is based on potential events with higher likelihood and higher impact.
- Profiling Threat Actors and Activities
 - Involves the creation of scenario that show how a prospective attacker might attempt an intrusion and what their objectives might be
- Threat hunting relies on the usage of the tools developed for regular security monitoring and incident response
 - Analyze network traffic
 - Analyze the executable process list
 - Analyze other infected host
 - Identify how the malicious process was executed
- Threat hunting consumes a lot of resources and time to conduct, but can yield a lot of benefits
 - Improve detection capabilities
 - Integrate intelligence
 - Reduce attack surface
 - Block attack vectors
 - Identify critical assets

Attack Frameworks

- Kill Chain
 - A model developed by Lockheed Martin that describes the stages by which a threat actor progresses a network intrusion
 - Reconnaissance
 - The attacker determines what methods to use to complete the phases of the attack
 - Weaponization
 - The attacker couples payload code that will enable access with exploit code that will use a vulnerability to execute on the target system
 - Delivery
 - The attacker identifies a vector by which to transmit the weaponized code to the target environment
 - Exploitation
 - The weaponized code is executed on the target system by this mechanism
 - Installation
 - This mechanism enables the weaponized code to run a remote access tool and achieve persistence on the target system
 - Command & Control (C2)
 - The weaponized code establishes an outbound channel to a remote server that can then be used to control the remote access tool and possibly download additional tools to progress the attack
 - Actions on Objectives
 - The attacker typically uses the access he has achieved to covertly collect information from target systems and transfer it to a remote system (data exfiltration) or achieve other goals and motives
 - Kill chain analysis can be used to identify a defensive course-of-action matrix to counter the progress of an attack at each stage

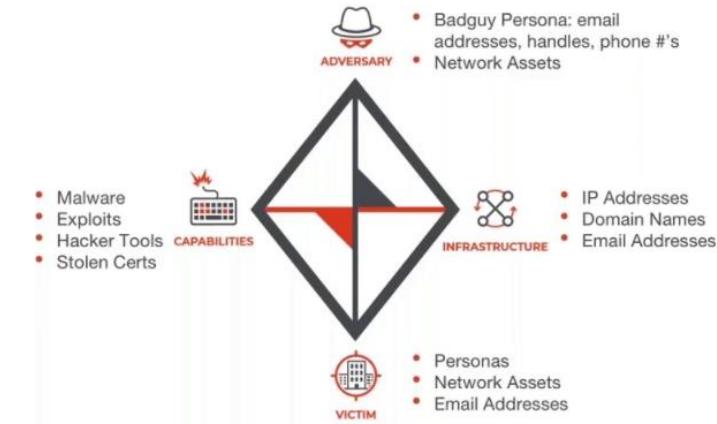
What is the CYBER KILL CHAIN?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.



SOURCE: LOCKHEED MARTIN

- MITRE ATT&CK Framework
 - A knowledge base maintained by the MITRE Corporation for listing and explaining specific adversary tactics, techniques, and common knowledge or procedures (attack.mitre.org)
 - The pre-ATT&CK tactics matrix aligns to the reconnaissance and weaponization phases of the kill chain
- Diamond Model of Intrusion Analysis
 - A framework for analyzing cybersecurity incidents and intrusions by exploring the relationships between four core features: adversary, capability, infrastructure, and victim



- **Malware**

- Software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent
 - Viruses
 - Worms
 - Trojan horses
 - Ransomware
 - Spyware
 - Rootkits
 - Spam

- **Viruses**

- Malicious code that runs on a machine without the user's knowledge and infects the computer when executed
- Viruses require a user action in order to reproduce and spread
 - Boot sector
 - Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up
 - Macro
 - Virus embedded into a document and is executed when the document is opened by the user
 - Program
 - Program viruses infect an executable or application
 - Multipartite
 - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
 - Encrypted
 - Polymorphic
 - Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection
 - Metamorphic
 - Virus that is able to rewrite itself entirely before it attempts to infect a file (advanced version of polymorphic virus)
 - Stealth
 - Armored
 - Armored viruses have a layer of protection to confuse a program or person analyzing it
 - Hoax

- **Trojans**
 - **Trojan Horse**
 - Malicious software that is disguised as a piece of harmless or desirable software
 - Trojans perform desired functions and malicious functions
 - **Remote Access Trojan (RAT)**
 - Provides the attacker with remote control of a victim computer and is the most commonly used type of Trojan
- **Ransomware**
 - Malware that restricts access to a victim's computer system until a ransom is received
 - Ransomware uses a vulnerability in your software to gain access and then encrypts your files
 - Example, in 2017 the SamSam cost the City of Atlanta over \$17 million
- **Spyware**
 - Malware that secretly gathers information about the user without their consent
 - Captures keystrokes made by the victim and takes screenshots that are sent to the attacker

- **Adware**
 - Displays advertisements based upon its spying on you
- **Grayware**
 - Software that isn't benign nor malicious and tends to behave improperly without serious consequences
- **Rootkits**
 - **Rootkit**
 - Software designed to gain administrative level control over a system without detection
 - DLL injection is commonly used by rootkits to maintain their persistent control
 - **DLL Injection**
 - Malicious code is inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime
 - **Driver Manipulation**
 - An attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level
 - A shim is placed between two components to intercept calls and redirect them
 - **Rootkits are activated before booting the operating system and are difficult to detect**
- **Spam**
 - Activity that abuses electronic messaging systems, most commonly through email
 - Spammers often exploit a company's open mail relays to send their messages
 - CAN-SPAM Act of 2003

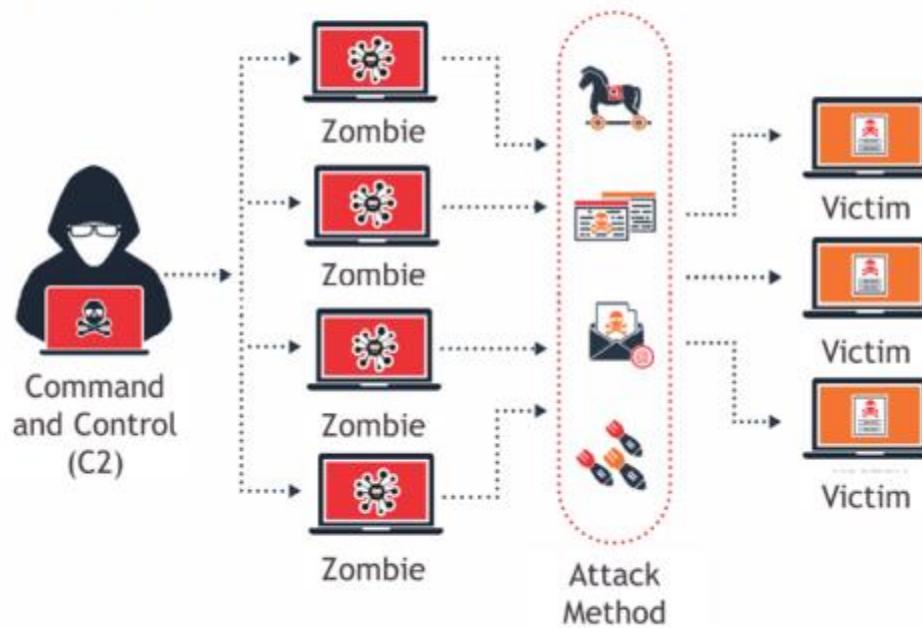
Malware Infections

- **Malware Infection**
 - **Threat Vector**
 - Method used by an attacker to access a victim's machine
 - **Attack Vector**
 - Method used by an attacker to gain access to a victim's machine in order to infect it with malware
- **Common Delivery Methods**
 - Malware infections usually start within software, messaging, and media
 - **Watering Holes**
 - Malware is placed on a website that you know your potential victims will access

- **Botnets and Zombies**

- **Botnet**

- A collection of compromised computers under the control of a master node



- **Active Interception & Privilege Escalation**
 - **Active Interception**
 - Occurs when a computer is placed between the sender and receiver and is able to capture or modify the traffic between them



- **Privilege Escalation**
 - Occurs when you are able to exploit a design flaw or bug in a system to gain access to resources that a normal user isn't able to access

- **Backdoors and Logic Bombs**
 - Backdoors are used to bypass normal security and authentication functions
 - Remote Access Trojan (RAT) is placed by an attacker to maintain persistent access
 - **Logic Bomb**
 - Malicious code that has been inserted inside a program and will execute only when certain conditions have been met
 - **Easter Egg**
 - Non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature
 - Logic bombs and Easter eggs should not be used according to secure coding standards

- **Symptoms of Infection**
 - **Your computer might have been infected if it begins to act strangely**
 - Hard drives, files, or applications are not accessible anymore
 - Strange noises occur
 - Unusual error messages
 - Display looks strange
 - Jumbled printouts
 - Double file extensions are being displayed, such as textfile.txt.exe
 - New files and folders have been created or files and folders are missing/corrupted
 - System Restore will not function
- **Removing Malware**
 - Identify symptoms of a malware infection
 - Quarantine the infected systems
 - Disable System Restore (if using a Windows machine)
 - Remediate the infected system
 - Schedule automatic updates and scans
 - Enable System Restore and create a new restore point
 - Provide end user security awareness training
 - If a boot sector virus is suspected, reboot the computer from an external device and scan it

Malware Exploitation

- Exploit Technique
 - Describes the specific method by which malware code infects a target host
 - Most modern malware uses fileless techniques to avoid detection by signature-based security software
 - How does an APT use modern malware to operate?
 - Dropper or downloader
 - Maintain access
 - Strengthen access
 - Actions on objectives
 - Concealment
- Dropper
 - Malware designed to install or run other types of malware embedded in a payload on an infected host
- Downloader
 - A piece of code that connects to the Internet to retrieve additional tools after the initial infection by a dropper
- Shellcode
 - Any lightweight code designed to run an exploit on the target, which may include any type of code format from scripting languages to binary code
- Living Off the Land
 - Exploit techniques that use standard system tools and packages to perform intrusions
 - Detection of an adversary is more difficult when they are executing malware code within standard tools and processes

Security Applications and Devices

- Software Firewalls

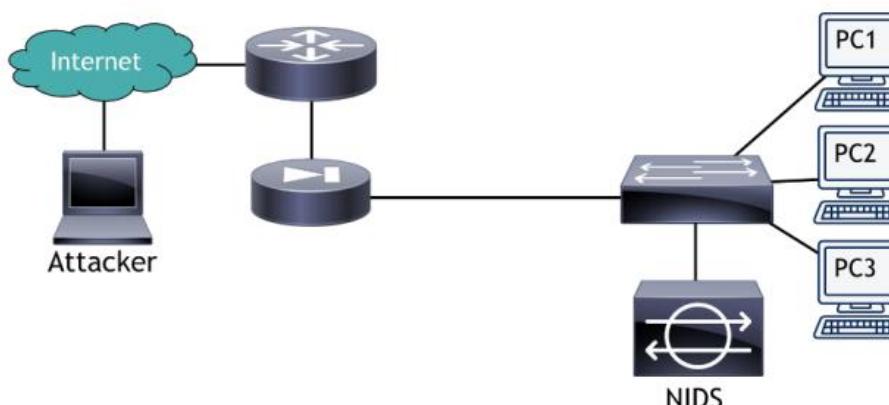
- Personal Firewalls

- Software application that protects a single computer from unwanted Internet traffic
 - Host-based firewalls
 - Windows Firewall (Windows)
 - PF and IPFW (OS X)
 - iptables (Linux)

- Many anti-malware suites also contain software firewalls

- Intrusion Detection System

- Device or software application that monitors a system or network and analyzes the data passing through it in order to identify an incident or attack
 - HIDS
 - Host-based IDS
 - NIDS
 - Network-based IDS



- **Signature, Policy, and Anomaly-based detection methods**
 - Signature-based
 - A specific string of bytes triggers an alert
 - Policy-based
 - Relies on specific declaration of the security policy (i.e., 'No Telnet Authorized')
 - Anomaly-based
 - Analyzes the current traffic against an established baseline and triggers an alert if outside the statistical average
- **Types of Alerts**
 - True positive
 - Malicious activity is identified as an attack
 - False positive
 - Legitimate activity is identified as an attack
 - True negative
 - Legitimate activity is identified as legitimate traffic
 - False negative
 - Malicious activity is identified as legitimate traffic
- IDS can only alert and log suspicious activity...
- IPS can also stop malicious activity from being executed
- HIDS logs are used to recreate the events after an attack has occurred

- **Pop-up Blockers**
 - Most web-browsers have the ability to block JavaScript created pop-ups
 - Users may enable pop-ups because they are required for a website to function
 - Malicious attackers could purchase ads (pay per click) through various networks
 - **Content Filters**
 - Blocking of external files containing JavaScript, images, or web pages from loading in a browser
 - Ensure your browser and its extensions are updated regularly
- **Data Loss Prevention (DLP)**
 - Monitors the data of a system while in use, in transit, or at rest to detect attempts to steal the data
 - Software or hardware solutions
 - Endpoint DLP System
 - Software-based client that monitors the data in use on a computer and can stop a file transfer or alert an admin of the occurrence
 - Network DLP System
 - Software or hardware-based solution that is installed on the perimeter of the network to detect data in transit
 - Storage DLP System
 - Software installed on servers in the datacenter to inspect the data at rest
 - Cloud DLP System
 - Cloud software as a service that protects data being stored in cloud services

- **Securing the BIOS**
 - **Basic Input Output System**
 - Firmware that provides the computer instructions for how to accept input and send output
 - Unified Extensible Firmware Interface (UEFI)
 - BIOS and UEFI are used interchangeable in this lesson
 - **1. Flash the BIOS**
 - **2. Use a BIOS password**
 - **3. Configure the BIOS boot order**
 - **4. Disable the external ports and devices**
 - **5. Enable the secure boot option**

