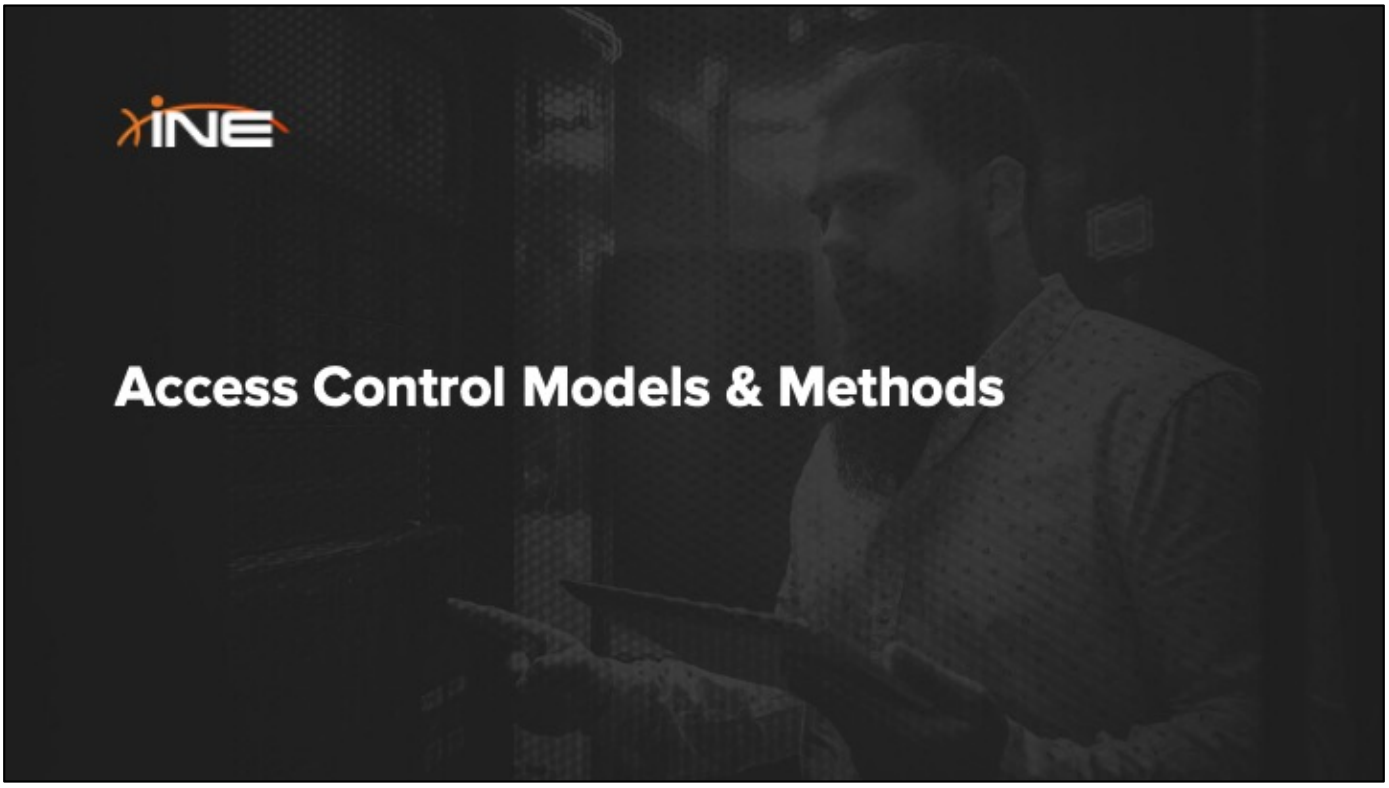


Course Objectives

- Become familiar with what Access Controls are and their importance
- Expose you to many types of Access Control categories, methods and implementations
- Compare and Contrast different types of Access Controls

- A basic understanding of file management within host Operating Systems
- Elementary understanding of computer networking
- Familiarity with IP packet structure

Course Prerequisites

Let's Get Started!

Access Control Introduction

- Access controls regulate the interactions between a subject and an object
  - Object: A passive object/entity which holds information
  - Subject:
    - An entity (person, application, device, etc) attempting to retrieve, edit or delete the information or resources held by the object
    - May perform an action on behalf of a "Principle"
- Primary objective of an access control is to grant, prevent, or revoke access to an object

- A single entity could be both a subject and an object. For example, if your web browser reaches out to a web server, from your browser's perspective (which is the Subject) the web server is the Object. However, once the web server receives your request, it may in turn, ask another server (which contains images, data, video files, authentication database, etc) for information. In that case, now the web server has become the subject and the database it is querying is an Object.

What Access Controls Protect

- Confidentiality of resources
  - Ensure only authorized use (login protections)
  - Attacks at this level are trying to gain access to resources by unauthorized users
- Integrity and state of resources
  - Protect against unauthorized modification of a resource
  - Write/Delete protections
- Availability of resources
  - Protect against malicious attacks designed to make a resource unavailable
  - Delete/Shutdown/Overwhelm protections

Access Control Characterization

- Access controls can be categorized by the type of service they provide:
  - Identification
  - Authentication
  - Authorization
  - Accounting
- A single access control may perform one or more of the above tasks

- For example, the Radius protocol, which is a form of an access control, performs both authentication and authorization within the same exchange of messages between subject and object.

Identification

- Access controls that concentrate on identification...
  - Require subjects to derive some form of identification
  - Provide rules around how identification is to be constructed
  - Provide rules concerning the lifetime of identification credentials
- Guidelines pertaining to identification
  - Each subject should have a unique identifier
  - Secure identities should be nondescriptive
  - Identities should be issued in a secure manner
    - Includes all steps in requesting and granting identities
    - Called, "Secure Issuance"

- A ruleset in an application that forces you to change your identity every 6-months and forces you to include certain characters in your identity would be an example of this.

Authentication

- The process of proving a subject's identity
- Subject must provide additional, unique information along with its identity
- How is the additional information guaranteed to be unique?
  - **Authentication by knowledge**:
    - Something only the subject would know
    - Passwords, PIN codes, Security questions
  - **Authentication by ownership**:
    - Providing something that only the true subject would own
    - Token cards, badge for facility access, USB authentication stick
  - **Authentication by characteristic:**
    - Authentication based on physical or behavioral characteristic of the subject
    - Biometric authentication, voice recognition, facial recognition

- Of the three methods above, authentication by characteristic is considered the most secure because (unless someone cuts off your finger or removes your eyeball) it is typically based on something that nobody could steal from you.
- Examples of behavioral characteristic: signature dynamics and keystroke dynamics/patterns (typing rhythm, pressure and dwell time on individual keys), Physical movement (gait analysis, mouse movements) and Location recognition (identification via GPS or network data to detect suspicious login attempts from unusual places)

Measuring Authentication by Characteristic

- There are several biometric or behavioral-based authentication mechanisms available
- Attempting to quantify effectiveness is a useful selection metric
- Errors produced by these systems fall into two categories:
  - Type-I error
    - **False Rejection Rate (FRR)**
    - Rejection of a valid user who should have been authenticated
  - Type-II error
    - **False Acceptance Rate (FAR)**
    - Acceptance of an invalid user who should have been rejected

CER and EER Metrics

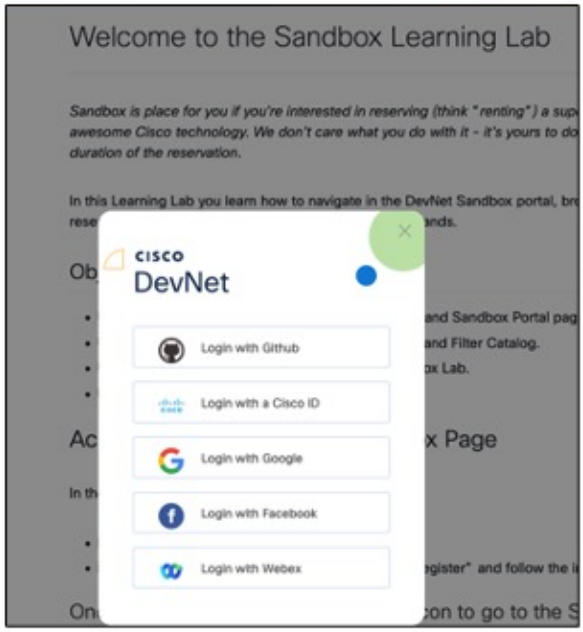
- CER = Crossover Error Rate
- EER = Equal Error Rate
  - Both terms are often interchangeable with each other
  - Metric used to determine the accuracy of an authentication system
  - Point at which the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are equal.
  - The lower the value the better

- In this case, by using the metric of CER we can see the Keystroke Analysis Method #2 is more accurate and a better choice.

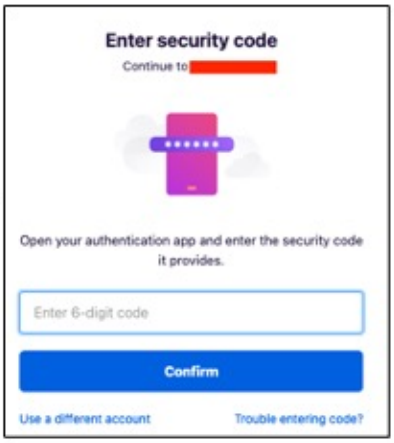
Multifactor Authentication

- A system may incorporate more than one method of authentication
  - Following a password an authentication token may be required
  - Following a fingerprint a password may be required
- This is called multifactor authentication
  - 2-Factor Authentication = Two authentication methods are used
  - 3-Factor Authentication = Three authentication methods are used
- The greater the “factor” = The stronger the authentication

Two-Factor Authentication Example



After supplying a password, the "2nd Factor" is presented



Authorization

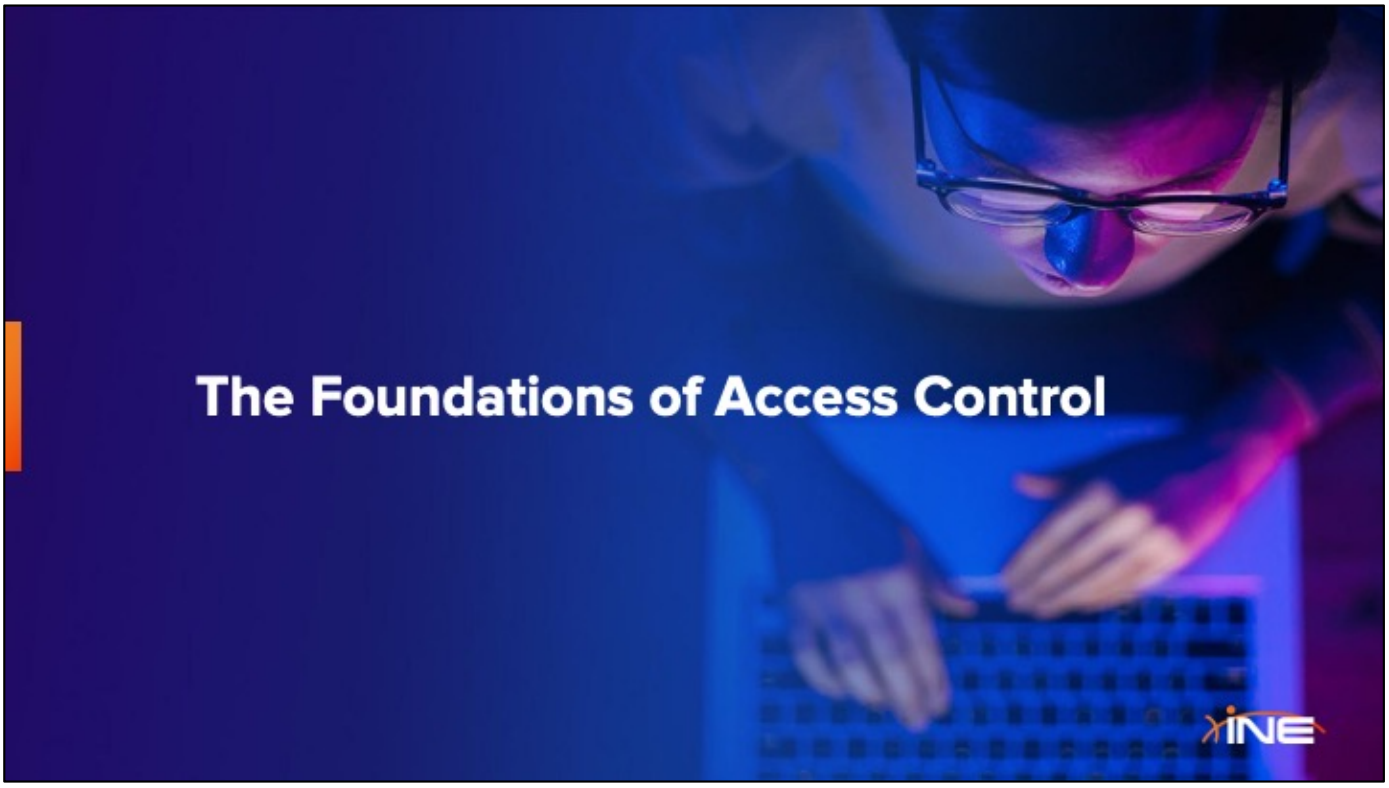
- Process of granting access rights to a subject for a given object or resource
- Dictated by rules created in access control models
- Authorization rules could be dictated by:
  - The object Owner
  - Business Management
  - Built-in OS rules
- Default authorization policy (if no matching subject/object rulesets apply) should be to deny access