- **Securing Storage Devices**
 - **Removable media comes in many different formats**
 - You should always encrypt files on removable media
 - **Removable media controls**
 - Technical limitations placed on a system in regards to the utilization of USB storage devices and other removable media
 - Create administrative controls such as policies
 - **Network Attached Storage (NAS)**
 - Storage devices that connect directly to your organization's network
 - NAS systems often implement RAID arrays to ensure high availability
 - **Storage Area Network (SAN)**
 - Network designed specifically to perform block storage functions that may consist of NAS devices
 - 1. Use data encryption
 - 2. Use proper authentication
 - 3. Log NAS access

- **Disk Encryption**
 - Encryption scrambles data into unreadable information
 - Self-Encrypting Drive (SED)
 - Storage device that performs whole disk encryption by using embedded hardware
 - **Encryption software is most commonly used**
 - FileVault
 - BitLocker
 - **Trusted Platform Module (TPM)**
 - Chip residing on the motherboard that contains an encryption key
 - If your motherboard doesn't have TPM, you can use an external USB drive as a key
 - **Advanced Encryption Standard**
 - Symmetric key encryption that supports 128-bit and 256-bit keys
 - **Encryption adds security but has lower performance**
 - **Hardware Security Module (HSM)**
 - Physical devices that act as a secure cryptoprocessor during the encryption process

- **Endpoint analysis**
 - **Anti-virus (AV)**
 - Software capable of detecting and removing virus infections and (in most cases) other types of malware, such as worms, Trojans, rootkits, adware, spyware, password crackers, network mappers, DoS tools, and others
 - **Host-based IDS/IPS (HIDS/HIPS)**
 - A type of IDS or IPS that monitors a computer system for unexpected behavior or drastic changes to the system's state on an endpoint
 - **Endpoint Protection Platform (EPP)**
 - A software agent and monitoring system that performs multiple security tasks such as anti-virus, HIDS/HIPS, firewall, DLP, and file encryption
 - **Endpoint Detection and Response (EDR)**
 - A software agent that collects system data and logs for analysis by a monitoring system to provide early detection of threats
 - **User and Entity Behavior Analytics (UEBA)**
 - A system that can provide automated identification of suspicious activity by user accounts and computer hosts
 - UEBA solutions are heavily dependent on advanced computing techniques like artificial intelligence (AI) and machine learning
 - Many companies are now marketing advanced threat protection (ATP), advanced endpoint protection (AEP), and NextGen AV (NGAV) which is a hybrid of EPP, EDR, and UEBA

Mobile Device Security

- **Securing Wireless Devices**
 - WiFi Protected Access 2 (WPA2) is the highest level of wireless security
 - AES
 - Advanced Encryption Standard
 - Bluetooth pairing creates a shared link key to encrypt the connection
 - Wired devices are almost always more secure than wireless ones
- **Mobile Malware**
 - Ensure your mobile device is patched and updated
 - Only install apps from the official App Store or Play Store
 - Do not jailbreak/root device
 - Don't use custom firmware or a custom ROM
 - Only load official store apps
 - Always update your phone's operating system
- **SIM Cloning & ID Theft**
 - **Subscriber Identity Module (SIM)**
 - Integrated circuit that securely stores the international mobile subscriber identity (IMSI) number and its related key
 - **SIM Cloning**
 - Allows two phones to utilize the same service and allows an attacker to gain access to the phone's data
 - SIM v1 cards were easy to clone but newer SIM v2 cards are much harder
 - Be careful with where you post phone numbers

- **Bluetooth Attacks**
 - **Bluejacking**
 - Sending of unsolicited messages to Bluetooth-enabled devices
 - **Bluesnarfing**
 - Unauthorized access of information from a wireless device over a Bluetooth connection
 - Bluejacking sends information to a device
 - Bluesnarfing takes information from a device

- **Mobile Device Theft**
 - Always ensure your device is backed up
 - Don't try to recover your device alone if it is stolen
 - **Remote Lock**
 - Requires a PIN or password before someone can use the device
 - **Remote Wipe**
 - Remotely erases the contents of the device to ensure the information is not recovered by the thief
- **Security of Apps**
 - Only install apps from the official mobile stores
 - **TLS**
 - Transport Layer Security
 - **Mobile Device Management**
 - Centralized software solution that allows system administrators to create and enforce policies across its mobile devices
 - Turn location services off to ensure privacy
 - **Geotagging**
 - Embedding of the geolocation coordinates into a piece of data (i.e., a photo)
 - Geotagging should be considered when developing your organization's security policies

- **Bring Your Own Device**
 - BYOD introduces a lot of security issues to consider
 - **Storage Segmentation**
 - Creating a clear separation between personal and company data on a single device
 - **Mobile Device Management**
 - Centralized software solution for remote administration and configuration of mobile devices
 - **CYOD**
 - Choose Your Own Device
 - MDM can prevent certain applications from being installed on the device
 - Ensure your organization has a good security policy for mobile devices

- **Hardening Mobile Devices**
 - 1. Update your device to the latest version of the software
 - 2. Install AntiVirus
 - 3. Train users on proper security and use of the device
 - 4. Only install apps from the official mobile stores
 - 5. Do not root or jailbreak your devices
 - 6. Only use v2 SIM cards with your devices
 - 7. Turn off all unnecessary features
 - 8. Turn on encryption for voice and data
 - 9. Use strong passwords or biometrics
 - 10. Don't allow BYOD
 - Ensure your organization has a good security policy for mobile devices

Hardening

- **Hardening**
 - Act of configuring an operating system securely by updating it, creating rules and policies to govern it, and removing unnecessary applications and services
 - We are not guaranteed security, but we can minimize the risk...
 - Mitigate risk by minimizing vulnerabilities to reduce exposure to threats
- **Unnecessary Applications**
 - **Least Functionality**
 - Process of configuring workstation or server to only provide essential applications and services
 - Personal computers often accumulate unnecessary programs over time
 - Utilize a secure baseline image when adding new computers
 - **SCCM**
 - Microsoft's System Center Configuration Management
- **Restricting Applications**
 - **Application Whitelist**
 - Only applications that are on the list are allowed to be run by the operating system while all other applications are blocked
 - **Application Blacklist**
 - Any application placed on the list will be prevented from running while all others will be permitted to run
 - **Whitelisting and blacklisting can be centrally managed**
- **Unnecessary Services**
 - Any services that are unneeded should be disabled in the OS
- **Trusted Operating Systems (TOS)**
 - An operating system that meets the requirements set forth by government and has multilevel security
 - Windows 7 (and newer)
 - Mac OS X 10.6 (and newer)
 - FreeBSD (TrustedBSD)
 - Red Hat Enterprise Server

- **Updates and Patches**
 - **Patches**
 - A single problem-fixing piece of software for an operating system or application
 - **Hotfix**
 - A single problem-fixing piece of software for an operating system or application
 - Patches and Hotfixes are now used interchangeably by most manufacturers
- **Categories of Updates**
 - Security Update
 - Software code that is issued for a product-specific security-related vulnerability
 - Critical Update
 - Software code for a specific problem addressing a critical, non-security bug in the software
 - Service Pack
 - A tested, cumulative grouping of patches, hotfixes, security updates, critical updates, and possibly some feature or design changes
 - Windows Update
 - Recommended update to fix a noncritical problem that users have found, as well as to provide additional features or capabilities
 - Driver Update
 - Updated device driver to fix a security issue or add a feature to a supported piece of hardware
 - Windows 10 uses the Windows Update program (wuapp.exe) to manage updates

- **Patch Management**
 - Process of planning, testing, implementing, and auditing of software patches
 - Planning
 - Testing
 - Implementing
 - Auditing
 - Verify it is compatible with your systems and plan for how you will test and deploy it
 - Always test a patch prior to automating its deployment
 - Manually or automatically deploy the patch to all your clients to implement it
 - Large organizations centrally manage updates through an update server
 - Disable the wuauserv service to prevent Windows Update from running automatically
 - It is important to audit the client's status after patch deployment
 - Linux and OSX also have built-in patch management systems

- **Group Policies**
 - **Group Policy**
 - A set of rules or policies that can be applied to a set of users or computer accounts within the operating system
 - Access the Group Policy Editor by opening the Run prompt and enter `gpedit`
 - Password complexity
 - Account lockout policy
 - Software restrictions
 - Application restrictions
 - Active Directory domain controllers have a more advanced Group Policy Editor
 - **Security Template**
 - A group of policies that can be loaded through one procedure
 - Group Policy objectives (GPOs) aid in the hardening of the operating system
 - **Baselining**
 - Process of measuring changes in the network, hardware, and software environment
 - A baseline establishes what is normal so you can find deviations

- **File Systems and Hard Drives**
 - Level of security of a system is affected by its file system type
 - NTFS
 - FAT32
 - ext4
 - HFS+
 - APFS
 - Windows systems can utilize NTFS or FAT32
 - NTFS
 - New Technology File System is the default file system format for Windows and is more secure because it supports logging, encryption, larger partition sizes, and larger file sizes than FAT32
 - Linux systems should use ext4 and OSX should use the APFS
 - **All hard drives will eventually fail**
 - 1. Remove temporary files by using Disk Cleanup
 - 2. Periodic system file checks
 - 3. Defragment your disk drive
 - 4. Back up your data
 - 5. Use and practice restoration techniques

Supply Chain Assessment

- Secure working in an unsecure environment involves mitigating the risks of the supply chain
- An organization must ensure that the operation of every element (hardware, firmware, driver, OS, and application) is consistent and tamper resistant to establish a trusted computing environment
 - **Due Diligence**
 - A legal principle identifying a subject has used best practice or reasonable care when setting up, configuring, and maintaining a system
 - Properly resourced cybersecurity program
 - Security assurance and risk management processes
 - Product support life cycle
 - Security controls for confidential data
 - Incident response and forensics assistance
 - General and historical company information
 - Due diligence should apply to all suppliers and contractors
 - **Trusted Foundry**
 - A microprocessor manufacturing utility that is part of a validated supply chain (one where hardware and software does not deviate from its documented function)
 - Trusted Foundry Program is operated by the Department of Defense (DoD)
 - **Hardware Source Authenticity**
 - The process of ensuring that hardware is procured tamper-free from trustworthy suppliers
 - Greater risk of inadvertently obtaining counterfeited or compromised devices when purchasing from second-hand or aftermarket sources

- **Hardware Root of Trust (ROT)**
 - A cryptographic module embedded within a computer system that can endorse trusted execution and attest to boot settings and metrics
 - A hardware root of trust is used to scan the boot metrics and OS files to verify their signatures, which we can then use to sign a digital report
- **Trusted Platform Module (TPM)**
 - A specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information
 - A TPM can be managed in Windows via the tpm.msc console or through group policy
- **Hardware Security Module (HSM)**
 - An appliance for generating and storing cryptographic keys that is less susceptible to tampering and insider threats than software-based storage
- **Anti-Tamper**
 - Methods that make it difficult for an attacker to alter the authorized execution of software
 - Anti-tamper mechanisms include a field programmable gate array (FPGA) and a physically unclonable function (PUF)

- **Trusted Firmware**

- A firmware exploit gives an attacker an opportunity to run any code at the highest level of CPU privilege

- **Unified Extensible Firmware Interface (UEFI)**

- A type of system firmware providing support for 64-bit CPU operation at boot, full GUI and mouse operation at boot, and better boot security

- **Secure Boot**

- A UEFI feature that prevents unwanted processes from executing during the boot operation

- **Measured Boot**

- A UEFI feature that gathers secure metrics to validate the boot process in an attestation report

- **Attestation**

- A claim that the data presented in the report is valid by digitally signing it using the TPM's private key

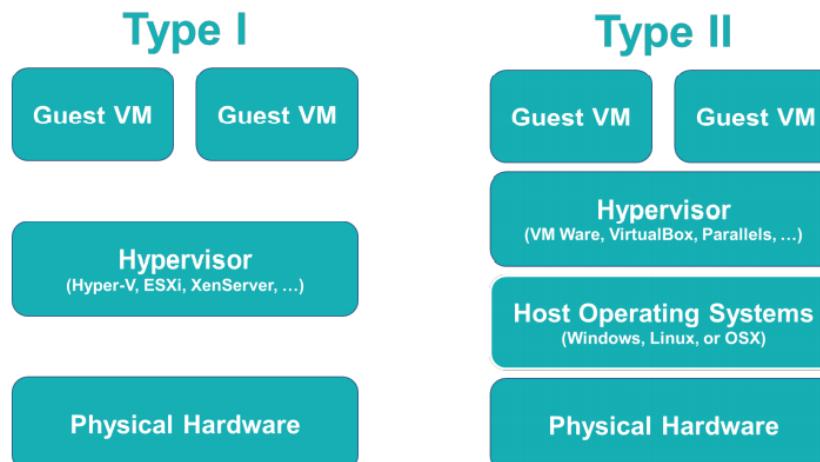
- **eFUSE**

- A means for software or firmware to permanently alter the state of a transistor on a computer chip

- **Secure Processing**
 - A mechanism for ensuring the confidentiality, integrity, and availability of software code and data as it is executed in volatile memory
- **Processor Security Extensions**
 - Low-level CPU changes and instructions that enable secure processing
 - AMD
 - Secure Memory Encryption (SME)
 - Secure Encrypted Virtualization (SEV)
 - Intel
 - Trusted Execution Technology (TXT)
 - Software Guard Extensions (SGX)
- **Trusted Execution**
 - The CPU's security extensions invoke a TPM and secure boot attestation to ensure that a trusted operating system is running
- **Secure Enclave**
 - The extensions allow a trusted process to create an encrypted container for sensitive data
- **Atomic Execution**
 - Certain operations that should only be performed once or not at all, such as initializing a memory location
- **Bus Encryption**
 - Data is encrypted by an application prior to being placed on the data bus
 - Ensures that the device at the end of the bus is trusted to decrypt the data

Virtualization

- **Virtualization** (Creation of a virtual resource)
 - A virtual machine is a container for an emulated computer that runs an entire operating system
 - **VM Types**
 - System Virtual Machine
 - Complete platform designed to replace an entire physical computer and includes a full desktop/server operating system
 - Processor Virtual Machine
 - Designed to only run a single process or application like a virtualized web browser or a simple web server
 - Virtualization continues to rise in order to reduce the physical requirements for data centers
- **Hypervisors**
 - Manages the distribution of the physical resources of a host machine (server) to the virtual machines being run (guests)