Accounting

- Auditing and monitoring resource usage after a subject is authorized
- Tremendously helps with forensics after a cybersecurity breach has occurred
- Care should be taken that applications and protocols selected for authentication and authorization also provide sufficiently detailed accounting logs to be useful when troubleshooting.

```
11/12/2013 21:27:58: P6699: Packet received from 10.1.9.204
11/12/2013 21:27:58: P6699: Trace of Accounting Request packet
11/12/2013 21:27:58: P6699: identifier = 127
11/12/2013 21:27:58: P6699: length = 45
11/12/2013 21:27:58: P6699: reqauth = ed:d6:a6:ae:57:09:b8:55:a8:d4:c4:0d:f7:be:06:2a
11/12/2013 21:27:58: P6699: User-Name = bob
11/12/2013 21:27:58: P6699: NAS-Identifier = localhost
11/12/2013 21:27:58: P6699: Acct-Status-Type = Start
11/12/2013 21:27:58: P6699: Acct-Session-Id = 1
11/12/2013 21:27:58: P6699: Using Client: cubone (10.1.9.204)
11/12/2013 21:27:58: P6699: Using NAS: localhost (127.0.0.1)
11/12/2013 21:27:58: P6699: Request is directly from a NAS: FALSE
11/12/2013 21:27:58: P6699: Running NAS localhost (127.0.0.1) IncomingScript: Pa seServiceHints
11/12/2013 21:27:58: P6699: Rex: environ->get( "Request-Type" ) -> "Accounting-Request"
11/12/2013 21:27:58: P6699: Rex: environ->get( "User-Name" ) -> ""
11/12/2013 21:27:58: P6699: Rex: request->get( "User-Name", 0 ) -> "bob"
11/12/2013 21:27:58: P6699: Accounting with Service accserv1
11/12/2013 21:27:58: P6699: Trace of Accounting-Response packet
11/12/2013 21:27:58: P6699: identifier = 127
11/12/2013 21:27:58: P6699: length = 20
11/12/2013 21:27:58: P6699: reqauth = a6:40:45:02:4c:8b:6f:00:4f:18:4a:b8:fe:28:9d:f4
11/12/2013 21:27:58: P6699: Sending response to 10.1.9.204
```

Thank you for watching!

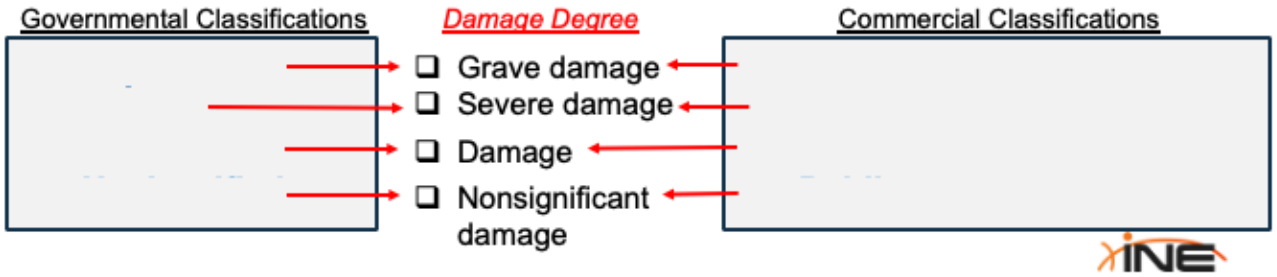


Access Control Policy Elements

- Access control policies consist of rulesets that govern:
  - The type of access to grant to an object (authorization)
  - Circumstances under which to grant that access (authentication)
- Several different access control models exist, but some foundational steps must be taken prior to selecting from a specific model.
- To design and implement an effective policy, the policy owner must:
  - Identify and categorize assets
  - Mark or tag assets for easy identification and application of rulesets
  - Define access policies to govern access to objects and the actions that can be taken against those objects
  - Define a data retention and disposal policy

Asset Classification Schema

- The first step in creating an access control policy is to create a *classification schema* which will be applied to assets/objects to determine:
  - The value of an asset/object
  - The business impact of unauthorized use.



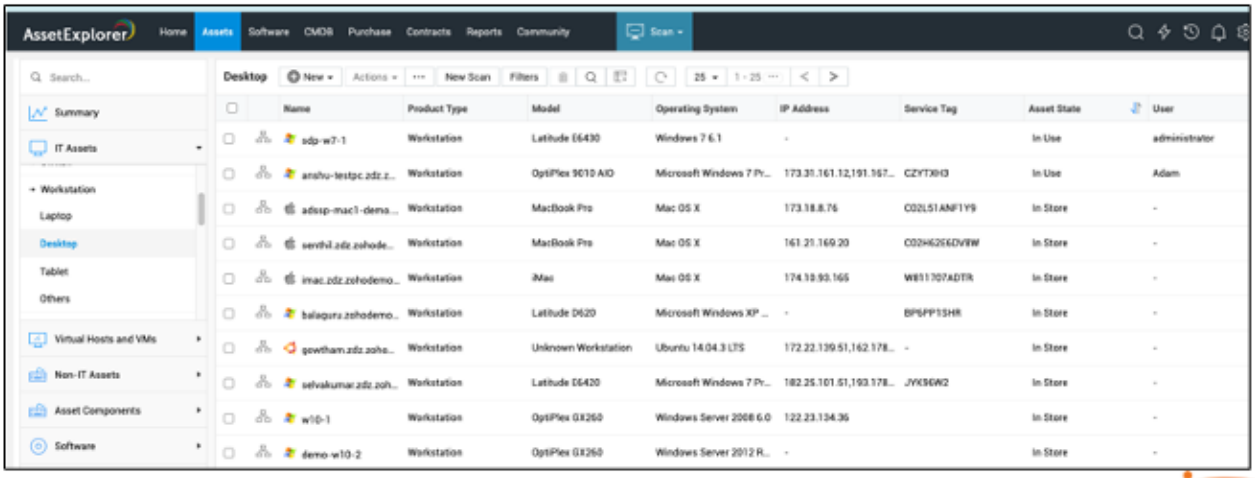
- Before you even start thinking about WHAT assets are in your company you have to think about HOW you will categorize them based on their value and secrecy. A classification schema is a ruleset you derive containing a generalized list of definitions that will later be applied to assets.
- Clearly understood definitions of each of the above should be created so it is clear which label should be applied to any given asset.
- Clearly defined rules should also be created to identify the circumstances under which a label for an asset no longer is applicable, and when/how/why a new label should be applied.

Asset Inventory

- The process of discovering and creating an inventory of your assets which could include:
  - Hardware (Computers, Servers, Printers, Network infrastructure, Safes, etc)
  - Software, files and data
- Tools can be used to accelerate and automate this process.
- Asset discovery and inventory tools can be cloud-based or on-premise.
- Examples of Asset Management Solutions include:
  - ServiceNOW
  - SolarWinds Web Help Desk
  - InvGate Assets
  - ManageEngine AssetExplorer

Asset Management Example

+ Demo available at: http://demo.assetexplorer.com



- The above is taken from an online demo of ManageEngine's AssetExplorer

Asset Marking

- Process of applying a mark, label, tag or other identifying feature to an asset so that its classification level is clear.
  - Applying a label reading “Top Secret” to a file
  - Watermarking a digital document with “Proprietary”
- Guidelines for asset labeling:
  - Each asset should be given a unique identifier
  - On physical assets, the identifier should be clearly visible
- Record detailed asset descriptions indicating intended use of the asset

- Choose a naming convention for assets that is consistent
- The identifier could also provide location information within the name

Hardware & Software Asset Marking

- For hardware devices record the following;
  - Manufacturer name, model and part number
  - Serial number and host name
  - Physical address
- For software you should record;
  - Publisher, version and revision
  - Department that purchased the software
  - Serial number or software key

Access Controls: Initial Design Considerations

- Access control policies are based on labels assigned to assets and objects
- The policy should include:
  - Who can access the data/asset/object
  - Under what conditions can they access it (Time of day? Location?)
  - What type of access can they have (Read? Write? Delete?)
- The policy should include details about how the data/asset will be protected while being accessed

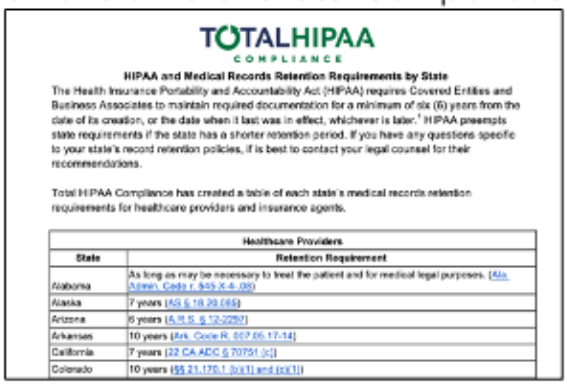
Data States

- Data defined in an access control policy can be in one of three states
- Definitions and rulesets must be created to protect data in any of these states:
  - *Data at rest*
    - Data residing on a hard drive, CD or other storage media
    - Usually protected by strong access controls and encryption
  - *Data in motion*
    - Data as it moves from Object to Subject
    - Usually protected by VPN and encryption techniques
  - *Data in use*
    - Data being processed by an application or program
    - Data stored in temporary registers or RAM

- Common attacks against “data in use” include:
  - Data breaches: Gaining unauthorized access to sensitive data by exploiting vulnerabilities in applications or user activities.
  - Privilege escalation attacks: Attackers leverage existing access to gain higher privileges and access sensitive data.
  - Malware injections: Injecting malicious code into applications or systems to steal or manipulate data in use.
- The same types of access controls applied against data at rest can be leveraged to protect data in use with the addition of logging and malware detection.

Data Retention Policies

- Organizations should create a "Data Retention Policy" which defines:
  - How data is to be saved for compliance or regulatory reasons
  - How records and data should be formatted
  - A data disposal policy
- Different types of records have different retention periods. Consider;
  - Personnel records
  - Financial records
  - Medical records



TOTALHIPAA COMPLIANCE

HIPAA and Medical Records Retention Requirements by State

The Health Insurance Portability and Accountability Act (HIPAA) requires Covered Entities and Business Associates to maintain required documentation for a minimum of six (6) years from the date of its creation, or the date when it last was in effect, whichever is later.[1] HIPAA preempts state requirements if the state has a shorter retention period. If you have any questions specific to your state's record retention policies, it is best to contact your legal counsel for their recommendations.

Total HIPAA Compliance has created a table of each state's medical records retention requirements for healthcare providers and insurance agents.

Healthcare Providers	
State	**Retention Requirement**
Alabama	As long as may be necessary to treat the patient and for medical legal purposes. (Ala. Admin. Code r. §45-X-4-.09)
Alaska	7 years (AS § 18.20.085)
Arizona	6 years (A.R.S. § 12-2297)
Arkansas	10 years (Ark. Code R. 007.05.17-14)
California	7 years (22 CA ADC § 70751 (c))
Colorado	10 years (§§ 21.170.1 (b)(1) and (c)(1))

Why Dispose of Data?

- "While deleting a file on an electronic device makes it invisible to the user, the information ***still exists on the device's memory chip or hard drive***.
- Data destruction entails making the data irretrievable, either by overwriting the current data with random data or destroying the electronic medium itself." – ***https://dataspan.com***

- The article from above comes from: https://www.techradar.com/news/millions-of-deleted-files-recovered-in-hard-drives-purchased-online-finds-research

Data Disposal Techniques

- Data disposal techniques fall into three categories
- **Clearing**
  - Ensures protection against simple and noninvasive data recovery techniques
  - Overwriting and File Deletion are examples
- **Purging**
  - Removing data from storage devices to a degree that makes recovery impossible using standard tools and techniques, including those used in laboratories.
  - Degaussing (exposure to strong magnetic fields) and cryptographic erasure (encrypting and then deleting the encryption keys) are examples
- **Destroying**
  - Physically damaging the storage media so that data recovery is not feasible by any means.
  - Incineration, crushing and pulverizing are examples

- Clearing methods are suitable when the storage media will remain within a controlled environment.
- Overwriting: Applying a software-based method to overwrite all areas of the device with nonsensitive data. This often involves writing a series of zeros (a single pass) or multiple passes of different patterns to obscure the original data.

To Help You Remember...

Image courtesy of:
https://degaussing-101.com/improper-it-asset-disposition-itad-is-a-risk-carried-forward-indefinitely-degaussing-101/

Thank you for watching!

Many Responsibilities = Many Roles

- As one starts to think about the logistics of building, maintaining, and monitoring an access control policy it quickly becomes clear that someone will need to...
  - Specify the requirements for the plan and be ultimately responsible for it
  - Design the plan according to the requirements
  - Decide on technical implementation details for the plan
  - Monitor its implementation and adherence
  - Adjust the plan and its implementation as needed
- For many institutions, it doesn't make sense for a single individual to be responsible for all of these tasks

Why We Need Roles

- Delineating Information Security Roles assists with;
  - Promoting accountability within the organization
  - Identifying who is ultimately responsible for each aspect of the policy
  - Reducing confusion
  - Assisting with balancing security requirements against business objectives
- Depending on an organization's size, a single individual may take on more than one role
- Despite anyone's role, protecting the security of assets is EVERYONE's responsibility

Common Roles: Execs & Data Owners

Well, as the Director of Payroll I'm responsible for that particular dataset and its accuracy, privacy, and security. I'll inform the other Directors about this initiative!

I'm ultimately responsible for our data and asset security. So, let's make a plan and put a new policy in place! I'll help you when I return from golfing.

Executives & Sr. Management

Hmm…I'm going to need to start thinking about what security protocols & rulesets I want…and how to categorize/classify my data!

Data Owner

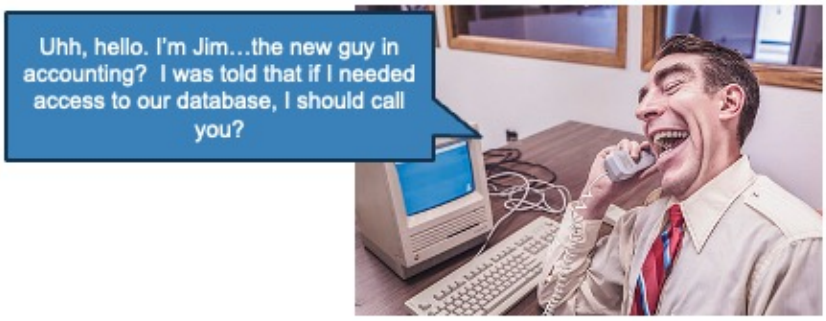
Responsible for:

- Determining who has access to their data (high-level)
- Classifying and tagging data
- Determining the risk level of their datasets
- Determine access control policies to be applied to their data (with Executive buy-in)

Tasked primarily with the "Governance" aspect of Access Control Policies

Image courtesy of Wannapik.com

Common Roles: Data Custodian

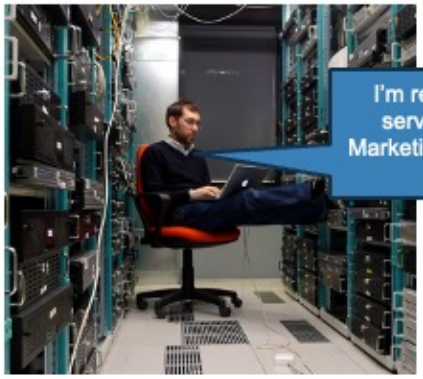


Data Custodian

- Responsible for maintaining and protecting the data.
- Implement and maintain security controls
- Perform regular backups of the data and restore data from backups
- Periodically validate the integrity of the data
- Retain records of activity

- This role is usually filled by the IT or security department
- They will figure out how to technically implement the policy dictated by the Data Owner.
- When you get locked out of an information system at work, who do you call?
- When you need access to a new database or credentials for a new application…who do you call?
- Whoever that is…that is your Data Custodian.

Common Roles: System Owner



System Owner

Responsible for:

- Security of systems that handle and process information
- Ensure that data is secure while it is processed by their system
- Work closely with Data Owners & Data Custodians to determine appropriate controls

- In this context, the main thing that makes the System Owner different from the Security Administrator is that the System Owner is primarily responsible for the Servers (real or virtualized) that house the data whereas the Security Admins handle the infrastructure connecting those servers to the end user's machines.
- While the Data Custodian will install and configure the appropriate software and security features to implement rules defined in the access control policy, the system owner will ensure that the software selected (and any hardware requirements it may have) are fulfilled by the physical (or virtual) servers and that the servers themselves are protected.

Common Roles: Security Administrator

We're going to need some more routers to handle the extra IPsec tunnel overhead to reach our new Azure resources!

Security Administrator

- Responsible for implementing and maintaining *specific security network devices and software* in the enterprise.
- These controls commonly include firewalls, IDS, IPS, antimalware, security proxies, data loss prevention, etc.

Common Roles: End User

End User

SUPPOSED to:

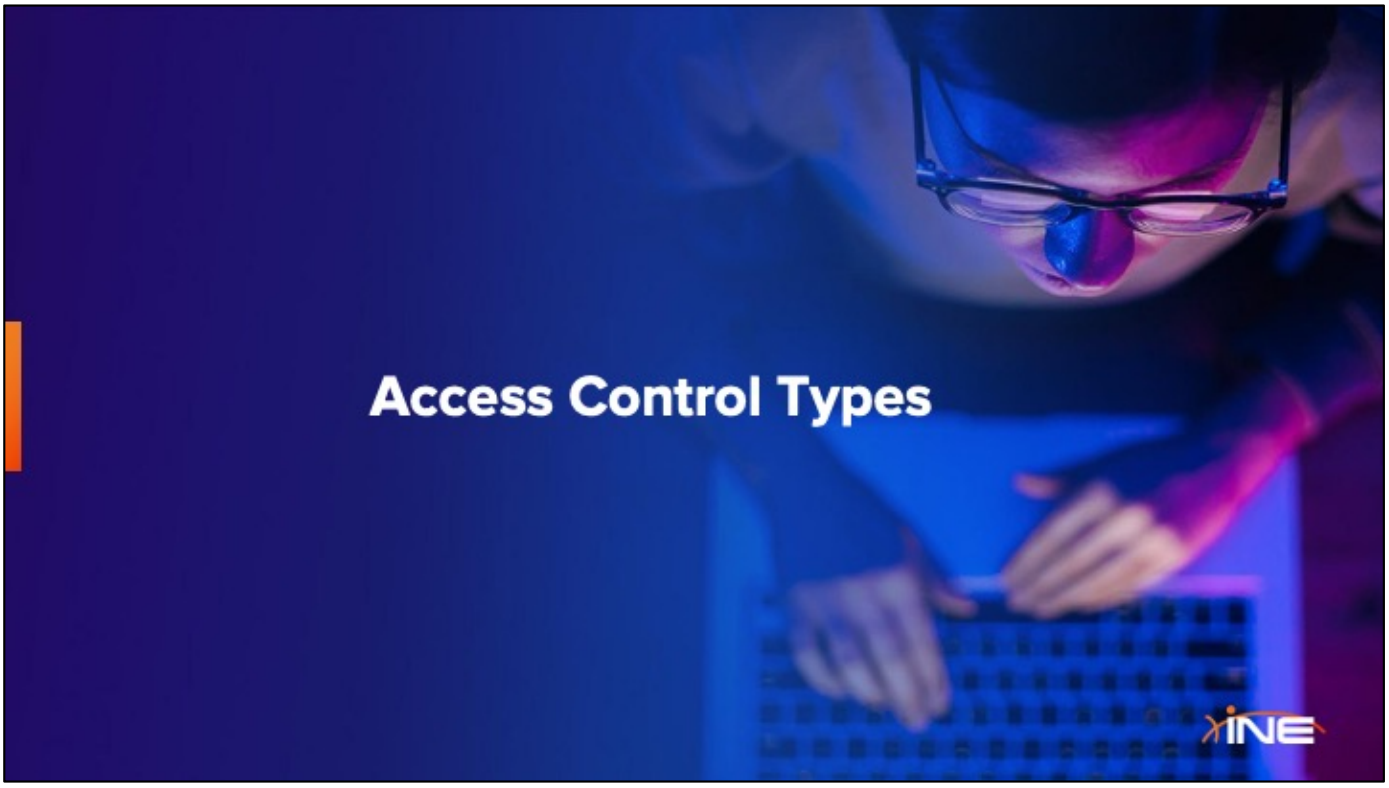
- Adhere to company security policies
- Work without complaining

Need More Roles?

- NIST Special Publication (SP) 800-181 provides a "framework" for the creation of new job roles
- Each job role description should be paired with relevant TKS:
  - Tasks
  - Knowledge
  - Skills
- Many Work Roles defined by NICE already exist

- National Initiative for CyberSecurity Education (NICE)

Thank you for watching!



Introduction to Access Control Categories

- Access control models fall into three different categories that are based on how the controls will be derived and implemented.
- Knowing each category, and the objective for that category, helps ensure you haven't missed anything critical when designing and implementing your access control policies.
- Those categories are:
  - Administrative controls
  - Physical controls
  - Technical controls

Administrative Controls

- Controls concerning policies, procedures, and guidelines that dictate how the organization manages and implements its security posture *through human actions or organizational methods*.
  - Defining what resources are important and how they are to be classified
  - Identifying who can access those resources and to what degree
  - Specifying where the resource is to be located and circumstances under which authorized access can take place
  - Defining when access to the resource is permissible
- Any actual implementation of administrative controls ***that requires the use of technology*** falls under a different categorization of control.

Examples of Administrative Controls

- Employee Security, Clearance, and Evaluation
- Employee training and awareness, etc.
- Privilege Management
- Change Control Policies
- Information Classification
- Data Retention and Disposal Policies
- Auditing and Monitoring Policies

Technical Controls

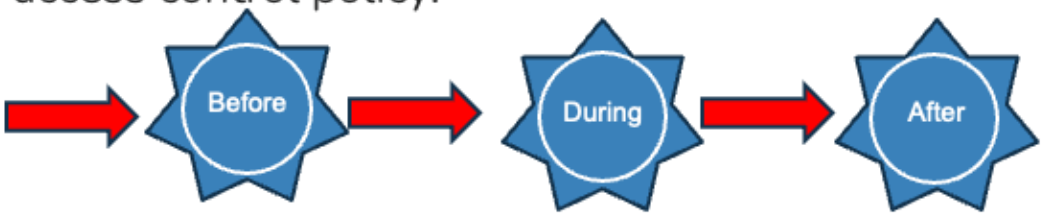
- Controls that *involve the use of technology* to enforce security policies and protect information assets.
  - Sometimes called, "Logical Controls"
- Examples include:
  - Authentication and authorization systems (software, databases, etc)
  - IDS and IPS systems
  - Firewalls
  - Security protocols configured on network infrastructure devices
  - Encryption of data (at rest or in-transit)

Physical Controls

- Security controls which are implemented physically to prevent unauthorized access to facilities, resources and systems that house data.
- Examples include:
  - Locks, keys, and keypad systems
  - Surveillance Cameras
  - Security Guards
  - Fencing and Barriers
  - Locked data center cages

The Attack Continuum

- The *Cisco Attack Continuum* identifies three points in time that must be considered when designing and implementing an access control policy:

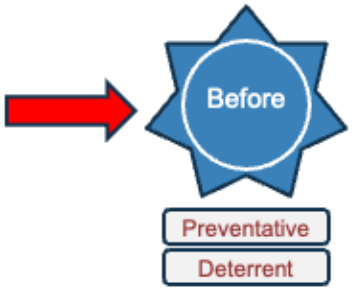


- Effective and wholistic access control policies should contain controls that are deal with each point within the attack continuum.

Preventative Controls

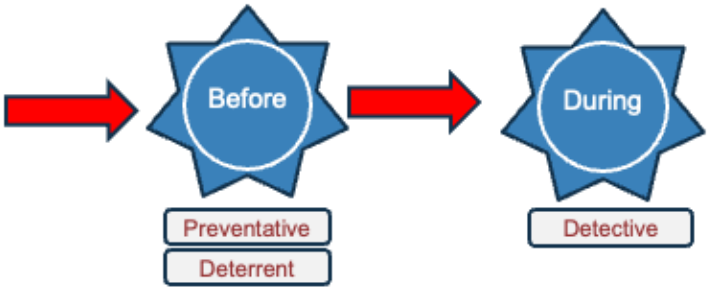
- Preventative Controls
  - Designed to prevent attacks *before* they begin
  - Enforce the security policy to prevent unauthorized access or authorization
  - May be visible or invisible to end users
  - Examples include; access-lists, identification enforcement mechanisms and physical controls.

Deterrent Controls



- Deterrent Controls
  - Designed to prevent attacks *before* they begin ***by discouraging a potential attacker***
  - Visible to end users
  - Examples include; system banners, warning popups after unsuccessful login attempts, physical signs, video surveillance equipment

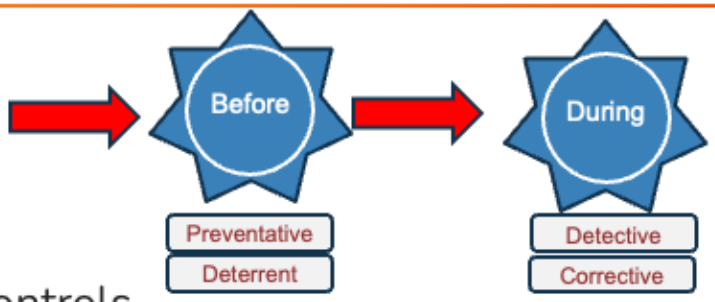
Detective Controls



- Detective Controls
  - ***Your preventative and deterrent controls have failed, and an attack is in-progress***, how do you find out about this? Detective controls.
  - Monitor, detect and log information about attacks in-progress.
  - Examples include; Audit logs, IDS systems, File Integrity Monitoring, Motion Detection and S.I.E.M systems

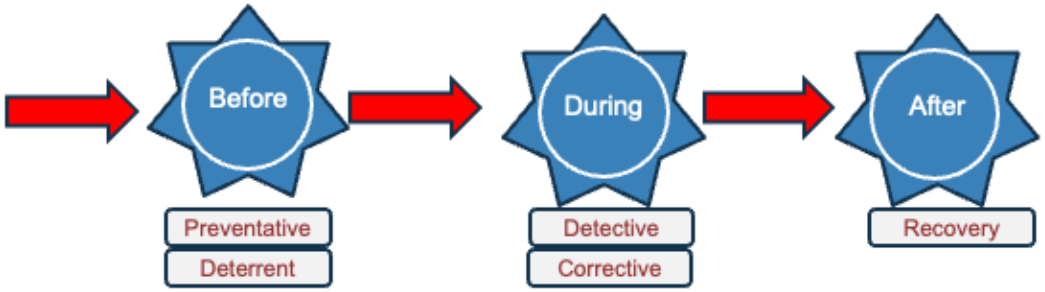
- S.I.E.M. stands for Security Information and Event Management. These are systems designed to collect massive amounts of logs and streaming data from your network and end systems and (often by using A.I.) apply meaning to all that massive data, offer logical insights and potentially provide suggestions for remediation.