- Type I (bare metal) hypervisors are more efficient than Type II

- **Container-based**
 - Application Containerization
 - A single operating system kernel is shared across multiple virtual machines but each virtual machine receives its own user space for programs and data
 - Containerization allows for rapid and efficient deployment of distributed applications
 - Docker
 - Parallels Virtuozzo
 - OpenVZ
- **Threats to VMs**
 - VMs are separated from other VMs by default
 - **VM Escape**
 - An attack that allows an attacker to break out of a normally isolated VM by interacting directly with the hypervisor
 - Elasticity allows for scaling up or down to meet user demands
 - **Data Remnants**
 - Contents of a virtual machine that exist as deleted files on a cloud-based server after deprovisioning of a virtual machine
 - **Privilege Elevation**
 - Occurs when a user is able to grant themselves the ability to run functions as a higher-level user
 - Live migration occurs when a VM is moved from one physical server to another over the network

- **Securing VMs**
 - Uses many of the same security measures as a physical server
 - Limit connectivity between the virtual machine and the host
 - Remove any unnecessary pieces of virtual hardware from the virtual machine
 - Using proper patch management is important to keeping your guest's operating system secure
 - **Virtualization Sprawl**
 - Occurs when virtual machines are created, used, and deployed without proper management or oversight by the system admins

Application Security

- **Application Security**
- **Web Browser Security**
 - Ensure your web browser is up-to-date with patches...
 - ...but don't adopt the newest browser immediately
 - Which web browser should I use?
 - **General Security for Web Browsers**
 - 1. Implement Policies
 - Create and implement web browsing policies as an administrative control or technical control
 - 2. Train Your Users
 - User training will prevent many issues inside your organization
 - 3. Use Proxy & Content Filter
 - Proxies cache the website to reduce requests and bandwidth usage
 - Content filters can be used to blacklist specific websites or entire categories of sites
 - 4. Prevent Malicious Code
 - Configure your browsers to prevent ActiveX controls, Java applets, JavaScript, Flash, and other active content

- **Web Browser Concerns**
 - **Cookies**
 - Text files placed on a client's computer to store information about the user's browsing habits, credentials, and other data
 - **Locally Shared Object (LSO)**
 - Also known as Flash cookies, they are stored in your Windows user profile under the Flash folder inside of your AppData folder
 - **Add-Ons**
 - Smaller browser extensions and plugins that provide additional functionality to the browser
 - **Advanced Security Options**
 - Browser configuration and settings for numerous options such as SSL/TLS settings, local storage/cache size, browsing history, and much more

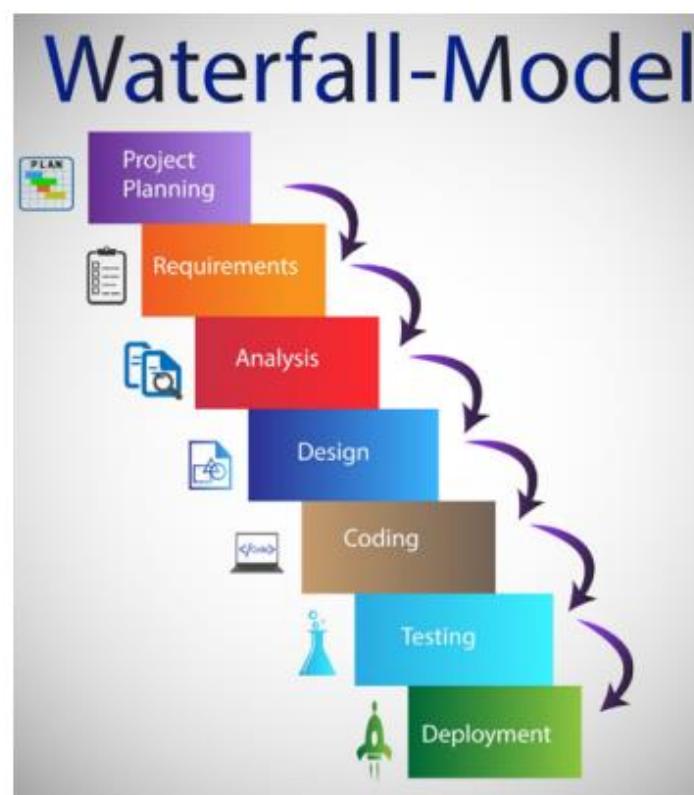
- **Securing Applications**
 - Use passwords to protect the contents of your documents
 - Digital signatures and digital certificates are used by MS Outlook for email security
 - **User Account Control**
 - Prevents unauthorized access and avoid user error in the form of accidental changes

Secure Software Development

- Software Development

- SDLC

- Software Development Life Cycle
 - SDLC is an organized process of developing a secure application throughout the life of the project



SDLC Phases

- 💡 Planning and Analysis
- 💡 Software/Systems Design
- 💡 Implementation
- 💡 Testing
- 💡 Integration
- 💡 Deployment
- 💡 Maintenance



- **Agile**
 - Software development is performed in time-boxed or small increments to allow more adaptivity to change
- **DevOps**
 - Software development and information technology operations
- **SDLC Principles**
 - Developers should always remember confidentiality, integrity, and availability
 - Confidentiality
 - Ensures that only authorized users can access the data
 - Integrity
 - Ensures that the data is not modified or altered without permission
 - Availability
 - Ensuring that data is available to authorized users when it is needed
 - Threat modeling helps prioritize vulnerability identification and patching

- **Least Privilege**
 - Users and processes should be run using the least amount of access necessary to perform a given function
- **Defense in Depth**
 - Layering of security controls is more effective and secure than relying on a single control
- **Never Trust User Input**
 - Any input that is received from a user should undergo input validation prior to allowing it to be utilized by an application
- **Minimize Attack Surface**
 - Reduce the amount of code used by a program, eliminate unneeded functionality, and require authentication prior to running additional plugins
- **Create Secure Defaults**
 - Default installations should include secure configurations instead of requiring an administrator or user to add in additional security

- **Authenticity and Integrity**
 - Applications should be deployed using code signing to ensure the program is not changed inadvertently or maliciously prior to delivery to an end user
- **Fail Securely**
 - Applications should be coded to properly conduct error handling for exceptions in order to fail securely instead of crashing
- **Fix Security Issues**
 - If a vulnerability is identified then it should be quickly and correctly patched to remove the vulnerability
- **Rely on Trusted SDKs**
 - SDKs must come from trusted source to ensure no malicious code is being added

- **Testing Methods**
 - **System Testing**
 - Black-box Testing
 - Occurs when a tester is not provided with any information about the system or program prior to conducting the test
 - White-box Testing
 - Occurs when a tester is provided full details of a system including the source code, diagrams, and user credentials in order to conduct the test



- **Structured Exception Handling (SEH)**
 - Provides control over what the application should do when faced with a runtime or syntax error
- **Programs should use input validation when taking data from users**
 - Input Validation
 - Applications verify that information received from a user matches a specific format or range of values
 - Example

```
get $ssn

if ($ssn >=000-00-0000 and
$ssn <= 999-99-9999)

then [do function]

else [conduct error handling]
```
- **Static Analysis**
 - Source code of an application is reviewed manually or with automatic tools without running the code
- **Dynamic Analysis**
 - Analysis and testing of a program occurs while it is being executed or run
- **Fuzzing**
 - Injection of randomized data into a software program in an attempt to find system failures, memory leaks, error handling issues, and improper input validation

- **Software Vulnerabilities and Exploits**
 - **Backdoors**
 - Code placed in computer programs to bypass normal authentication and other security mechanisms
 - Backdoors are a poor coding practice and should not be utilized
 - **Directory Traversal**
 - Method of accessing unauthorized directories by moving through the directory structure on a remote server
 - **Arbitrary Code Execution**
 - Occurs when an attacker is able to execute or run commands on a victim computer
 - **Remote Code Execution (RCE)**
 - Occurs when an attacker is able to execute or run commands on a remote computer
 - **Zero Day**
 - Attack against a vulnerability that is unknown to the original developer or manufacturer

- **Buffer Overflows**
 - **Buffer Overflow**
 - Occurs when a process stores data outside the memory range allocated by the developer
 - **Buffer**
 - A temporary storage area that a program uses to store data
 - Over 85% of data breaches were caused by a buffer overflow
 - **Example**

555-1234

Example of an 8-digit Buffer (A)							
0	1	2	3	4	5	6	7

Example of an 8-digit Buffer (A)

0 1 2 3 4 5 6 7

555-1234

What happens if we try to enter a number that is too long?

Phone Number

410-555-1234

Example of an 8-digit Buffer (A)							
0	1	2	3	4	5	6	7

Example of an 8-digit Buffer (A)

0 1 2 3 4 5 6 7

Example of an 8-digit Buffer (B)							
0	1	2	3	4	5	6	7

Example of an 8-digit Buffer (B)

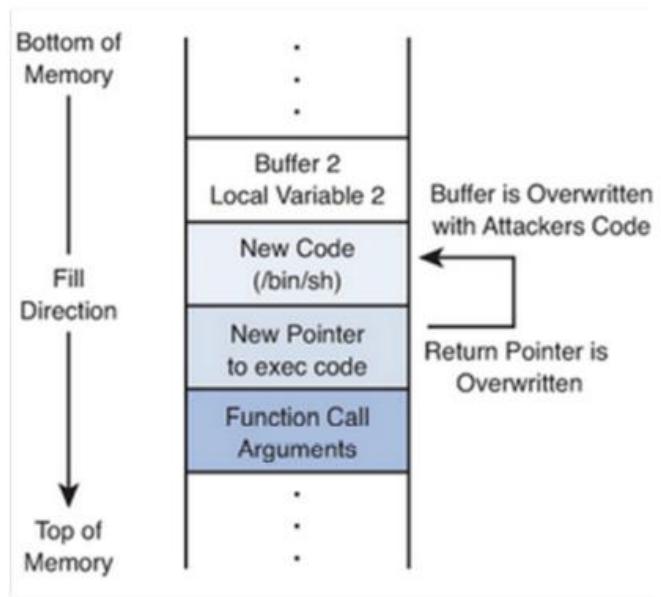
0 1 2 3 4 5 6 7

410-555-1234

- Let's get technical...

- Stack

- Reserved area of memory where the program saves the return address when a function call instruction is received



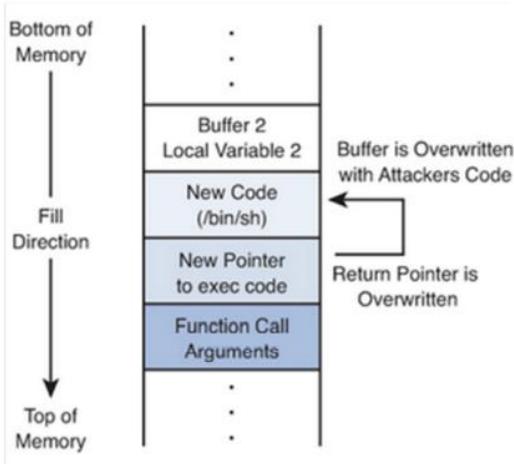
- “Smash the Stack”

- Occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attacker’s code to run

- Let's get technical...

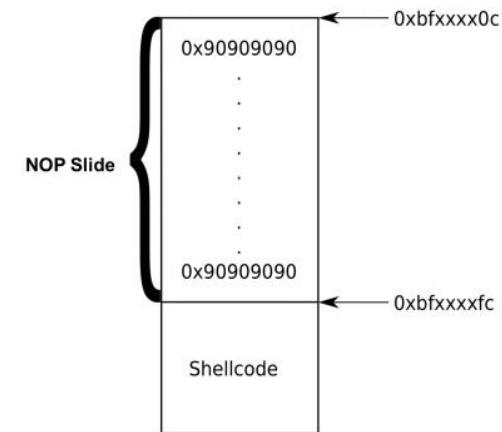
- Stack

- Reserved area of memory where the program saves the return address when a function call instruction is received



- "Smash the Stack"

- Occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attacker's code to run



- Address Space Layout Randomization

- Method used by programmers to randomly arrange the different address spaces used by a program or process to prevent buffer overflow exploits

- *Buffer overflows attempt to put more data into memory than it is designed to hold*

- **Cross-Site Scripting (XSS)**
 - Occurs when an attacker embeds malicious scripting commands on a trusted website
 - Stored/Persistent
 - Attempts to get data provided by the attacker to be saved on the web server by the victim
 - Reflected
 - Attempts to have a non-persistent effect activated by a victim clicking a link on the site
 - DOM-based
 - Attempt to exploit the victim's web browser
 - Prevent XSS with output encoding and proper input validation
- **Cross-Site Request Forgery (XSRF/CSRF)**
 - Occurs when an attacker forces a user to execute actions on a web server for which they are already authenticated
 - Prevent XSRF with tokens, encryption, XML file scanning, and cookie verification

- **Injection Attacks**

- **SQL Injection**

- Attack consisting of the insertion or injection of an SQL query via input data from the client to a web application

- **Injection Attack**

- Insertion of additional information or code through data input from a client to an application

- SQL
 - HTML
 - XML
 - LDAP

- Most common type is an SQL injection

- **How does a normal SQL request work?**

The sequence shows a user attempting to log in. In the first three steps, the user enters 'jason' in the username field and 'pass123' in the password field. In the fourth step, the password is correctly entered. In the fifth step, the user clicks the 'Login' button, which triggers the SQL query: `select * from Users where user_id = 'jason' and password = 'pass123'`.

- **How does an SQL injection work?**

The sequence shows a user attempting to log in with 'jason' and 'OR 1=1'. In the fourth step, the password field contains the injected value. In the fifth step, the user clicks the 'Login' button, which triggers the SQL query: `select * from Users where user_id = 'jason' and password = 'OR 1=1'`.