Corrective Controls



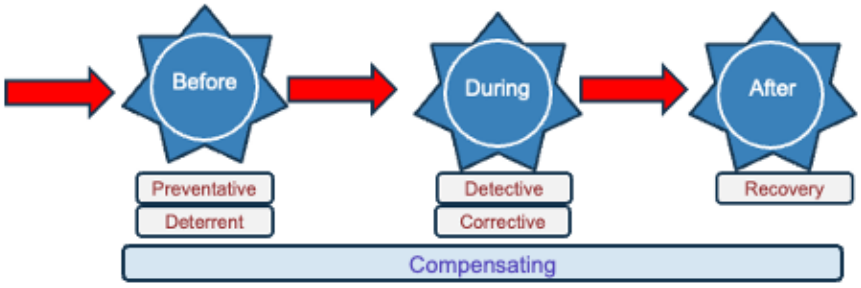
- Corrective Controls
  - Controls used during an incident to correct the problem and prevent it from getting worse.
  - ***Designed to mitigate and contain damage.***
  - Examples include; Incident Response Procedures, Quarantining an infected system, terminating an employee for not following security procedures,

Recovery Controls



- Recovery Controls
  - Designed to **restore** information systems, data, and operations **to a secure, operational state** following a security breach, system failure, or disaster.
  - Examples include; Performing (and recovering from) data backups, Implementing Redundant Systems, and Creating a Disaster Recovery Plan.

Compensating Controls



- Compensating controls
  - Alternative or backup controls to be used either as a stopgap when the primary controls haven't been implemented yet, or if a primary control has failed.
  - These are not your primary controls but compliment the primary controls
  - Examples include; Placing a security guard in front of your door while the badge reader is down, Providing read-only access to files if the authentication database becomes unresponsive

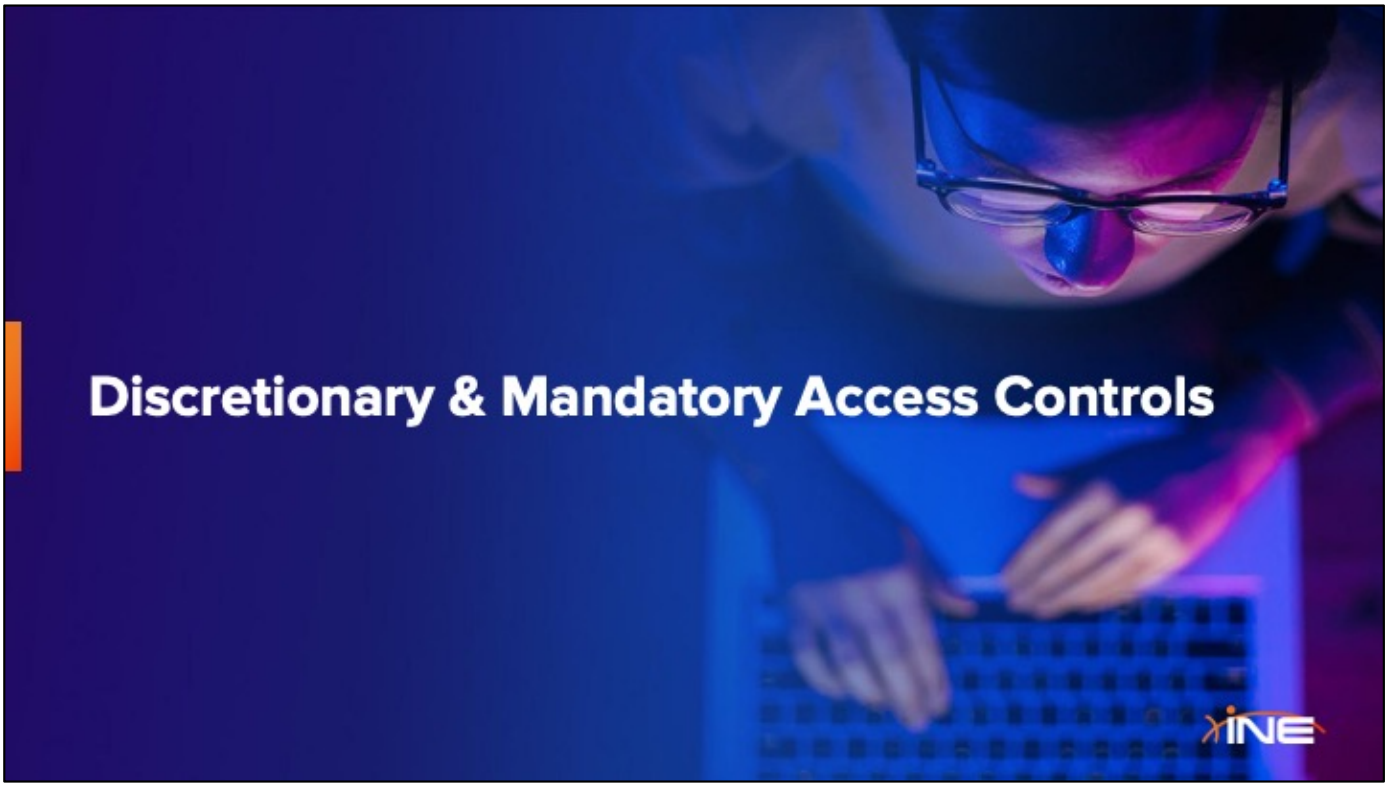
- Courtesy of ChatGPT: Compensating Controls are ecurity measures that are implemented as alternatives to the standard controls that may be impractical or impossible to deploy in a given environment. They are designed to provide equivalent or comparable protection to the original requirement, ensuring that the overall security posture and compliance objectives are maintained even when primary controls cannot be applied.

In Summary

- Access control models fall into three, high-level categories depending on if they are primarily theoretical and design-based (Administrative) or implementation-centric (Technical and Physical).
- Specific controls defined in access control models can be characterized (such as Preventative, Detective, and Recovery) based on which part of the Cisco Attack Continuum they are designed to address.
- Some access controls might fall into more than one category.

- An access-control list could be categorized as a Preventative control as well as a Deterrent if the potential attacker knows in advance that the ACL exists. It could also serve as a Detective Control if the ACL is logging hit counts.

Thank you for watching!

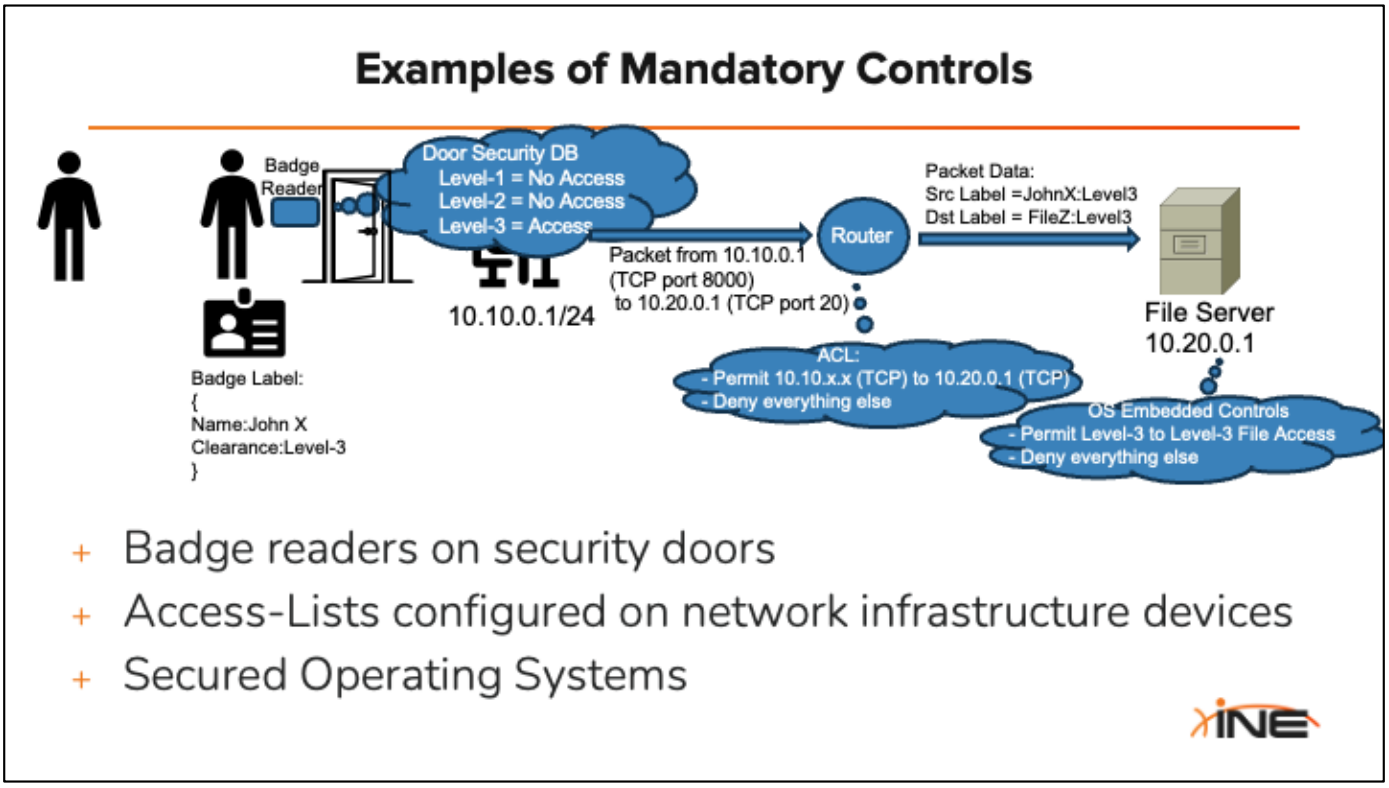


Reviewing Access Control Definitions

- Access control models define the need for, scope of, and implementation requirements for one or more access controls
- Access controls govern the security relationship between subjects and objects
- Access controls can be implemented as;
  - Administrative controls
  - Technical controls
  - Physical controls
- All controls fall into one of two categories;
  - Mandatory Access Controls
  - Discretionary Access Controls

Mandatory Controls

- Mandatory access controls are defined by upper management or senior executives.
- They are implemented in such a way that end users must adhere to them and cannot modify them.
- They are applied against the pairing of subject and object security labels or tags, and not specific objects themselves.
- Very secure but not very flexible

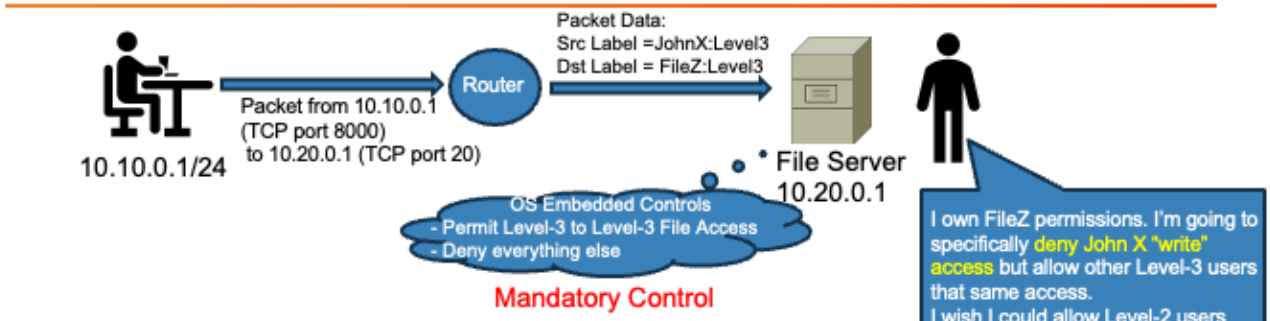


- What makes each of these “mandatory access controls”?
  - The subject (John X) who is interacting with the objects (badge reader, ACL, or File) doesn’t have the ability to modify or set any access permissions. He is restricted by mandatory permissions that have already been designed by upper management and implemented as physical or technical controls.
  - The owner of the object (whoever owns the file that John X is trying to access) does not have permissions to grant or deny people with Level-3 access to Level-3 files. That permission is strictly determined by a comparison of labels performed in the secure OS of the File Server.

Discretionary Controls

- Discretionary access controls are controlled by the object owner.
- They are implemented in such a way that they must conform to any existing Mandatory controls.
- They are applied directly against the object.
- Less secure but very flexible.

Examples of Discretionary Controls



+ File permissions
+ Database Access Controls
+ Shared Folders
+ Email Filters and Rules

- Think of Google Drive and Dropbox. Mandatory controls specify that you must first login to those platforms, and you (the owner of the objects within Google Drive or Dropbox) can't change that restriction.
- However, after you pass that mandatory control, you can specify your own Discretionary controls on your own files within those platforms.

Where are these defined?

+ Mandatory and Discretionary Access Control definitions can be found in the U.S. Department of Defense (DoD) document, "Trusted Computer System Evaluation Criteria" (aka the "Orange Book")

5.3.1.2 Discretionary Security Policy

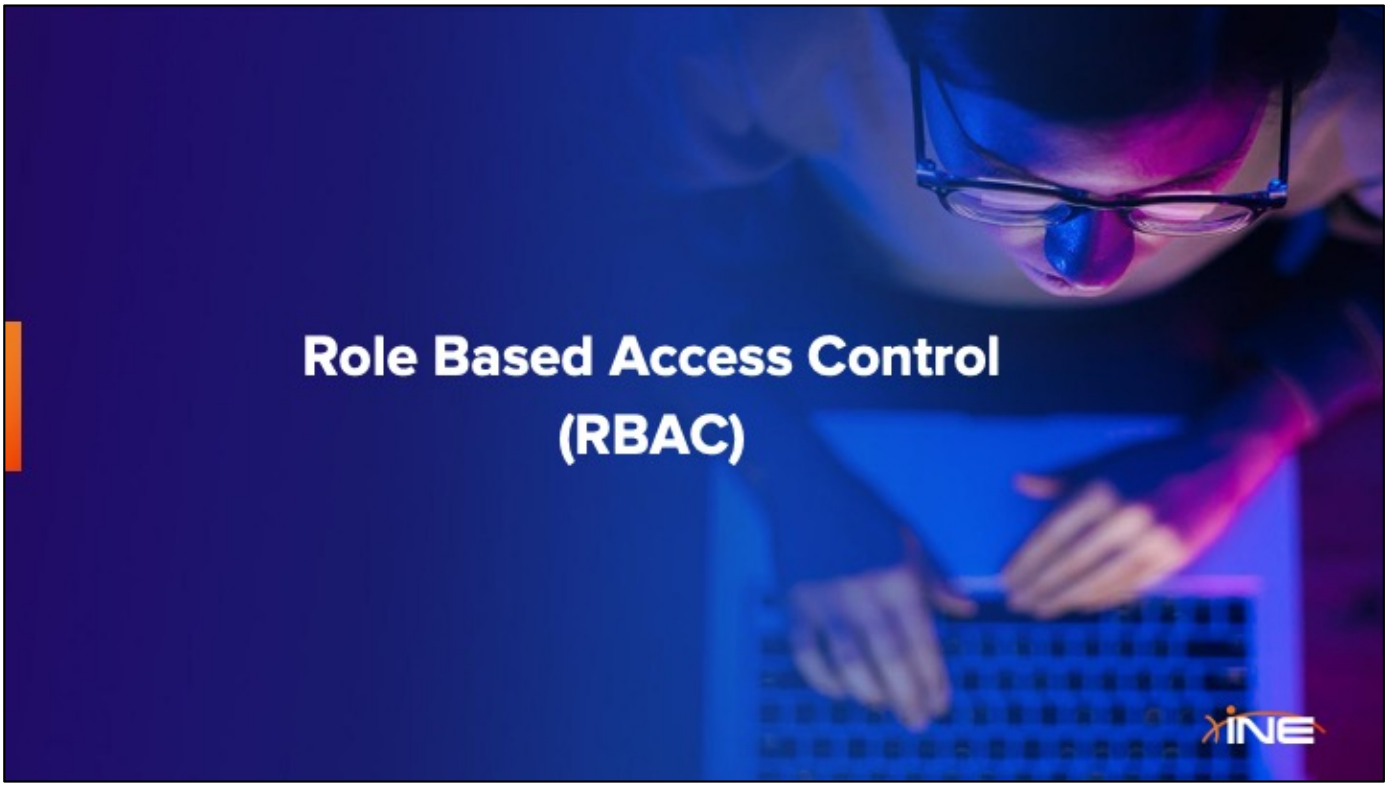
Discretionary security is the principal type of access control available in computer systems today. The basis of this kind of security is that an individual user, or program operating on his behalf, is allowed to specify explicitly the types of access other users may have to information under his control. Discretionary security differs from mandatory security in that it implements an access control policy on the basis of an individual's need-to-know as opposed to mandatory controls which are driven by the classification or sensitivity designation of the information.

MANDATORY SECURITY CONTROL OBJECTIVE

Security policies defined for systems that are used to process classified or other specifically categorized sensitive information must include provisions for the enforcement of mandatory access control rules. That is, they must include a set of rules for controlling access based directly on a comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information being sought, and indirectly on considerations of physical and other environmental factors of control. The mandatory access control rules must accurately reflect the laws, regulations, and general policies from which they are derived.

- Please note that the Orange Book was created in 1985 and has since been superseded by other documents. However, none of the newer documents formally defined the concepts of "Mandatory Access Controls" and "Discretionary Access Controls" so we still need to refer to this old document to obtain those definitions.

Thank you for watching!



Discretionary Control Challenges

- Discretionary access controls often associate file permissions to individual users.
- While this provides great flexibility, it is not scalable and can be prone to error
- RBAC (Role Based Access Control) is a type of discretionary access control that provides a scalable alternative.
  - Users are assigned to one or more roles
  - Object permissions are assigned to roles, rather than users

- Depending on how RBAC is implemented and the location/accessibility of the authorization source, RBAC could also be considered a form of Mandatory Control.

RBAC Reference Model Overview

- RBAC was formally defined in *ANSI INCITS 359-2004*
- The RBAC Reference Model consists of four model components
  - Core RBAC (required in all RBAC systems)
  - Hierarchical RBAC (optional)
  - Static Separation of Duties Relations (optional)
  - Dynamic Separation of Duties Relations (optional)
- In RBAC terminology an RBAC "session" is when a subject is assigned to one or more roles while attempting to gain access to an object

- INCITS 359-2004 was updated in 2012 so if you want to read that document, search for INCITS 359-2012
- The Cisco CyberOps Associate Certification Guide states that the RBAC standard defines "three" components. This is probably because both "Static Separation of Duties" and "Dynamic Separation of Duties" fall under the (book) category of "Constraint RBAC". But this actual type of RBAC is not mentioned in the original standard.

Core RBAC Elements

+ Core RBAC consists of five "elements" which must be recognized and implemented in every RBAC solution:

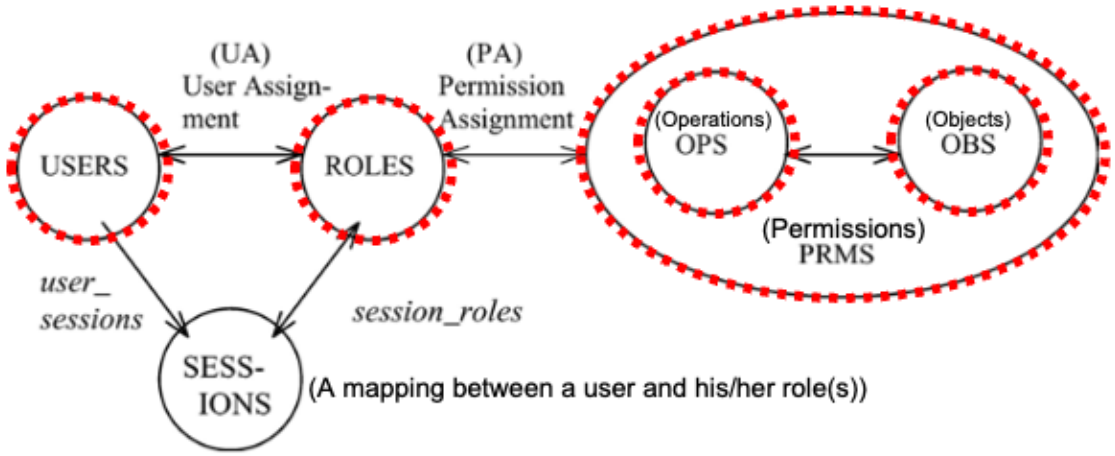


Figure 1: Core RBAC
Image courtesy of ANSI INCITS 359-2004

- Within the standard a "Role" is defined as a job function…but in reality, any arbitrary value can be used as a role if that value is clearly defined within your security policy.
- An "Operation" is the action that the user/role is attempting to take upon the Object such as Read, Write, Execute or Delete
- A "Permission" is an approval to perform an operation on one or more RBAC protected objects (that's why its circle encompasses the OPS and OBS circles)

Many-to-Many

- Core RBAC supports a many-to-many model
  - A single user can be assigned to one or more roles
    - Bob belongs to the roles of "Executives" and "Payroll"
  - A single role can be assigned to one or more users
    - The role of "Payroll" is given to Bob, Sally, Rohit and Brian
  - Multiple roles can be assigned the same (or different) permission levels as related to Operations that can be performed against an Object

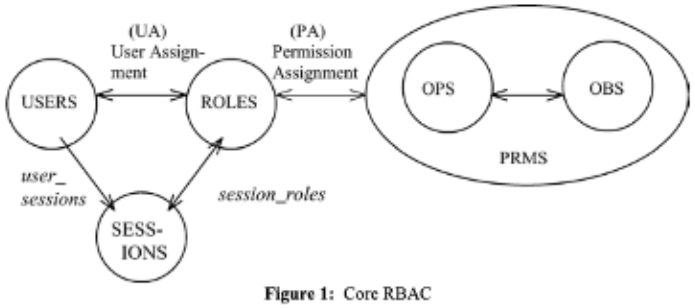
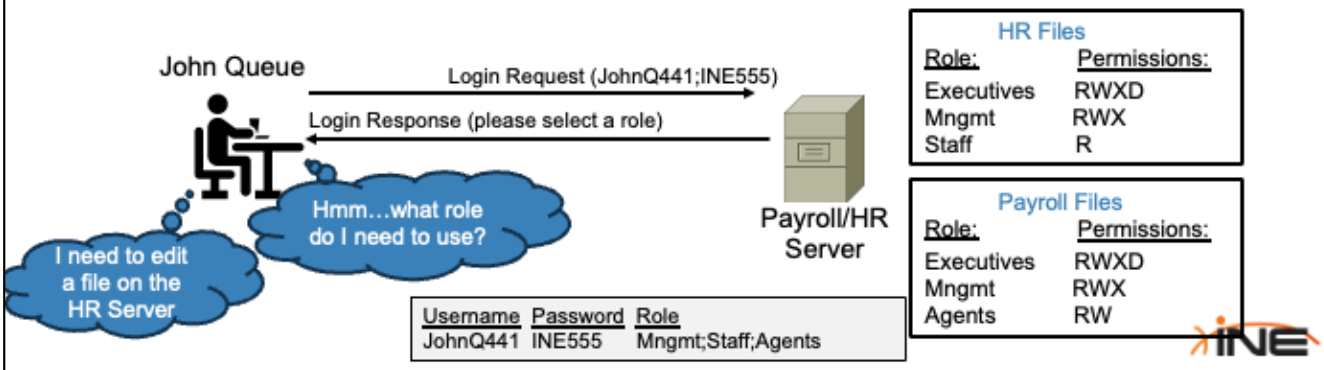


Figure 1: Core RBAC

- If an RBAC system is only implementing Core RBAC functionality (with zero relationship or hierarchy between Roles) this can also be said to be running "Flat RBAC".

Core RBAC Challenges

- With a system that only implements Core RBAC, users assigned to multiple roles must:
  - Remember what roles they can utilize
  - Remember the credentials to access that role
  - Remember which roles are required for specific object permissions

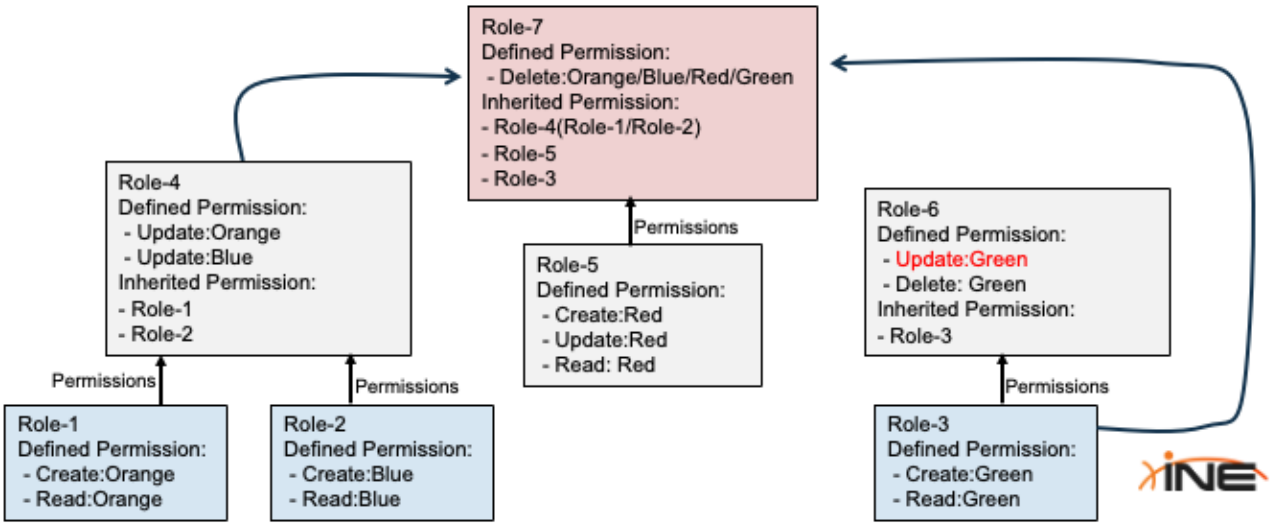


Hierarchical RBAC

- Hierarchical RBAC is an optional module for RBAC
- Allows roles to be associated to each other following a hierarchy
  - Roles can be designed an implemented that match organizational charts
  - Upper-level roles inherit the privileges of associated lower-level roles
- RBAC INCITS standard supports two role hierarchies;
  - General Role Hierarchies
  - Limited Role Hierarchies (aka “Restricted Hierarchical RBAC”)

General Role Hierarchy RBAC

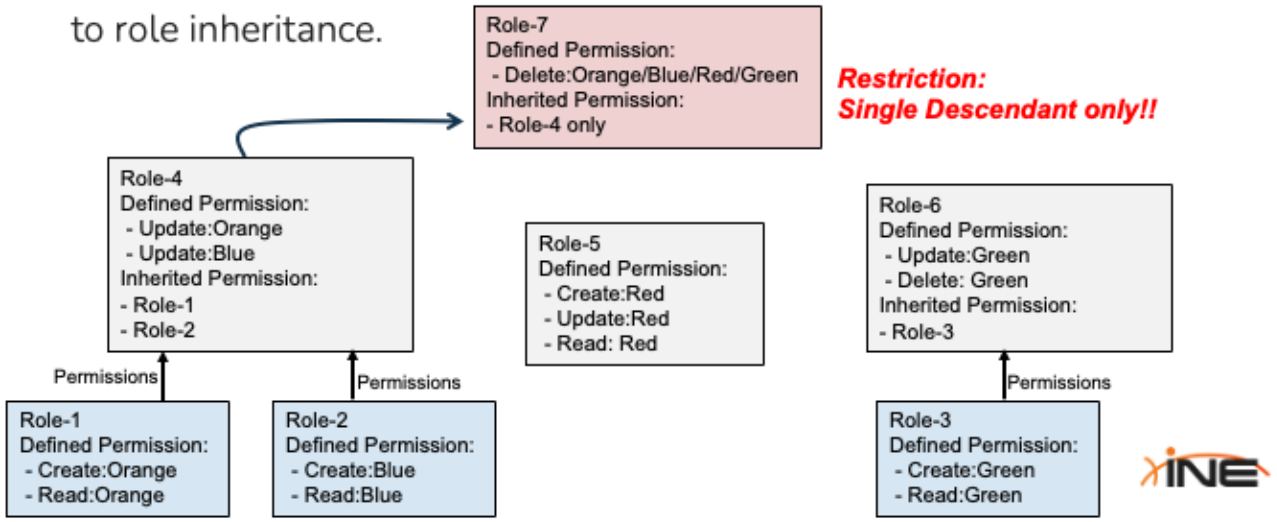
+ Systems that implement General Role Hierarchies are the most flexible and don't adhere to any pre-defined structure.