- SQL injection is prevented through input validation and using least privilege when accessing a database
 - If you see ` OR 1=1; on the exam, it's an SQL injection

- **XML Vulnerabilities**
 - XML data submitted without encryption or input validation is vulnerable to spoofing, request forgery, and injection of arbitrary code
 - XML Bomb (Billion Laughs Attack)
 - XML encodes entities that expand to exponential sizes, consuming memory on the host and potentially crashing it
 - XML External Entity (XXE)
 - An attack that embeds a request for a local resource
 - To prevent XML vulnerabilities from being exploited, use proper input validation

- **Race Conditions**
 - A software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer
 - A race condition vulnerability is found where multiple threads are attempting to write a variable or object at the same memory location
 - Dereferencing
 - A software vulnerability that occurs when the code attempts to remove the relationship between a pointer and the thing it points to.
 - Race conditions are difficult to detect and mitigate
 - Race conditions can also be used against databases and file systems
 - Time of Check to Time of Use (TOCTTOU)
 - The potential vulnerability that occurs when there is a change between when an app checked a resource and when the app used the resource
 - How can you prevent race conditions and TOCTTOU?
 - Develop applications to not process things sequentially if possible
 - Implement a locking mechanism to provide app with exclusive access

- **Design Vulnerabilities**
 - Vulnerabilities often arise from the general design of the software code
 - Insecure Components
 - Any code that is used or invoked outside the main program development process
 - Code Reuse
 - Third-party Library
 - Software Development Kit (SDK)
 - Insufficient Logging and Monitoring
 - Any program that does not properly record or log detailed enough information for an analyst to perform their job
 - Logging and monitoring must support your use case and answer who, what, when, where, and how
 - Weak of Default Configurations
 - Any program that uses ineffective credentials or configurations, or one in which the defaults have not been changed for security
 - Many applications choose to simply run as root or as a local admin
 - Permissions may be too permissive on files or directories due to weak configurations
 - BEST PRACTICE: Utilize scripted installations and baseline configuration templates to secure applications during installation

- **Switches**
 - Switches are the combined evolution of hubs and bridges
 - **MAC Flooding**
 - Attempt to overwhelm the limited switch memory set aside to store the MAC addresses for each port
 - Switches can fail-open when flooded and begin to act like a hub
 - **MAC Spoofing**
 - Occurs when an attacker masks their own MAC address to pretend they have the MAC address of another device
 - MAC Spoofing is often combined with an ARP spoofing attack
 - Limit static MAC addresses accepted
 - Limit duration of time for ARP entry on hosts
 - Conduct ARP inspection
 - **Physical Tampering**
 - Physical tampering occurs when an attacker attempts to gain physical access
- **Routers**
 - **Routers operate at Layer 3**
 - **Routers**
 - Used to connect two or more networks to form an internetwork
 - Routers rely on a packet's IP Addresses to determine the proper destination
 - Once on the network, it conducts an ARP request to find final destination
 - **Access Control List**
 - An ordered set of rules that a router uses to decide whether to permit or deny traffic based upon given characteristics
 - IP Spoofing is used to trick a router's ACL

- **Network Zones**

- Any traffic you wish to keep confidential crossing the internet should use a VPN
- **De-Militarized Zone (DMZ)**
 - Focused on providing controlled access to publicly available servers that are hosted within your organizational network
 - Sub-zones can be created to provide additional protection for some servers
- **Extranet**
 - Specialized type of DMZ that is created for your partner organizations to access over a wide area network
- Intranets are used when only one company is involved

- **Jumpbox**

- **Internet-facing Host**
 - Any host that accepts inbound connections from the internet
- **Demilitarized Zone (DMZ)**
 - A segment isolated from the rest of a private network by one or more firewalls that accepts connections from the Internet over designated ports
 - Everything behind the DMZ is invisible to the outside network
- **Bastion Hosts**
 - Hosts or servers in the DMZ which are not configured with any services that run on the local network
 - To configure devices in the DMZ, a jumpbox is utilized
- **Jumpbox**
 - A hardened server that provides access to other hosts within the DMZ
 - An administrator connects to the jumpbox and the jumpbox connects to hosts in the DMZ
 - The jumpbox and management workstation should only have the minimum required software to perform their job and be well hardened

- **Network Access Control**
 - **Network Access Control (NAC)**
 - Security technique in which devices are scanned to determine its current state prior to being allowed access onto a given network
 - If a device fails the inspection, it is placed into digital quarantine
 - **Persistent Agents**
 - A piece of software that is installed on the device requesting access to the network
 - **Non-Persistent Agents**
 - Uses a piece of software that scans the device remotely or is installed and subsequently removed after the scan
 - NAC can be used as a hardware or software solution
 - IEEE 802.1x standard is used in port-based NAC

- **VLANs**
 - Segment the network
 - Reduce collisions
 - Organize the network
 - Boost performance
 - Increase security
 - **Switch Spoofing**
 - Attacker configures their device to pretend it is a switch and uses it to negotiate a trunk link to break out of a VLAN
 - **Double Tagging**
 - Attacker adds an additional VLAN tag to create an outer and inner tag
 - Prevent double tagging by moving all ports out of the default VLAN group
- **Subnetting**
 - **Subnetting**
 - Act of creating subnetworks logically through the manipulation of IP addresses
 - Efficient use of IP addresses
 - Reduced broadcast traffic
 - Reduced collisions
 - Compartmentalized
 - Subnet's policies and monitoring can aid in the security of your network

- **Network Address Translation**
 - **Network Address Translation (NAT)**
 - Process of changing an IP address while it transits across a router
 - Using NAT can help us hide our network IPs
 - **Port Address Translation (PAT)**
 - Router keeps track of requests from internal hosts by assigning them random high number ports for each request
 - **Class A**
 - 10.0.0.0 to 10.255.255.255
 - **Class B**
 - 172.16.0.0 to 172.31.255.255
 - **Class C**
 - 192.168.0.0 to 192.168.255.255

- **Telephony**
 - **Telephony**
 - Term used to describe devices that provide voice communication to users
 - **Modem**
 - A device that could modulate digital information into an analog signal for transmission over a standard dial-up phone line
 - **War Dialing**
 - Protect dial-up resources by using the callback feature
 - **Public Branch Exchange (PBX)**
 - Internal phone system used in large organizations
 - **Voice Over Internet Protocol (VoIP)**
 - Digital phone service provided by software or hardware devices over a data network
 - **Quality of Service (QoS)**

Perimeter Security

- **Perimeter Security**
 - Security devices focused on the boundary between the LAN and the WAN in your organization's network
 - Perimeter security relies on several different devices
- **Firewalls**
 - Firewalls screen traffic between two portions of a network
 - Software
 - Hardware
 - Embedded
 - **Packet Filtering**
 - Inspects each packet passing through the firewall and accepts or rejects it based on the rules
 - Stateless Packet Filtering
 - Stateful packet filtering tracks the requests leaving the network
 - **NAT Filtering**
 - Filters traffic based upon the ports being utilized and type of connection (TCP or UDP)
 - Application-layer gateway conducts an in-depth inspection based upon the application being used
 - **Circuit-Level gateway**
 - Operates at the session layer and only inspects the traffic during the establishment of the initial session over TCP or UDP
 - **MAC Filtering**
 - **Explicit Allow**
 - Traffic is allowed to enter or leave the network because there is an ACL rule that specifically allows it
 - Example: allow TCP 10.0.0.2 any port 80
 - **Explicit Deny**
 - Traffic is denied the ability to enter or leave the network because there is an ACL rule that specifically denies it
 - Example: deny TCP any any port 23

- **Implicit Deny**
 - Traffic is denied the ability to enter or leave the network because there is no specific rule that allows it
 - Example: deny TCP any any port any
- Most operate at Layer 3 (blocking IP addresses) and Layer 4 (blocking ports)
- **Web Application Firewall**
 - Firewall installed to protect your server by inspecting traffic being sent to a web application
 - A WAF can prevent a XSS or SQL injection
- **Proxy Server**
 - A device that acts as a middle man between a device and a remote server
 - IP Proxy
 - IP Proxy is used to secure a network by keeping its machines anonymous during web browsing
 - Caching Proxy
 - Attempts to serve client requests by delivering content from itself without actually contacting the remote server
 - Disable Proxy Auto-Configuration (PAC) files for security
 - Internet Content Filter
 - Used in organizations to prevent users from accessing prohibited websites and other content
 - Web Security Gateway
 - A go-between device that scans for viruses, filters unwanted content, and performs data loss prevention functions
- **Honeypots and Honeynets**
 - Honeypots and honeynets are used to attract and trap potential attackers
 - **Honeypot**
 - A single computer (or file, group of files, or IP range) that might be attractive to an attacker
 - **Honeynet**
 - A group of computers, servers, or networks used to attract an attacker

- **Data Loss Prevention**
 - Systems designed to protect data by conducting content inspection of data being sent out of the network
 - Also called Information Leak Protection (ILP) or Extrusion Prevention Systems (EPS)
 - DLP is used to ensure your private data remains secure
- **NIDS vs NIPS**
 - **Network Intrusion Detection Systems**
 - Attempts to detect, log, and alert on malicious network activities
 - NIDS use promiscuous mode to see all network traffic on a segment
 - **Network Intrusion Prevention Systems**
 - Attempts to remove, detain, or redirect malicious traffic
 - NIPS should be installed in-line of the network traffic flow
 - Should a NIPS fail open or fail shut?
 - NIPS can also perform functions as a protocol analyzer
- **Unified Threat Management**
 - Relying on a firewall is not enough
 - **Unified Threat Management**
 - Combination of network security devices and technologies to provide more defense in depth within a single device
 - UTM may include a firewall, NIDS/NIPS, content filter, anti-malware, DLP, and VPN
 - UTM is also known as a Next Generation Firewall (NGFW)

Cloud Security

- **Cloud Computing**
 - **Cloud Computing**
 - A way of offering on-demand services that extend the traditional capabilities of a computer or network
 - Cloud computing relies on virtualization to gain efficiencies and cost savings
 - Hyperconvergence allows providers to fully integrate the storage, network, and servers
 - **Virtual Desktop Infrastructure (VDI)**
 - VDI allows a cloud provider to offer a full desktop operating system to an end user from a centralized server
 - **Secure Enclaves and Secure Volumes**
- **Cloud Types**
 - **Public Cloud**
 - A service provider makes resources available to the end users over the Internet
 - **Private Cloud**
 - A company creates its own cloud environment that only it can utilize as an internal enterprise resource
 - A private cloud should be chosen when security is more important than cost
 - **Hybrid**
 - **Community Cloud**
 - Resources and costs are shared among several different organizations who have common service needs

- **As a Service**

- **Software as a Service (SaaS)**

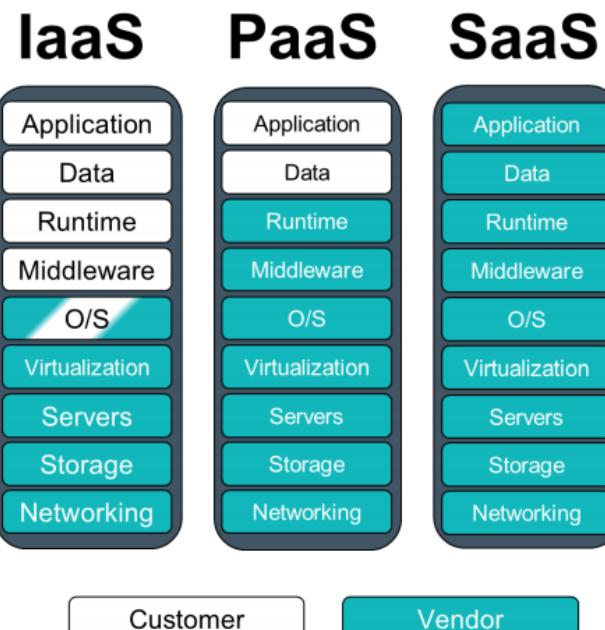
- Provides all the hardware, operating system, software, and applications needed for a complete service to be delivered

- **Infrastructure as a Service (IaaS)**

- Provides all the hardware, operating system, and backend software needed in order to develop your own software or service

- **Platform as a Service (PaaS)**

- Provides your organization with the hardware and software needed for a specific service to operate



- **Cloud Security**
 - Collocated data can become a security risk
 - Configure, manage, and audit user access to virtualized servers
 - Utilizing the cloud securely requires good security policies
 - Data remnants may be left behind after deprovisioning
- **Defending Servers**
 - **File Servers** are used to store, transfer, migrate, synchronize, and archive files for your organization
 - Email servers are a frequent target of attacks for the data they hold
 - Web servers should be placed in your DMZ
 - **FTP Server**
 - A specialized type of file server that is used to host files for distribution across the web
 - FTP servers should be configured to require TLS connections
 - **Domain Controller**
 - A server that acts as a central repository of all the user accounts and their associated passwords for the network
 - Active Directory is targeted for privileged escalation and lateral movement
- **Cloud-based Infrastructure**
 - Cloud-based infrastructure must be configured to provide the same level of security as a local solution

- **Virtual Private Cloud (VPC)**
 - A private network segment made available to a single cloud consumer within a public cloud
 - The consumer is responsible for configuring the IP address space and routing within the cloud
 - VPC is typically used to provision internet-accessible applications that need to be accessed from geographically remote sites
 - On-premise solutions maintain their servers locally within the network
 - Many security products offer cloud-based and on-premise versions
 - Consider compliance or regulatory limitations of storing data in a cloud-based security solution
 - Be aware of the possibility of vendor lock in

- **Cloud Access Security Broker (CASB)**

- Enterprise management software designed to mediate access to cloud services by users across all types of devices
 - Single sign-on
 - Malware and rogue device detection
 - Monitor/audit user activity
 - Mitigate data exfiltration
- Cloud Access Service Brokers provide visibility into how clients and other network nodes use cloud services
 - **Forward Proxy**
 - A security appliance or host positioned at the client network edge that forwards user traffic to the cloud network if the contents of that traffic comply with policy
 - WARNING: Users may be able to evade the proxy and connect directly
 - **Reverse Proxy**
 - An appliance positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with policy
 - WARNING: This approach can only be used if the cloud application has proxy support
 - **Application Programming Interface (API)**
 - A method that uses the brokers connections between the cloud service and the cloud consumer
 - WARNING: Dependent on the API supporting the functions that your policies demand

- **Application Programming Interface (API)**
 - A library of programming utilities used to enable software developers to access functions of another application
 - APIs allow for the automated administration, management, and monitoring of a cloud service
- **curl**
 - A tool to transfer data from or to a server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP, FILE)
- **Function as a Service (FaaS)**
 - A cloud service model that supports serverless software architecture by provisioning runtime containers in which code is executed in a particular programming language

- **Serverless**
 - A software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances
 - Everything in serverless is developed as a function or microservice
 - Serverless eliminates the need to manage physical or virtual servers
 - No patching
 - No administration
 - No file system monitoring
 - The underlying architecture is managed by the cloud service provider
 - Ensure that the clients accessing the services have not been compromised
 - Serverless depends on orchestration

- **Cloud Threats**

- **Insecure Application Programming Interface (API)**
 - WARNING: An API must only be used over an encrypted channel (HTTPS)
 - Data received by an API must pass service-side validation routines
 - Implement throttling/rate-limiting mechanisms to protect from a DoS
- **Improper Key Management**
 - APIs should use secure authentication and authorization such as SAML or OAuth/OIDC before accessing data
 - WARNING: Do not hardcode or embed a key into the source code
 - Do not create one key with full control to access an application's functions
 - Delete unnecessary keys and regenerate keys when moving into a production environment
- **Insufficient Logging and Monitoring**
 - WARNING: Software as a service may not supply access to log files or monitoring tools
 - Logs must be copied to non-elastic storage for long-term retention
- **Unprotected Storage**
 - Cloud storage containers are referred to as buckets or blobs

- WARNING: Access control to storage is administered through container policies, IAM authorizations, and object ACLs
 - Incorrect permissions may occur due to default read/write permissions leftover from creation
 - Incorrect origin settings may occur when using content delivery networks
- **Cross Origin Resource Sharing (CORS) Policy**
 - A content delivery network policy that instructs the browser to treat requests from nominated domains as safe
 - WARNING: Weak CORS policies expose the site to vulnerabilities like XSS

Workflow Orchestration

- **Orchestration**
 - The automation of multiple steps in a deployment process
 - Orchestration is the automation of the automations
 - Rapid elasticity in cloud computing would not be possible without orchestration
 - Resource Orchestration
 - Workload Orchestration
 - Service Orchestration
 - Third-party orchestration platform is protection from vendor lock in
 - Chef
 - Puppet
 - Ansible
 - Docker
 - Kubernetes
 - GitHub

- **CI/CD**
 - Phases: Development, Testing/Integration, Staging, and Production
 - **Continuous Integration**
 - A software development method where code updates are tested and committed to a development or build server/code repository rapidly
 - Continuous integration can test and commit updates multiple times per day
 - Continuous integration detects and resolves development conflicts early and often
 - **Continuous Delivery**
 - A software development method where application and platform requirements are frequently tested and validated for immediate availability
 - **Continuous Deployment**
 - A software development method where application and platform updates are committed to production rapidly
 - Continuous delivery focuses on automated testing of code in order to get it ready for release
 - Continuous deployment focuses on automated testing and release of code in order to get it into the production environment more quickly

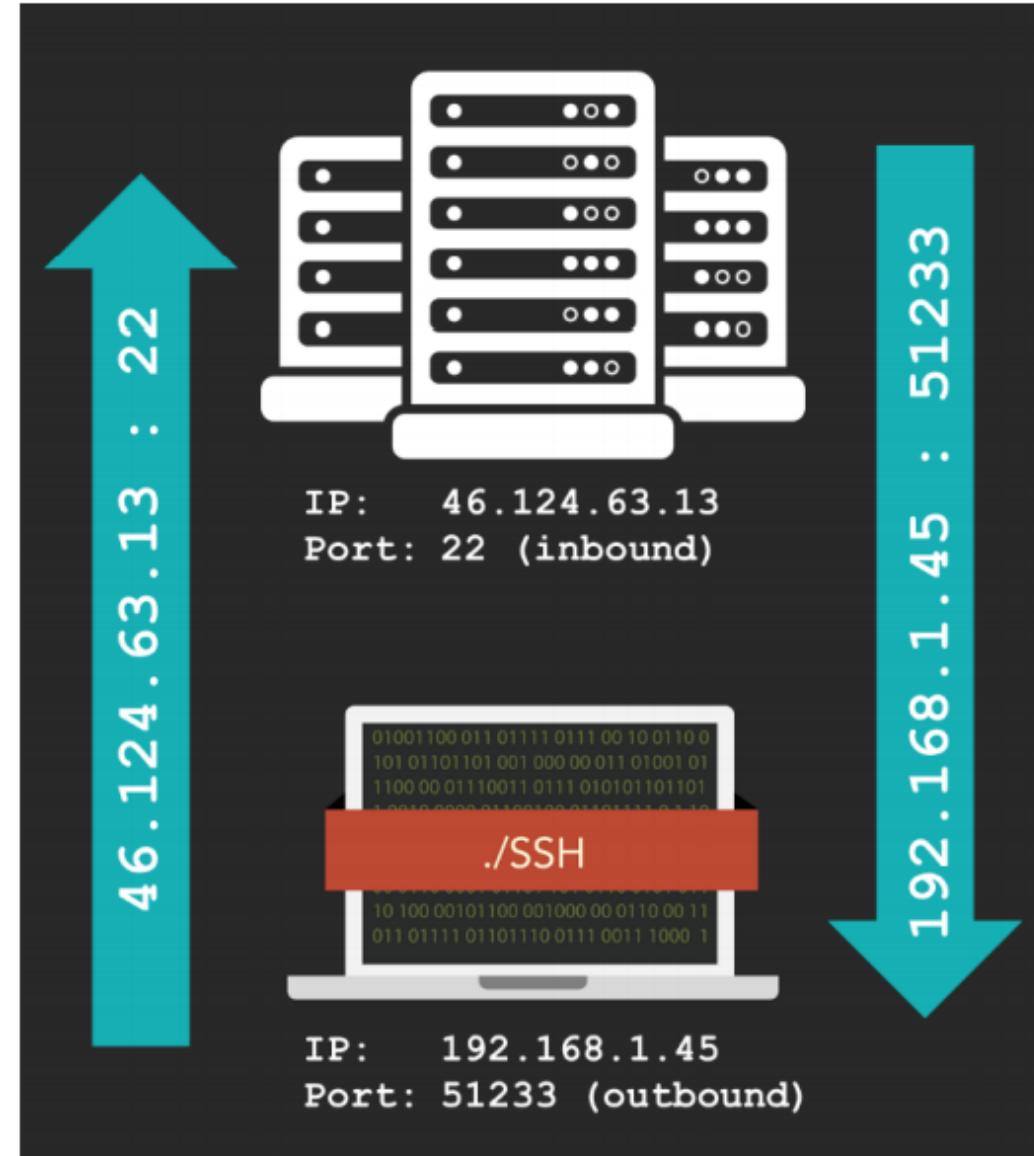
- **DevOps**
 - An organizational culture shift that combines software development and systems operations by referring to the practice of integrating the two disciplines within a company
 - Operations and developers can build, test, and release software faster and more reliably
- **DevSecOps**
 - A combination of software development, security operations, and systems operations by integrating each discipline with the others
 - DevSecOps utilizes a shift-left mindset
 - Integrate security from the beginning
 - Test during and after development
 - Automate compliance checks

- IAC
 - **Infrastructure as Code (IaC)**
 - A provisioning architecture in which deployment of resources is performed by scripted automation and orchestration
 - IaC allows for the use of scripted approaches to provisioning infrastructure in the cloud
 - Robust orchestration can lower overall IT costs, speed up deployments, and increase security
 - **Snowflake Systems**
 - Any system that is different in its configuration compared to a standard template within an infrastructure as code architecture
 - Lack of consistency leads to security issues and inefficiencies in support
 - **Idempotence**
 - A property of IaC that an automation or orchestration action always produces the same result, regardless of the component's previous state
 - IaC uses carefully developed and tested scripts and orchestration runbooks to generate consistent builds

- **Artificial Intelligence (AI)**
 - The science of creating machines with the ability to develop problem solving and analysis strategies without significant human direction or intervention
- **Machine Learning (ML)**
 - A component of AI that enables a machine to develop strategies for solving a task given a labeled dataset where features have been manually identified but without further explicit instructions
 - Machine learning is only as good as the datasets used to train it
- **Artificial Neural Network (ANN)**
 - An architecture of input, hidden, and output layers that can perform algorithmic analysis of a dataset to achieve outcome objectives
 - A machine learning system adjusts its neural network to reduce errors and optimize objectives
- **Deep Learning**
 - A refinement of machine learning that enables a machine to develop strategies for solving a task given a labeled dataset and without further explicit instructions
 - Deep learning uses complex classes of knowledge defined in relation to simpler classes of knowledge to make more informed determinations about an environment

Network Attacks

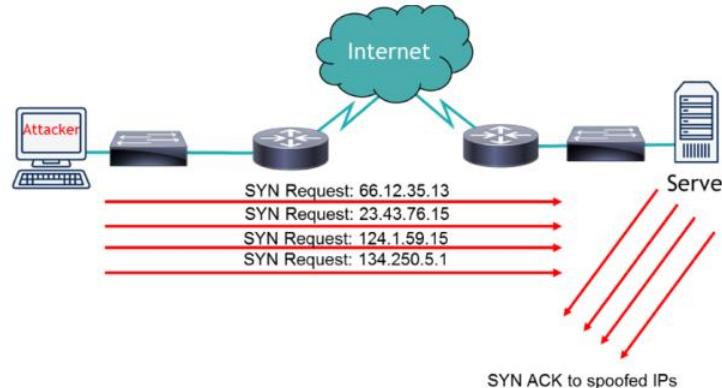
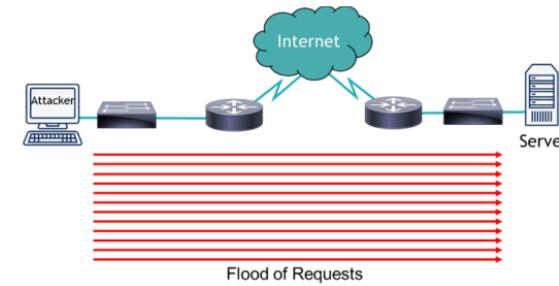
- **Network Attacks**
 - Denial of Service
 - Spoofing
 - Hijacking
 - Replay
 - Transitive Attacks
 - DNS attacks
 - ARP Poisoning
 - Ports and protocols will be tested on the Security+ exam
- **Ports and Protocols**
 - **Port**
 - A logical communication endpoint that exists on a computer or server
 - **Inbound Port**
 - A logical communication opening on a server that is listening for a connection from a client
 - **Outbound Port**
 - A logical communication opening created on a client in order to call out to a server that is listening for a connection



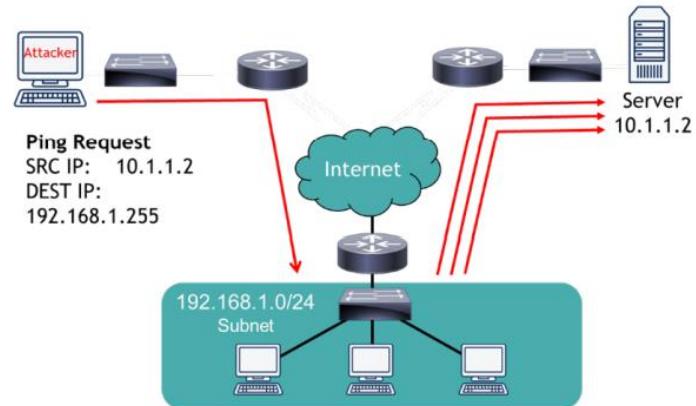
21 TCP	FTP	File Transfer Protocol is used to transfer files from host to host
22 TCP/UDP	SSH, SCP, SFTP	Secure Shell is used to remotely administer network devices and systems. SCP is used for secure copy and SFTP for secure FTP.
23 TCP/UDP	Telnet	Unencrypted method to remotely administer network devices (should not be used)
25 TCP	SMTP	Simple Mail Transfer Protocol is used to send email over the Internet
53 TCP/UDP	DNS	Domain Name Service is used to resolve hostnames to IPs and IPs to hostnames
69 UDP	TFTP	Trivial FTP is used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host
80 TCP	HTTP	Hyper Text Transfer Protocol is used to transmit web page data to a client for unsecured web browsing
88 TCP/UDP	Kerberos	Used for network authentication using a system of tickets within a Windows domain
110 TCP	POP3	Post Office Protocol v3 is used to receive email from a mail server
119 TCP	NNTP	Network News Transfer Protocol is used to transport Usenet articles
135 TCP/UDP	RPC/DCOM-scm	Remote Procedure Call is used to locate DCOM ports request a service from a program on another computer on the network
137-139 TCP/UDP	NetBIOS	NetBIOS is used to conduct name querying, sending of data, and other functions over a NetBIOS connection
143 TCP	IMAP	Internet Message Access Protocol is used to receive email from a mail server with more features than POP3
161 UDP	SNMP	Simple Network Management Protocol is used to remotely monitor network devices
162 TCP/UDP	SNMPTRAP	Used to send Trap and InformRequests to the SNMP Manager on a network
389 TCP/UDP	LDAP	Lightweight Directory Access Protocol is used to maintain directories of users and other objects
443 TCP	HTTPS	Hyper Text Transfer Protocol Secure is used to transmit web page data to a client over an SSL/TLS-encrypted connection
445 TCP	SMB	Server Message Block is used to provide shared access to files and other resources on a network
465/587 TCP	SMTP with SSL/TLS	Simple Mail Transfer Protocol used to send email over the Internet with an SSL and TLS secured connection
514 UDP	Syslog	Syslog is used to conduct computer message logging, especially for routers and firewall logs
636 TCP/UDP	LDAP SSL/TLS	LDAP is used to maintain directories of users and other objects over an encrypted SSL/TLS connection
860 TCP	iSCSI	iSCSI is used for linking data storage facilities over IP
989/990 TCP	FTPS	File Transfer Protocol Secure is used to transfer files from host to host over an encrypted connection
993 TCP	IMAP4 with SSL/TLS	Internet Message Access Protocol is used to receive email from a mail server over an SSL/TLS-encrypted connection
995 TCP	POP3 (SSL/TLS)	Post Office Protocol v3 is used to receive email from a mail server using an SSL/TLS-encrypted connection
1433 TCP	Ms-sql-s	Microsoft SQL server is used to receive SQL database queries from clients
1645/1646 UDP	RADIUS (alternative)	Remote Authentication Dial-In User Service is used for authentication and authorization (1645) and accounting (1646)
1701 UDP	L2TP	Layer 2 Tunnel Protocol is used as an underlying VPN protocol but has no inherent security
1723 TCP/UDP	PPTP	Point-to-Point Tunneling Protocol is an underlying VPN protocol with built-in security
1812/1813 UDP	RADIUS	Remote Authentication Dial-In User Service is used for authentication and authorization (1812) and accounting (1813)
3225 TCP/UDP	FCIP	Fibre Channel IP is used to encapsulate Fibre Channel frames within TCP/IP packets
3260 TCP	iSCSI Target	iSCSI Target is the listening port for iSCSI-targeted devices when linking data storage facilities over IP
3389 TCP/UDP	RDP	Remote Desktop Protocol is used to remotely view and control other Windows systems via a Graphical User Interface
3868 TCP	Diameter	A more advanced AAA protocol that is a replacement for RADIUS
6514 TCP	Syslog over TLS	It is used to conduct computer message logging, especially for routers and firewall logs, over a TLS-encrypted connection