- Note that given this artificial structure, Role-7 will not be able to perform any "Update" action on Green files because Role-7 has not listed Role-6 as a "descendant" role.

Restricted Role Hierarchical RBAC

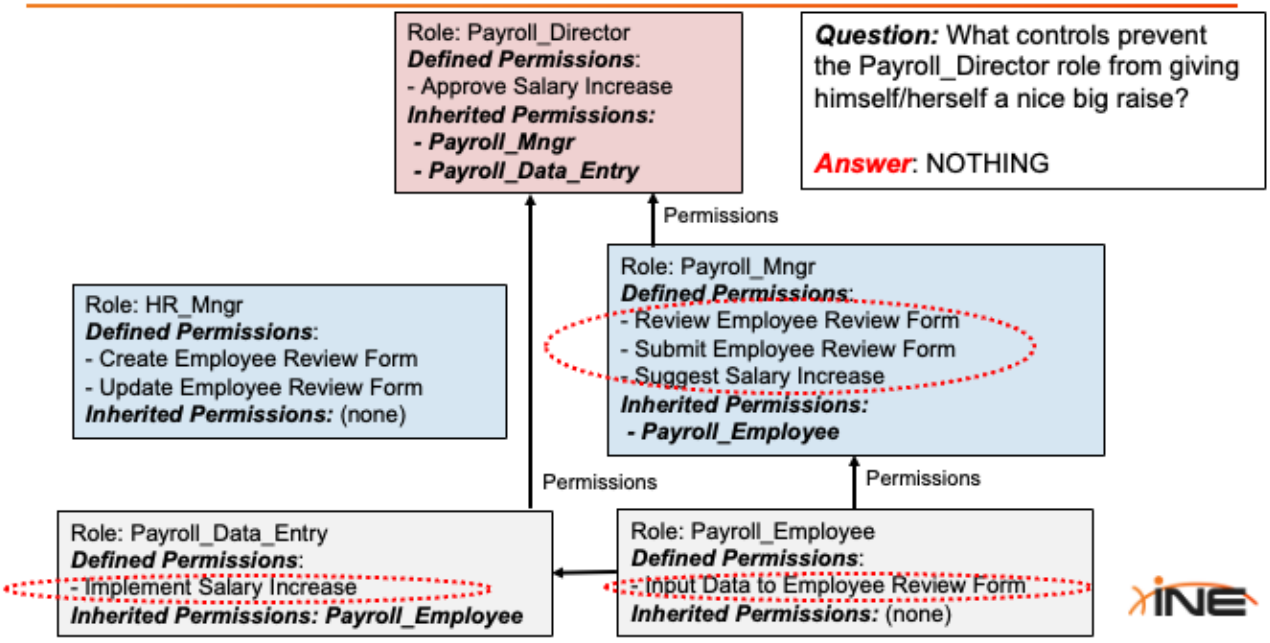
+ Systems that implement Restricted/Limited Role Hierarchies impose some kind of restrictions on the topology that can be used with regards to role inheritance.



- The original standard stated that a Restricted role hierarchical RBAC means that an upper role can only inherit permissions from a single descendant role. However, over time this type of RBAC has come to mean any implementation that places any kind of restrictions on how you create inheritances between roles.
- In this example, if only a single descendant (eg., single lower-level role) is allowed, then Role-7 can inherit the defined permissions of Role-4 but CANNOT inherit the permissions of Role-1 or Role-2.
- The document titled, “The NIST Model for Role-Based Access Control: Towards A Unified Standard” reads, “Some systems may impose restrictions on the role hierarchy. Most commonly, hierarchies are limited to simple structures such as trees or inverted trees.”

Thank you for watching!

The Problem With Hierarchical RBAC



Constraint RBAC

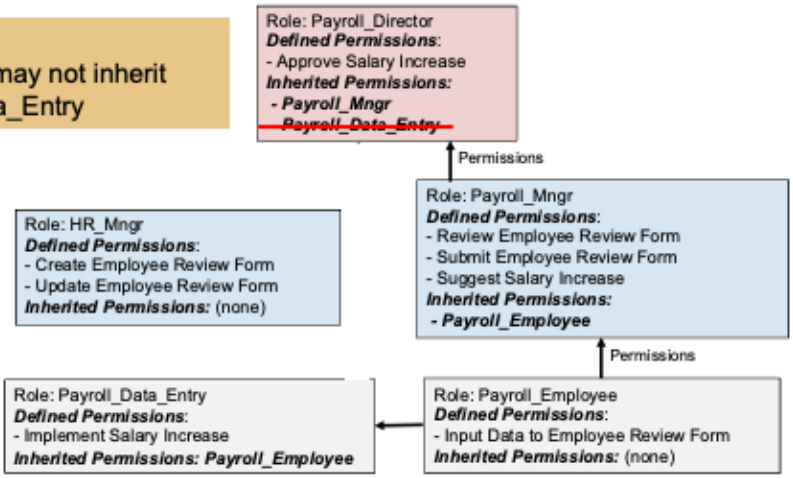
- RBAC implementations that impose some kind of constraint against associating users with certain roles is called "Constraint RBAC".
- Two ways exist of implementing this:
  - Static Separation of Duties
  - Dynamic Separation of Duties
- Main goal is to "avoid collusion and fraud" by dividing the permissions to accomplish a critical task among multiple roles or users.

- Per ANSI INCITS 359-2004, "The motivation is to ensure that fraud and major errors cannot occur without deliberate collusion of multiple users"

Benefits of Constraint RBAC

- Constraint RBAC prevents unauthorized actions by:
  - Implementing critical tasks with multiple roles (Separation of Duties)
  - Preventing certain roles from inheriting the permissions of other roles

Role Rules:
Payroll_Director may not inherit from Payroll_Data_Entry



Static Separation of Duties

- SSOD (Static Separation of Duties) Enforces constraints on the assignment of Users to Roles
  - Enforces rules that prevent a single user from being assigned roles that have conflicting responsibilities or permissions.
  - Also limits permission inheritance between roles
- SSOD Occurs at the time Roles are created and users are authorized for those roles ***within RBAC database/system***.

Ruleset:

- **No pairings between Permission-X and Permission-Y**
- **No pairings between Permission-Y and Permission-Z**

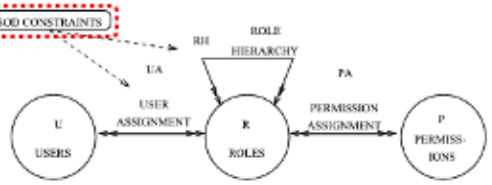
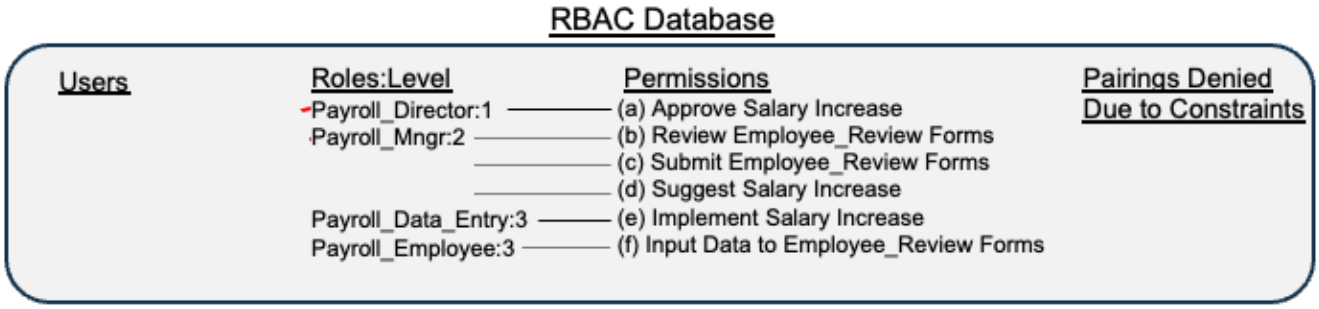


Figure 6: Constrained RBAC—Static SOD

NIST Publication 916402

Static Separation of Duties Example

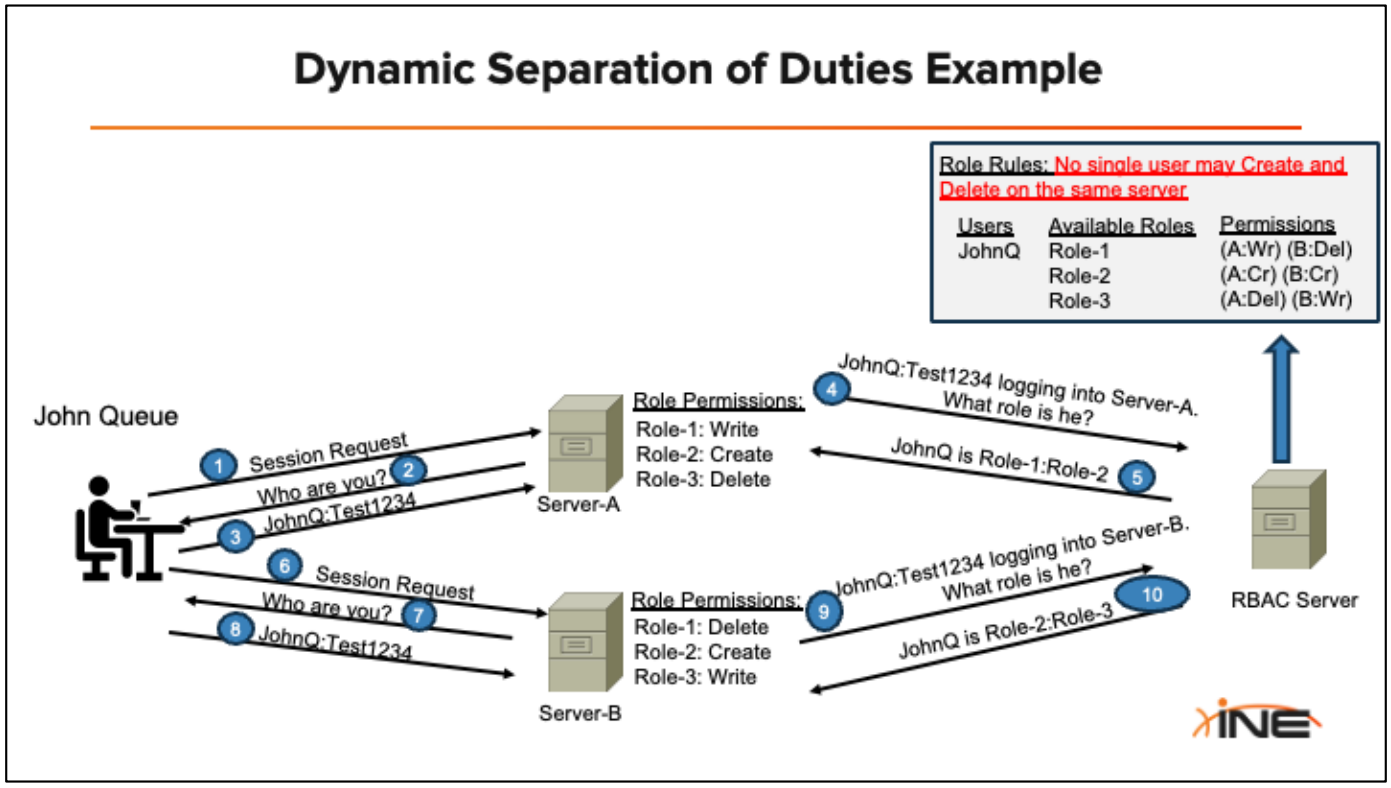
+ In the example below, due to static constraint rules, no user will ever be authorized for both the "Payroll_Director" and "Payroll_Data_Entry" roles.



- From our previous example, without the availability of the role "Payroll_Data_Entry" the user will never be able to have the associated permissions ("Implement Salary Increase") so there is no way this user can give themselves a pay raise.
- In this example, even if (elsewhere in the database) a permission inheritance was configured between Payroll_Mngr and Payroll_Employee, Kbogart88 will not inherit the permissions of Payroll_Employee because that particular role is not a part of this person's available roleset.