- Ports can be any number between 0 and 65,535
- **Well-Known Ports**
 - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)
- **Registered Ports**
 - Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols
- **Dynamic or Private Ports**
 - Ports 49,152 to 65,535 can be used by any application without being registered with IANA
- **Memorization of Ports**
 - 65,536 ports are available for use
- **Unnecessary Ports**
 - 65,536 ports available
 - 35 ports to memorize
 - **Unnecessary Port**
 - Any port that is associated with a service or function that is non-essential to the operation of your computer or network
 - Any open port represents a possible vulnerability that might be exposed
 - **Inbound Port**
 - A logical communication opening on a server that is listening for a connection from a client
 - C:\ net stop service
 - # sudo stop service

- Denial of Service
 - Denial of Service (DoS)
 - Term used to describe many different types of attacks which attempt to make a computer or server's resources unavailable
 - Flood Attacks
 - Ping of Death
 - Teardrop Attack
 - Permanent DoS
 - Fork Bomb
 - Flood Attack
 - A specialized type of DoS which attempts to send more packets to a single server or host than they can handle
 - Fraggle Attack
 - Attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets
 - SYN Flood
 - Variant on a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions but never completes the 3-way handshake
 - Flood guards, time outs, and an IPS can prevent SYN Floods



- Ping Flood
 - An attacker attempts to flood the server by sending too many ICMP echo request packets (which are known as pings)
- Smurf Attack
 - Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (victim server), using up bandwidth and processing



- **XMAS Attack**
 - A specialized network scan that sets the FIN, PSH, and URG flags set and can cause a device to crash or reboot
 - **Ping of Death**
 - An attack that sends an oversized and malformed packet to another computer or server
 - **Teardrop Attack**
 - Attack that breaks apart packets into IP fragments, modifies them with overlapping and oversized payloads, and sends them to a victim machine
 - **Permanent Denial of Service**
 - Attack which exploits a security flaw to permanently break a networking device by reflashing its firmware
 - **Fork Bomb**
 - Attack that creates a large number of processes to use up the available processing power of a computer
-
- **DDoS**
 - **Distributed Denial of Service (DDoS)**
 - A group of compromised systems attack simultaneously a single target to create a Denial of Service (DOS)
 - **DNS Amplification**
 - Attack which relies on the large amount of DNS information that is sent in response to a spoofed query on behalf of the victimized server

- **Stopping a DDoS**
 - GitHub suffered a 1.35 Tbps DDoS
 - **Blackholing or Sinkholing**
 - Identifies any attacking IP addresses and routes all their traffic to a non-existent server through the null interface
 - An IPS can prevent a small-scale DDoS
 - Specialized security services cloud providers can stop DDoS attacks
- **Spoofing**
 - Occurs when an attacker masquerades as another person by falsifying their identity
 - Anything that uniquely identifies a user or system can be spoofed
 - Proper authentication is used to detect and prevent spoofing

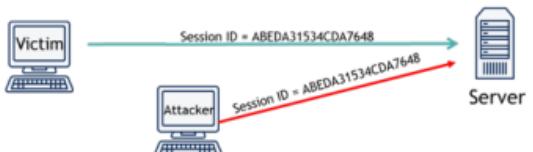
- **Hijacking**

- **Hijacking**

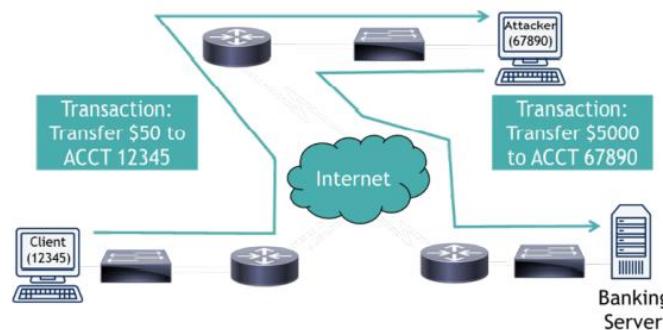
- Exploitation of a computer session in an attempt to gain unauthorized access to data, services, or other resources on a computer or server
 - Session theft
 - TCP/IP hijacking
 - Blind hijacking
 - Clickjacking
 - Man-in-the-Middle
 - Man-in-the-Browser
 - Watering hole
 - Cross-site scripting

- **Session Theft**

- Attacker guesses the session ID for a web session, enabling them to take over the already authorized session of the client



- **TCP/IP Hijacking**
 - Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access
- **Blind Hijacking**
 - Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not
- **Clickjacking**
 - Attack that uses multiple transparent layers to trick a user into clicking on a button or link on a page when they were intending to click on the actual page
- **Man-in-the-Middle (MITM)**
 - Attack that causes data to flow through the attacker's computer where they can intercept or manipulate the data



- **Man-in-the-Browser (MITB)**
 - Occurs when a Trojan infects a vulnerable web browser and modifies the web pages or transactions being done within the browser
- **Watering Hole**
 - Occurs when malware is placed on a website that the attacker knows his potential victims will access

- **DNS Attacks**

- **DNS Poisoning**

- Occurs when the name resolution information is modified in the DNS server's cache
 - If the cache is poisoned, then the user can be redirected to a malicious website

- **Unauthorized Zone Transfer**

- Occurs when an attacker requests replication of the DNS information to their systems for use in planning future attacks

- **Altered Hosts File**

- Occurs when an attacker modifies the host file to have the client bypass the DNS server and redirects them to an incorrect or malicious website
 - Windows stores the hosts file in the following directory:

\%systemroot%\system 32\drivers\etc

- **Pharming**

- Occurs when an attacker redirects one website's traffic to another website that is bogus or malicious

- **Domain Name Kiting**

- Attack that exploits a process in the registration process for a domain name that keeps the domain name in limbo and cannot be registered by an authenticated buyer

- **ARP Poisoning**

- Attack that exploits the IP address to MAC resolution in a network to steal, modify, or redirect frames within the local area network
 - Allows an attacker to essentially take over any sessions within the LAN
 - ARP Poisoning is prevented by VLAN segmentation and DHCP snooping

Securing Networks

- **Securing Networks**
 - Wired and wireless networks are vulnerable to attacks
- **Securing Network Devices**
 - Network devices include switches, routers, firewalls, and more
 - **Default Accounts**
 - A user or administrator-level account that is installed on a device by the manufacturer during production
 - **Weak Passwords**
 - A password should be long, strong, and complex. This should require at least 14 characters with a mix of uppercase, lowercase, numbers, and special characters
 - password
 - PaSSworD
 - Pa55w0rd
 - P@\$w0rd
 - **Privilege Escalation**
 - Occurs when a user is able to gain the rights of another user or administrator
 - Vertical Privilege Escalation
 - Horizontal Privilege Escalation
 - **Backdoor**
 - A way of bypassing normal authentication in a system
 - An IPS, proper firewall configs, network segmentation, and firmware updates are the keys to having network security

- **Securing Network Media**
 - **Network Media**
 - Copper, fiber optic, and coaxial cabling used as the connectivity method in a wired network
 - **Electromagnetic Interference (EMI)**
 - A disturbance that can affect electrical circuits, devices, and cables due to radiation or electromagnetic conduction
 - EMI can be caused by TVs, microwaves, cordless phones, motors, and other devices
 - Shielding the cables (STP) or the source can minimize EMI
 - **Radio Frequency Interference (RFI)**
 - A disturbance that can affect electrical circuits, devices, and cables due to AM/FM transmissions or cell towers
 - RFI causes more problems for wireless networks
 - **Crosstalk**
 - Occurs when a signal transmitted on one copper wire creates an undesired effect on another wire
 - UTP is commonly used more often than STP
 - **Data Emanation**
 - The electromagnetic field generated by a network cable or device when transmitting
 - A Faraday cage can be installed to prevent a room from emanating
 - Split the wires of a twisted-pair connection
 - **Protected Distribution System (PDS)**
 - Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats

- **Securing WiFi Devices**
 - **Service Set Identifier (SSID)**
 - Uniquely identifies the network and is the name of the WAP used by the clients
 - Disable the SSID broadcast in the exam
 - **Rogue Access Point**
 - An unauthorized WAP or Wireless Router that allows access to the secure network
 - **Evil Twin**
 - A rogue, counterfeit, and unauthorized WAP with the same SSID as your valid one
- **Wireless Encryption**
 - Encryption of data in transit is paramount to security
 - **Pre-Shared Key**
 - Same encryption key is used by the access point and the client

- **Wired Equivalent Privacy**
 - Original 802.11 wireless security standard that claims to be as secure as a wired network
 - WEP's weakness is its 24-bit IV (Initialization Vector)
- **WiFi Protected Access (WPA)**
 - Replacement for WEP which uses TKIP, Message Integrity Check (MIC), and RC4 encryption
 - WPA was flawed, so it was replaced by WPA2
- **WiFi Protected Access version 2 (WPA2)**
 - 802.11i standard to provide better wireless security featuring AES with a 128-bit key, CCMP, and integrity checking
 - WPA2 is considered the best wireless encryption available

If you are asked about...	Look for the answer with...
Open	No security or protection provided
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

- If we make operations easier, then security is reduced
- **WiFi Protected Setup (WPS)**
 - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable
 - Always disable WPS
- Encryption and VPNs are always a good idea

- **Wireless Access Points**
 - Wireless security also relies upon proper WAP placement

Omnidirectional Unidirectional



- Wireless B, G, and N use a 2.4 GHz signal
- Wireless A, N, and AC use a 5.0 GHz signal
- 2.4 GHz signals can travel further than 5 GHz
- **Jamming**
 - Intentional radio frequency interference targeting your wireless network to cause a denial of service condition
 - Wireless site survey software and spectrum analyzers can help identify jamming and interference
- **AP Isolation**
 - Creates network segment for each client when it connects to prevent them from communicating with other clients on the network

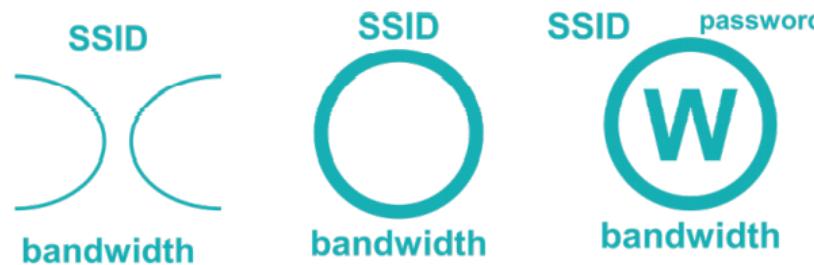
- **Wireless Attacks**

- **War Driving**

- Act of searching for wireless networks by driving around until you find them
 - Attackers can use wireless survey or open source attack tools

- **War Chalking**

- Act of physically drawing symbols in public places to denote the open, closed, and protected networks in range
 - War chalking digitally is becoming more commonplace



- **IV Attack**

- Occurs when an attacker observes the operation of a cipher being used with several different keys and finds a mathematical relationship between those keys to determine the clear text data
 - This happened with WEP and makes it easy to crack

- **WiFi Disassociation Attack**

- Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects
 - Used as part of an attack on WPA/WPA2

- **Brute Force Attack**

- Occurs when an attacker continually guesses a password until the correct one is found
 - Brute force will always find the password...eventually!

- **WPA3**
 - Wi-Fi Protected Access 3 (WPA3) was introduced in 2018 to strengthen WPA2
 - WPA3 has an equivalent cryptographic strength of 192-bits in WPA3 - Enterprise Mode
 - WPA3 - Enterprise Mode
 - AES-256 encryption with a SHA-384 hash for integrity checking
 - WPA3 - Personal Mode
 - CCMP-128 as minimum encryption required for secure connectivity
 - Largest improvement in WPA3 is the removal of the Pre-Shared Key (PSK) exchange
 - Simultaneous Authentication of Equals (SAE)
 - A secure password-based authentication and password-authenticated key agreement method
 - Simultaneous Authentication of Equals (SAE) provides forward secrecy
 - Perfect Forward Secrecy or Forward Secrecy
 - A feature of key agreement protocols (like SAE) that provides assurance that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised
 - The AP and the client use a public key system to generate a pair of long-term keys
 - The AP and the client exchange a one-time use session key using a secure algorithm like Diffie-Hellman
 - The AP sends the client messages and encrypts them using the session key created in Step 2

- **Other Wireless Technologies**
 - **Bluejacking**
 - Sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets
 - **Bluesnarfing**
 - Unauthorized access of information from a wireless device through a Bluetooth connection
 - Bluejacking sends information
 - Bluesnarfing takes information
 - Don't allow Bluetooth devices to use default PINs for pairing
 - **Radio Frequency Identification (RFID)**
 - Devices that use a radio frequency signal to transmit identifying information about the device or token holder
 - RFID can operate from 10 cm to 200 meters depending on the device
 - **Near Field Communication (NFC)**
 - Allows two devices to transmit information when they are within close range through automated pairing and transmission
 - NFC devices are operated within 4 cm from each other

OPERATIONS AND INCIDENT RESPONSE

16%

Governance, Risk, and Compliance

14%

Cryptography

and Public Key Infrastructure

Data Protection

- **Data-in-Transit**
 - SSL
- **Data-at-Rest**
 - Disk Encryption
- **Data-in-Use**
 - Intel's Software Guard Extensions (SGX)
- Data-in-transit, data-at-rest, and data-in-use are terms commonly used to describe states of data in a computing system. Understanding how to differentiate these terms based on their similarities and differences when it comes to cryptography is important.

Cryptography Definitions and Concepts

- *Plaintext*
 - *Readable Data*
- *Ciphertext*
 - random and unreadable



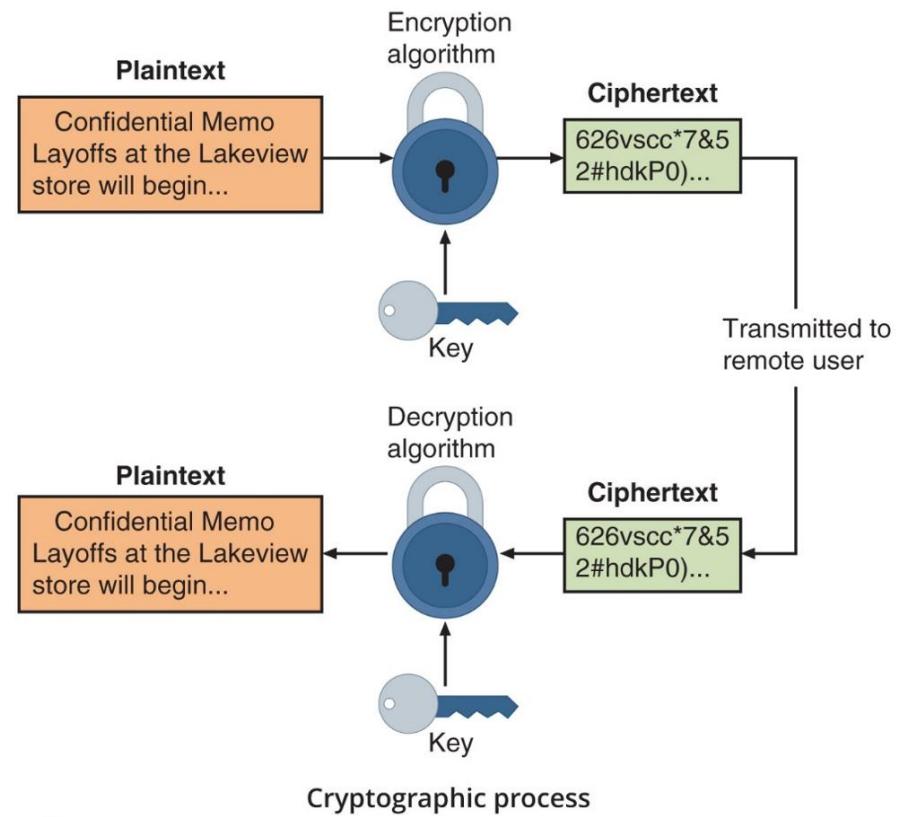
- *Cryptosystem*
 - Encryption
 - Converting Plaintext to Ciphertext
 - Decryption
 - Converting Ciphertext to Plaintext

Cryptography Definitions and Concepts

- **Algorithms**
 - The set of rules also known as the *cipher*, dictates how enciphering and deciphering take place
- **KEY**
 - Works with the algorithm to encrypt and decrypt the text.
- **Cryptanalysis**
 - The science of studying and breaking the secrecy of encryption processes, compromising authentication schemes, and reverse-engineering algorithms and keys.

Cryptography Definitions and Concepts

- Plaintext data is input into a **cryptographic algorithm** (also called a **cipher**)
 - Consists of procedures based on a mathematical formula used to encrypt and decrypt the data
- Key
 - A mathematical value entered into the algorithm to produce ciphertext
 - The reverse process uses the key to decrypt the message



Cryptographic Basics

Goals

- ***Confidentiality*** ensures that data remains private in three different situations: when it is at rest, when it is in transit, and when it is in use.
- ***Integrity*** ensures that data is not altered without authorization.
- ***Authentication*** verifies the claimed identity of system users and is a major function of cryptosystems.
- ***Nonrepudiation*** provides assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender

Modern Cryptography

- **Security through obscurity**

- Early days of cryptography relied on secrecy as the main method of providing security to a system or component.
- If you know that a ROT3 (or Rotate 3) cipher is being used you can easily decrypt messages
- Modern cryptosystems do not rely on the secrecy of their algorithms
 - Instead they rely on the secrecy of one or more cryptographic keys used to personalize the algorithm for specific users or groups of users.

- **Private-Key Encryption**

- *Private-key encryption* systems use a secret key, which is shared between the authorized sender and the intended receiver.

- **Public-Key Encryption**

- Asymmetrical cryptography is referred to as *public-key cryptography* (a.k.a. publickey interchange, or PKI). This design uses a separate pair of keys for encryption and

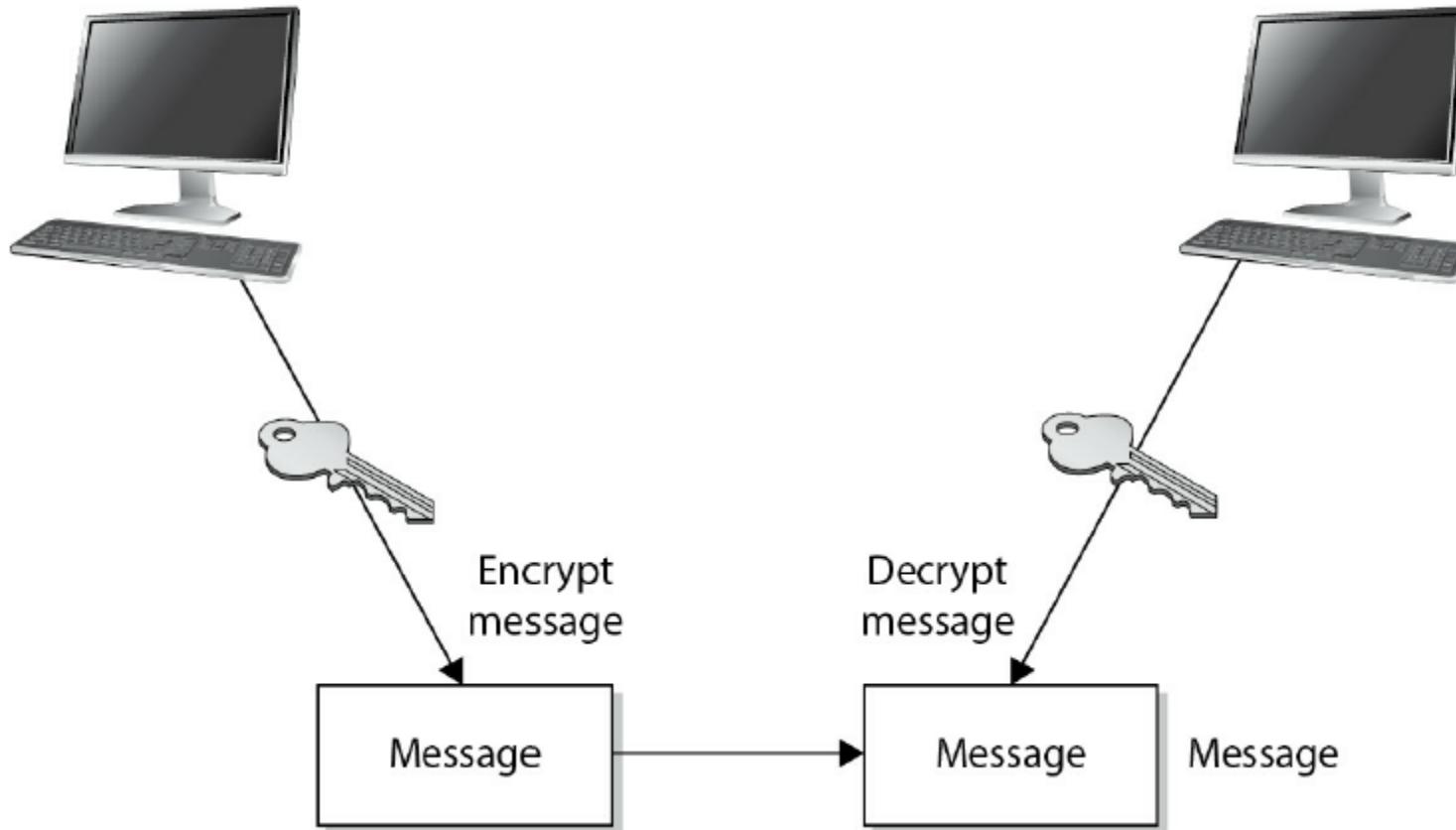
Modern Cryptography

- Modern cryptographic algorithms rely upon underlying mathematical formulas
 - Depend upon the quality of random numbers (no identifiable pattern or sequence)
- Software relies upon a **pseudorandom number generator (PRNG)**
 - An algorithm for creating a sequence of numbers whose properties approximate those of a random number
- Two factors that can thwart threat actors from discovering the underlying key to cryptographic algorithms:
 - **Diffusion** – if a single character of plaintext is changed then it should result in multiple characters of the ciphertext changing
 - **Confusion** – the key does not relate in a simple way to the ciphertext

Cryptographic Algorithms

- Three categories of cryptographic algorithms
 - Symmetric cryptographic algorithms
 - Asymmetric cryptographic algorithms
 - Hash algorithms
- **Cryptographic operations** include encryption for the protection of confidentiality, hashing for the protection of integrity, digital signatures to manage non-repudiation, and a bevy of specialty operations such as key exchanges.
- **Encryption operations** are characterized by the quantity and type of data, as well as the level and type of protection sought. Integrity protection operations are characterized by the level of assurance desired. Data is characterized by its usage: data-in-transit, data-at-rest, or data-in-use. It is also characterized in how it can be used, either in block form or stream form.

Symmetric encryption uses the same keys.

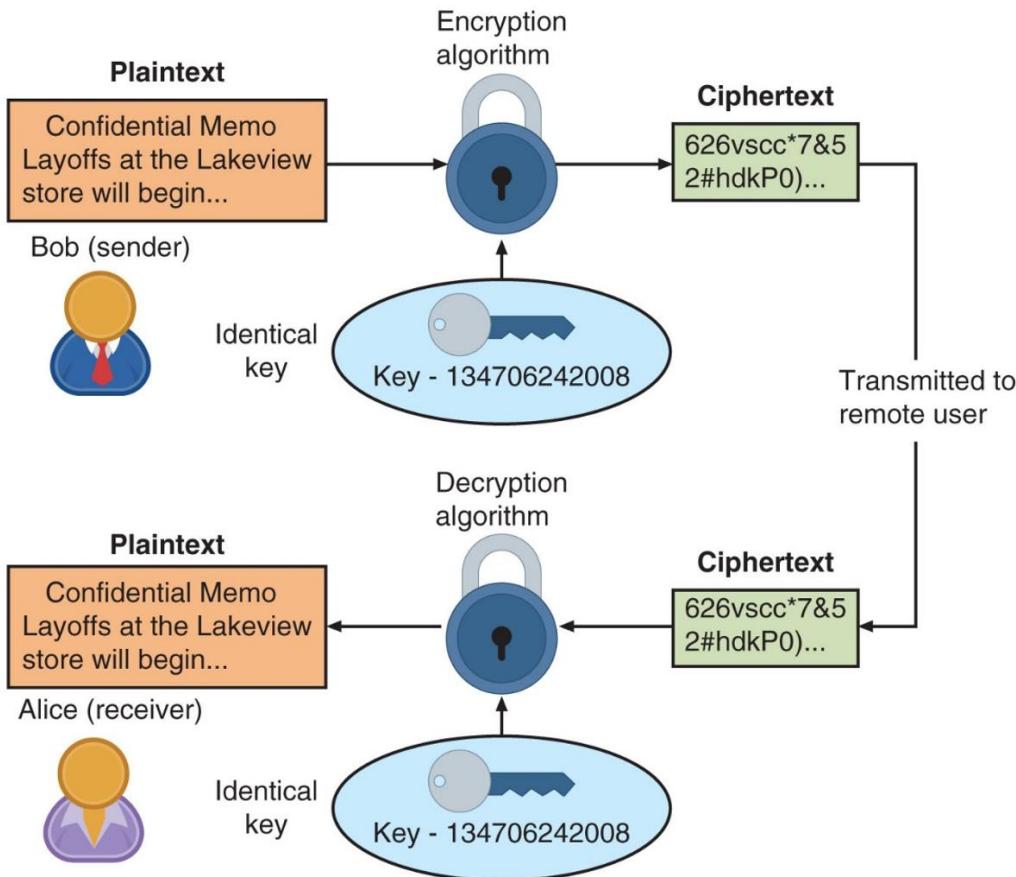


The equation used to calculate the number of symmetric keys needed is $N(N - 1)/2 = \text{number of keys}$