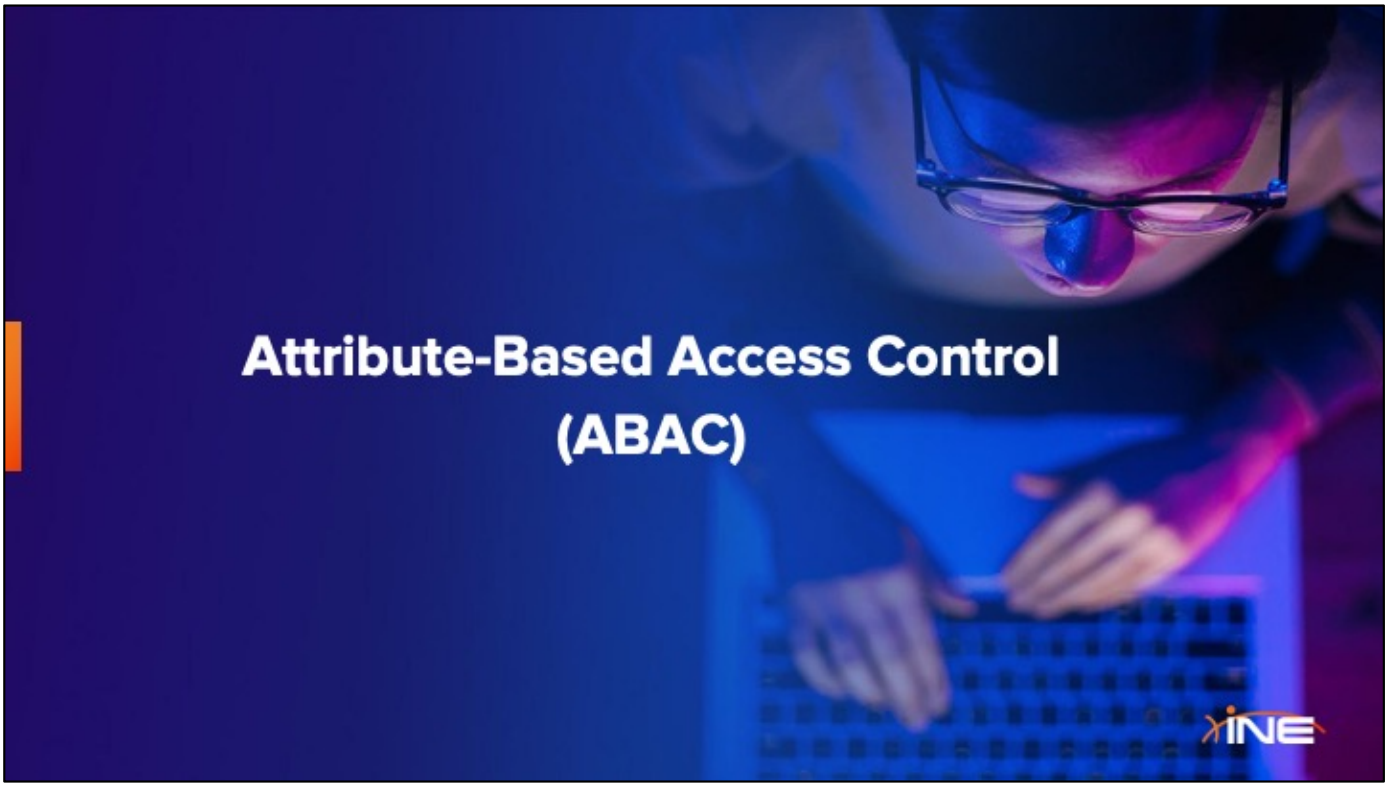
Dynamic Separation of Duties

- DSOD (Dynamic Separation of Duties) Enforces constraints on the assignment of Users to Roles *at time of session creation*
- From NIST document 916402: ***"(allows) a user to be authorized as a member of a set of roles which do not constitute a conflict of interest when acted in independently but produce policy concerns when allowed to be acted in simultaneously."***



- In order for this system to work, the RBAC server would obviously need to also understand the permissions assigned to each role so that it could dynamically allocate them appropriately.
- If John attempted to login to Server-B he could not use the same roles as before (Role-1 and Role-2) but instead would be assigned Role-2 and Role-3.

Thank you for watching!



Problems Solved by ABAC

- RBAC (Role Based Access Control) systems are great for scalability as multiple users can share a common role.
- IBAC (Identity Based Access Control) systems provide more granular control over access than RBAC but are not as scalable.
- Some situations require more granular and dynamic classification mechanisms applied against access control than either IBAC or RBAC can provide.
- *Attribute-Based Access Control (ABAC)* is an evolution of IBAC and RBAC.

ABAC Definition

- ABAC definitions can be found in NIST Special Publication 800-162
- Per NIST SP 800-162 (emphasis added);

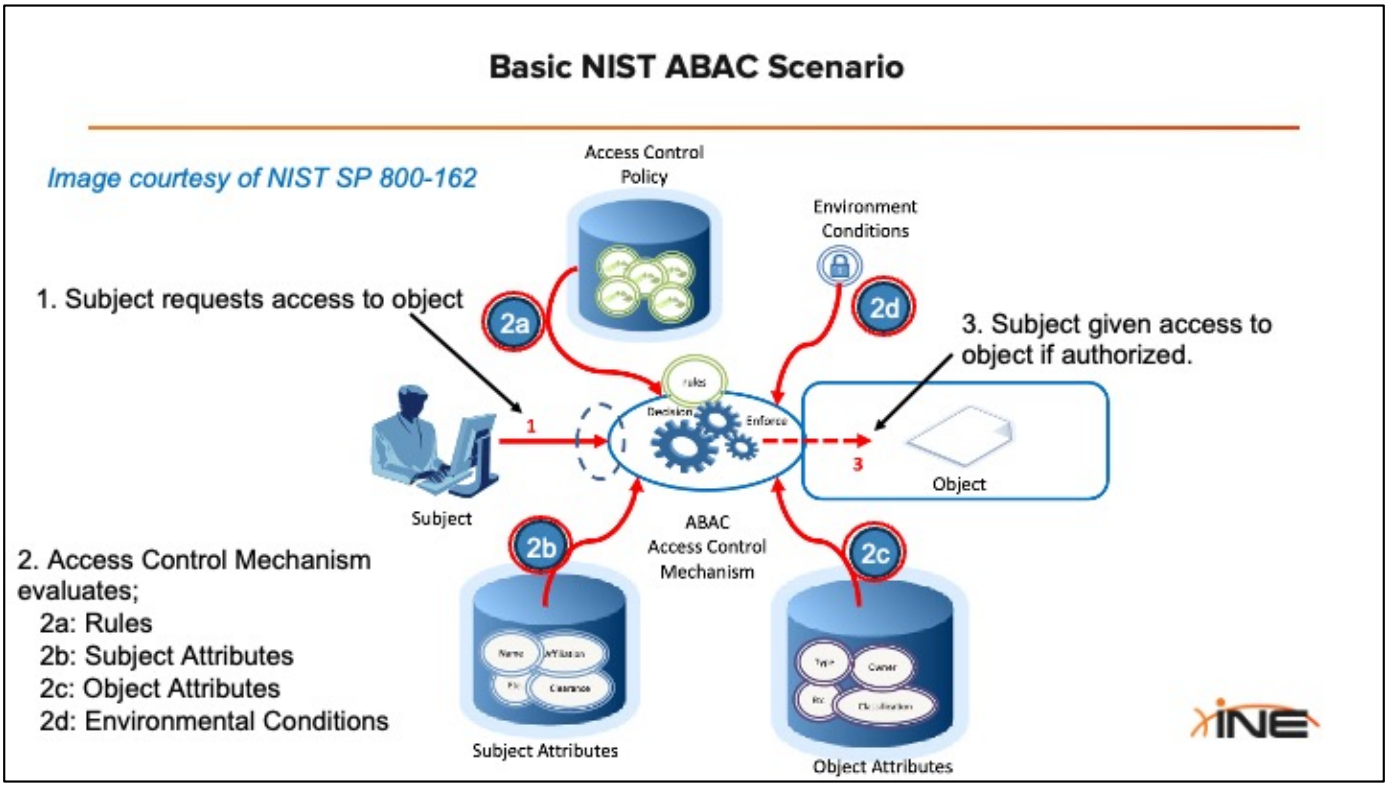
  "ABAC is a logical access control methodology where ***authorization*** to perform a set of operations *is determined by evaluating attributes* associated with
  - The subject
  - The object
  - Requested operations
  - ...and, in some cases, environment conditions

  ...against policy, rules, or relationships that describe ***the allowable operations for a given set of attributes***."

Example ABAC Attributes

- Examples of subject-based attributes include;
  - Name
  - Role
  - Organization
  - Security clearance
- Examples of object-based attributes include;
  - Name
  - Owner
  - Data creation
  - Data type
- Examples of environmental attributes include;
  - Current Location
  - Time of Day
  - Device Security Status
  - Resource Load

- Device security status would reference the security posture of the device being used to request access, such as whether it has updated antivirus software, is encrypted, or meets certain compliance requirements, can influence access decisions.



- The “gears” next to the word “Decision” in the middle of the diagram would be considered the PDP (Policy Decision Point) in ABAC terminology.
- The “gears” next to the word “Enforce” in the middle of the diagram would be considered the PEP (Policy Enforcement Point) in ABAC terminology.

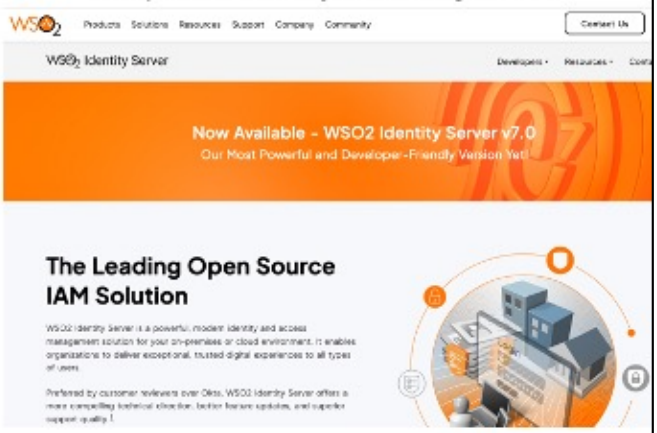
Example ABAC Policy

- ABAC policies can be described textually such as;
  - *All Engineers who work in the Routing Business Unit and are working on the 4500-RTR Project are allowed to Read and Update all the Functional-Specification documents in the "4500-RTR" folder when connecting between the hours of 8:00am and 6:00pm.*
- The above example contains the following attributes;
  - Subject Attributes
  - Object Attributes
  - Environmental Attributes

A Practical Example of ABAC

+ eXtensible Access Control Markup Language (XACML) is a standard that facillitates the ABAC model.
+ Defined by OASIS (Organization for the Advancement of Structured Information Standards) for expressing access control policies.
+ A framework for defining access control policies in XML format.
+ Can be complex to implement and manage

Example of an ABAC system utilizing XACML



- The WS02 Identity Server is an example of a system that utilizes XACML.
- OASIS is an international consortium that works on the development, convergence, and adoption of open standards for the global information society.
- When it comes to ABAC…what is the difference between NIST 800-162 and OASIS?
    - The NIST special publication defines the overall architecture of ABAC and provides general guidance on how to implement it. So NIST is more concerned with answering the “What” questions about ABAC.
    - OASIS defined XACML which is one (of several) frameworks/protocols that can be used to implement ABAC. OASIS’s XACML language is one answer to the technical “How” of ABAC.