Symmetric Cryptographic Algorithms

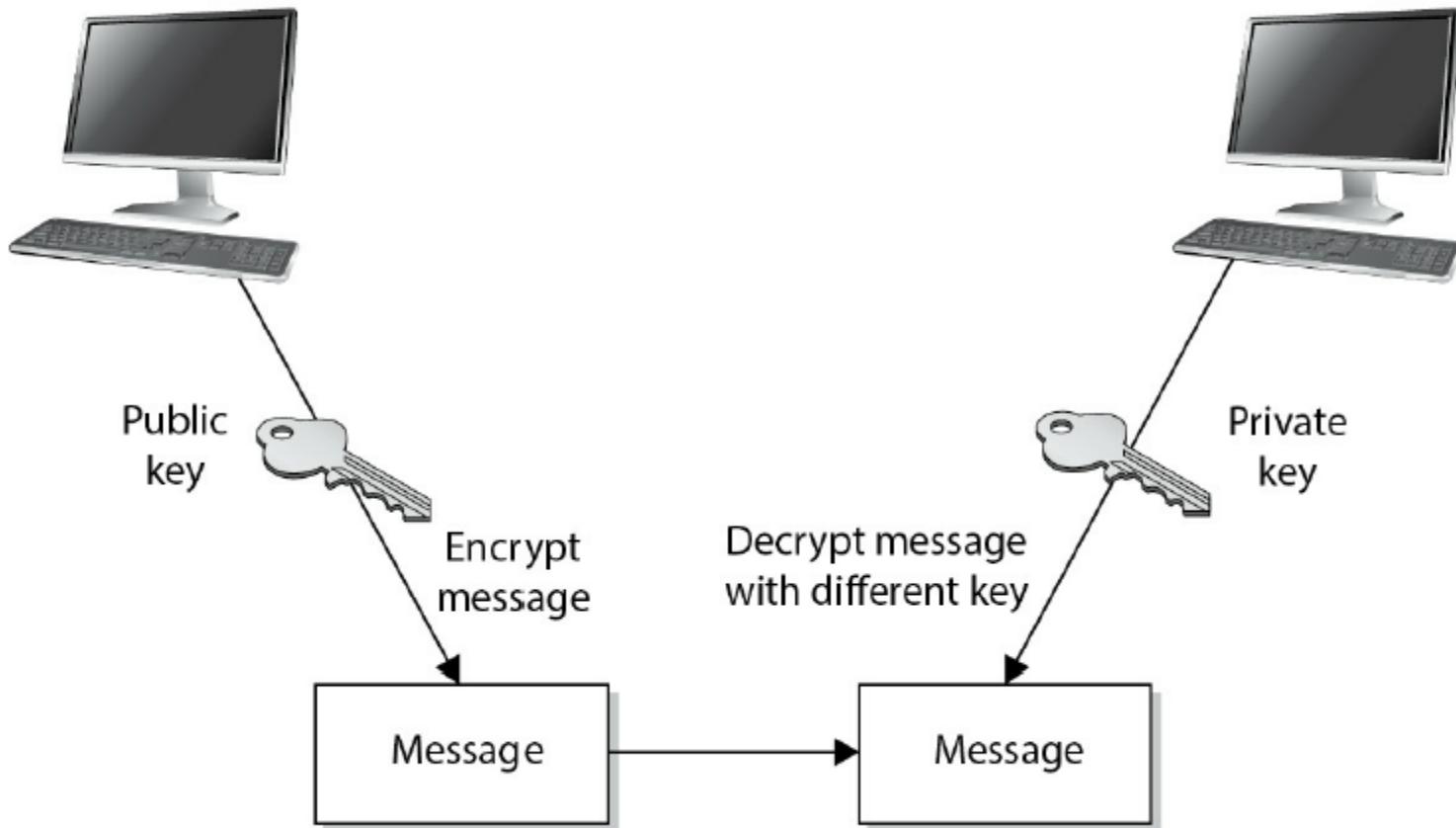
- Symmetric cryptographic algorithms
 - use the same single key to encrypt and decrypt a document
 - Original cryptographic algorithms were symmetric
 - Also called **private key cryptography** (the key is kept private between sender and receiver)
 - Common algorithms include:
 - Data Encryption Standard
 - Triple Data Encryption Standard
 - Advanced Encryption Standard
 - Several other algorithms
- **Strengths:**
 - Much faster (less computationally intensive) than asymmetric systems.
 - Hard to break if using a large key size.
 - **Weaknesses:**
 - Requires a secure mechanism to deliver keys properly.
 - Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
 - Provides confidentiality but not authenticity or nonrepudiation.

Symmetric Cryptographic Algorithms



Symmetric (private key) cryptography

Asymmetric systems use two different keys
for encryption and decryption purposes.



Asymmetric Cryptographic Algorithms

- Weakness of symmetric algorithms
 - Distributing and maintaining a secure single key among multiple users distributed geographically
- Asymmetric cryptographic algorithms
 - Also known as **public key cryptography**
 - Uses two mathematically related keys
 - Public key available to everyone and freely distributed
 - Private key known only to individual to whom it belongs

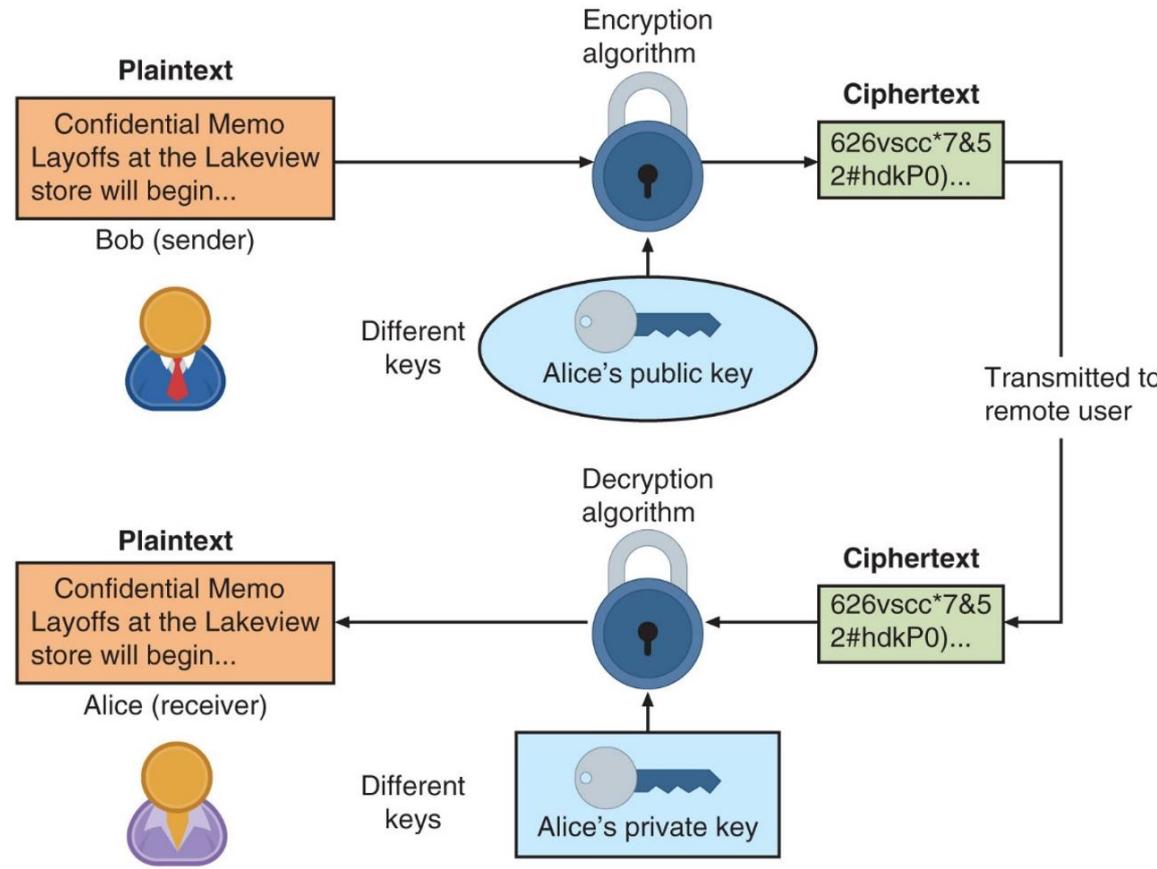
Strengths:

- Better key distribution than symmetric systems.
- Better scalability than symmetric systems.
- Can provide authentication and nonrepudiation.

Weaknesses:

- Works much more slowly than symmetric systems.
- Mathematically intensive tasks.

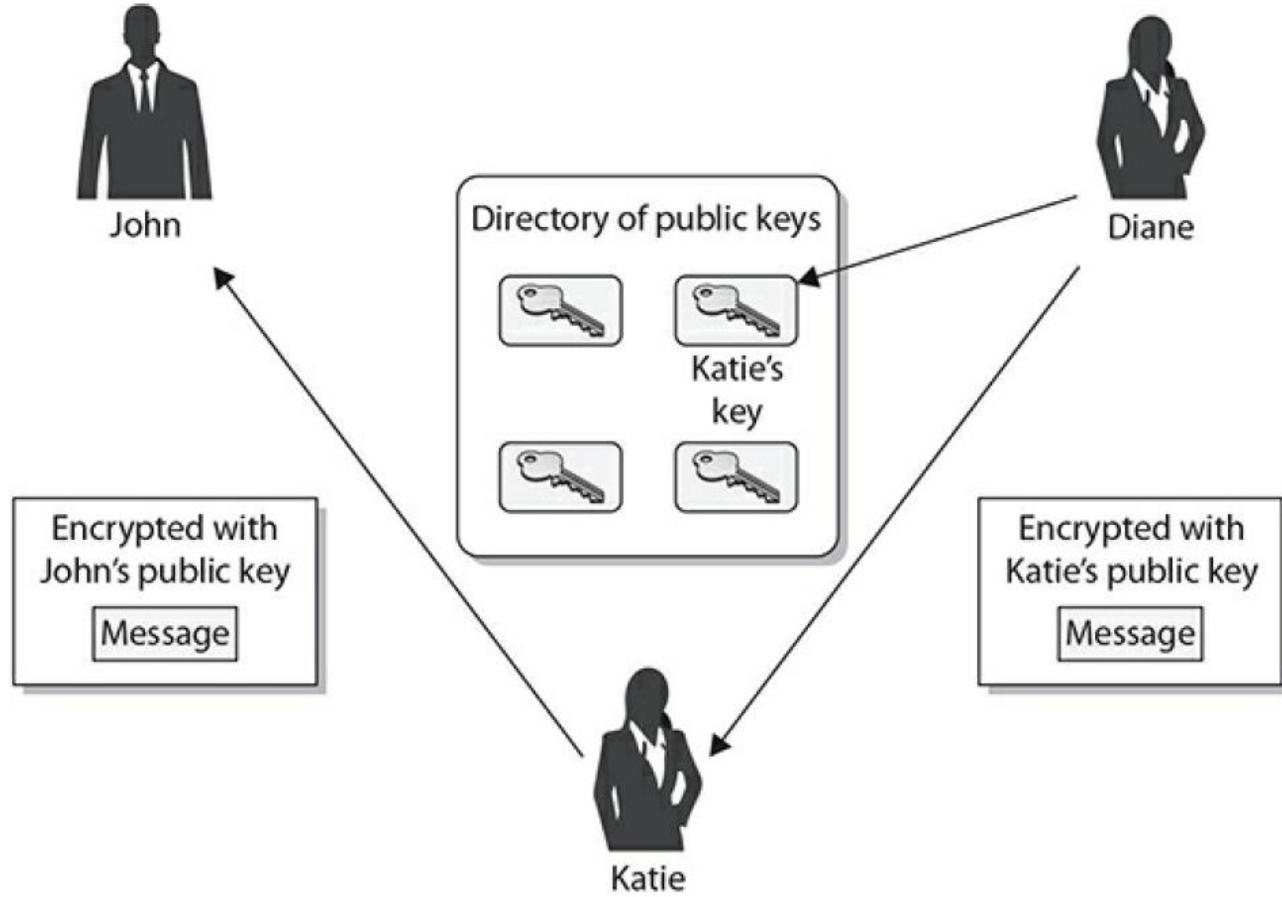
Asymmetric Cryptographic Algorithms



Asymmetric (public key) cryptography

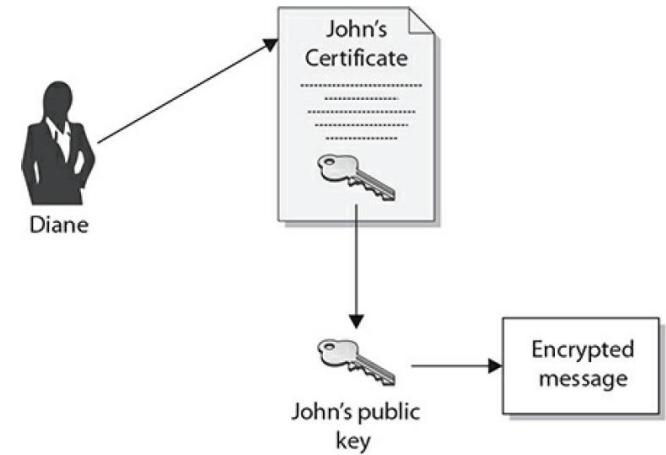
Public key infrastructure(PKI)

- *Public key infrastructure(PKI)* is not an algorithm, a protocol, or an application—it is an infrastructure based on public key cryptography
- PKI is made up of many different parts:
 - certificate authorities,
 - registration authorities,
 - certificates, keys,
 - and users.



Man-in-the Middle Attack

1. Katie replaces John's public key with her key in the publicly accessible directory.
2. Diane extracts what she thinks is John's key, but it is in fact Katie's key.
3. Katie can now read messages Diane encrypts and sends to John.
4. After Katie decrypts and reads Diane's message, she encrypts it with John's public key and sends it on to him so he will not be the wiser.



Public keys are components of digital certificates.

Without PKIs, individuals could spoof others' identities, a man-in-the-middle attack.

Certificate Authority (CA)

- **Certificate Authority** is the trusted authority that certifies individuals' identities and creates electronic documents indicating that individuals are who they say they are.