XACML Reference Architecture

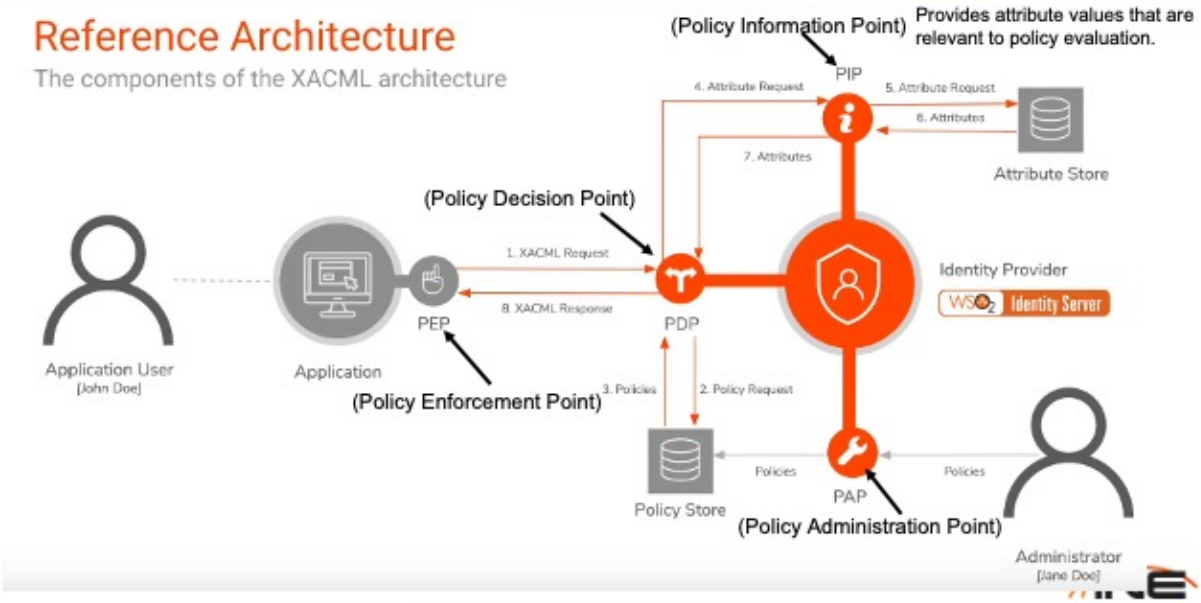
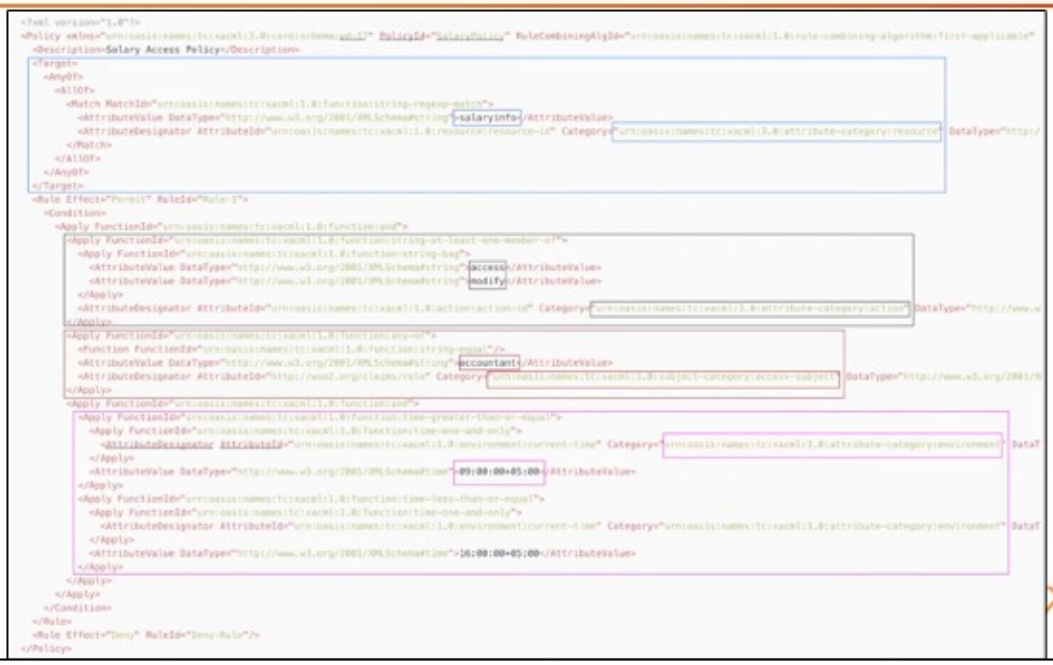
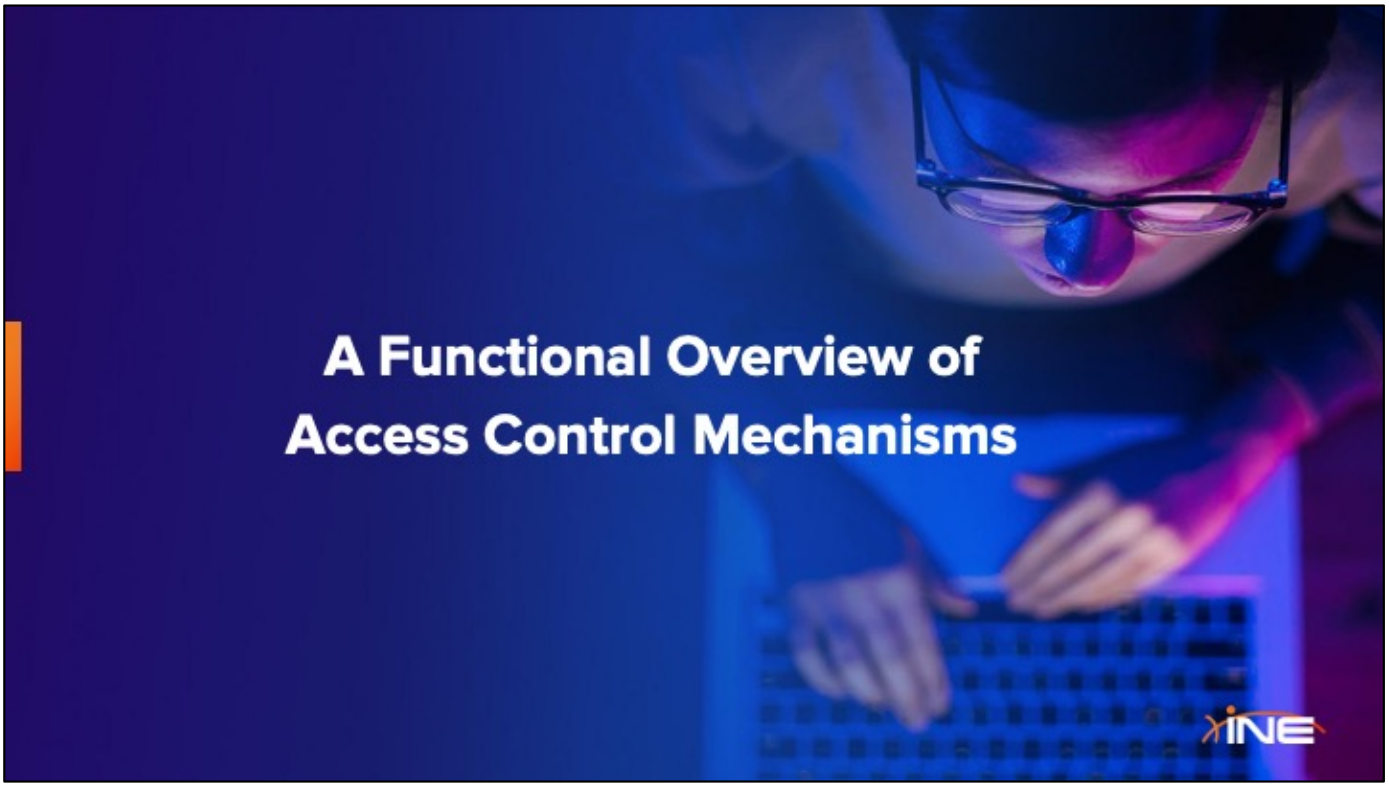


Image courtesy of http://wso2.com/training/

Sample XACML File



Thank you for watching!



What are Access Control Mechanisms?

- A method for implementing access control models
- Systems may employ several access control mechanisms
- Some examples;
  - Access Control Lists
  - Capability Tables
  - Restricted Interface
  - Content-dependent Access Control
  - Context-dependent Access Control

Access Control Lists

- *Assigned to the Objects* they are protecting
- Specifies Subjects allowed to access the Object and their permissions
- Commonly found on Discretionary Access Control (DAC) implementations.

Capability Tables

- Defines a collection of Objects that a Subject is allowed to access and the associated permissions.
- *A Subject-centric* access control mechanism.

	Objects				
Subject	File-123	Program-X	File-667	Database-E	File-111
kbogart112	R-W	X	W	R-W	R

Restricted Interface

- Subjects will use a variety of “interfaces” to interact with Objects such as:
  - Menus
  - Shells
  - Dashboards
- A method of access control where the *user interface itself is limited or customized based on the access level of the user*.
- A user can only interact with, view, or manipulate those parts of the system or application for which they have the necessary permissions.
- Examples include Role-based Dashboards, Restricted Menus and Educational Platforms

Content-Dependent Access Control

- An access control that determines a user's access rights *based on the content within the resource or data* they are attempting to access.
- The actual data content or attributes of the data being accessed influence the decision-making process about who can read, modify, or interact with it.
- Examples include:
  - Email filtering systems (SPAM determination, Junk Mail, etc)
  - Controls applied to restrict viewing of mature video content
  - The children's book section at a library

Context-Dependent Access Control

- A system that utilizes contextual information as well as the user's identity to make an authorization decision.
- The "context" encompasses situational aspects of the access request, such as the time, location, device security posture, network security, and current threat level.
- Examples include:
  - Maximum thresholds against unsuccessful authentication attempts
  - Time of access requests
  - Location of the source of an access request
- Context-Dependent access control is one element of ABAC

- ABAC – Attribute-Based Access Control

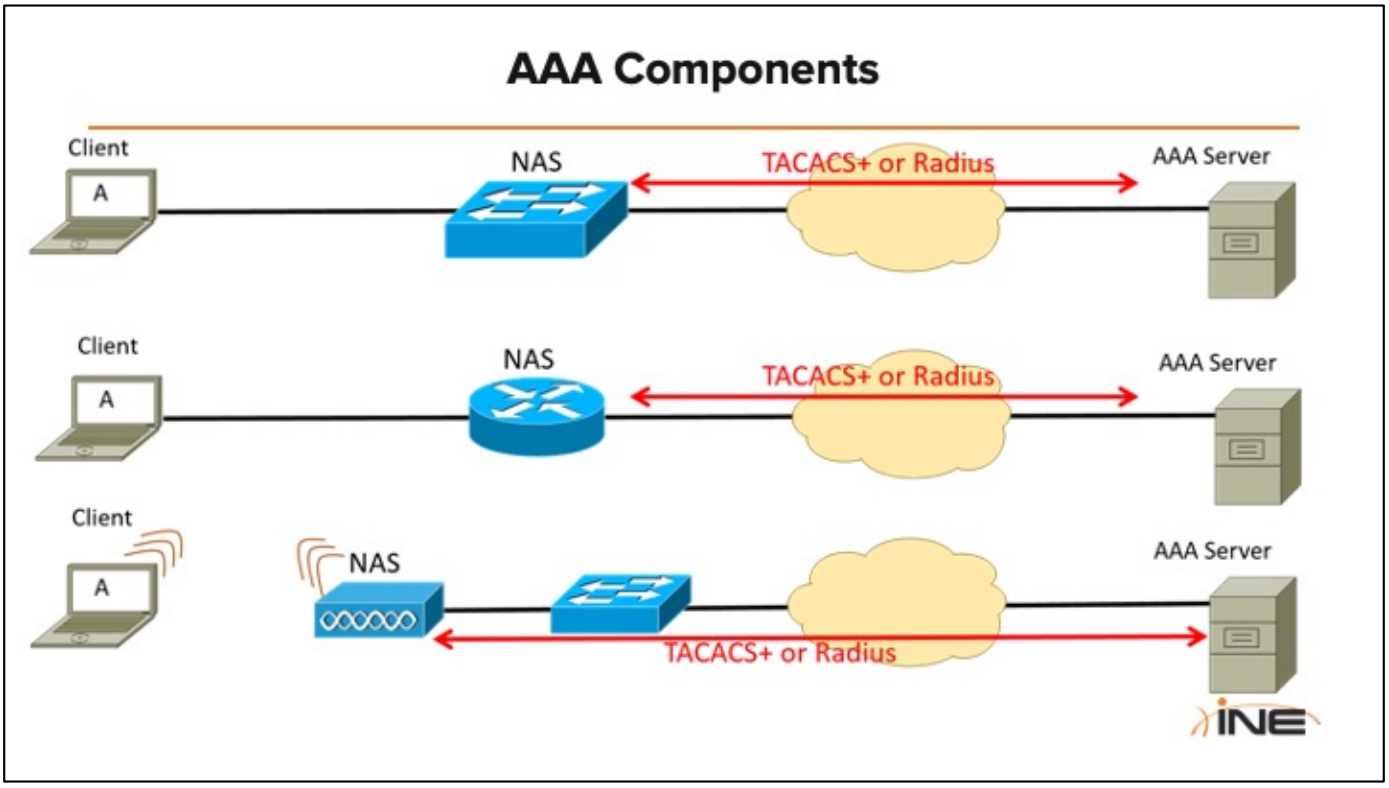
Thank you for watching!

AAA Usage Within IBAC

- Identity Based Access Control (IBAC) requires the implementation of protocols that can;
  - Retrieve and format identity information about Subjects
  - Transport identity information (and any other additional needed information) to and from identity policy servers
  - Transport authentication and authorization status between identity servers and identity enforcement systems
- The above process can be categorized as AAA

What Is AAA?

- Authentication, Authorization, & Accounting
- Client – NAS – Server Architecture
- Typically used to secure access to Management Plane
  - Client wants CLI access to network device or...
- Can also assist in controlling access to the Data Plane
  - Client wants network access (802.1x)



Common AAA Protocols

- Three protocols are commonly associated with AAA
  - TACACS+
  - Radius
  - Diameter
- While all three facilitate authentication, authorization and accounting they do so using different message formats and different transport protocols

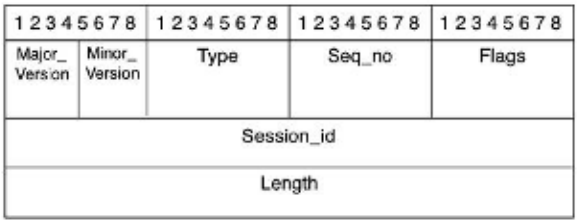
TACACS+

- Terminal Access Controller Access Control System
- Protocol designed to carry Authentication, Authorization and Accounting information
  - Cisco Proprietary
  - Utilizes TCP port-49
- Considers Authentication, Authorization and Accounting as separate processes
  - i.e. For Authentication, one could use something other than TACACS+ (like Kerberos) and still use TACACS+ for Authorization and Accounting
- All packets encrypted between AAA Client and Server

TACACS really designed to control which specific IOS commands a Network Admin is allowed access to.

TACACS+ Header

- TACACS+ Header Structure



  - Type (distinguishes the packet type - AUTHEN, AUTHOR, ACCT)
    - Different packets support different messages
      - E.g. START, REPLY, CONTINUE, ACCEPT, REJECT
  - Seq_no (packet sequence number for the session)
  - Flags (controls body encryption & session multiplexing)

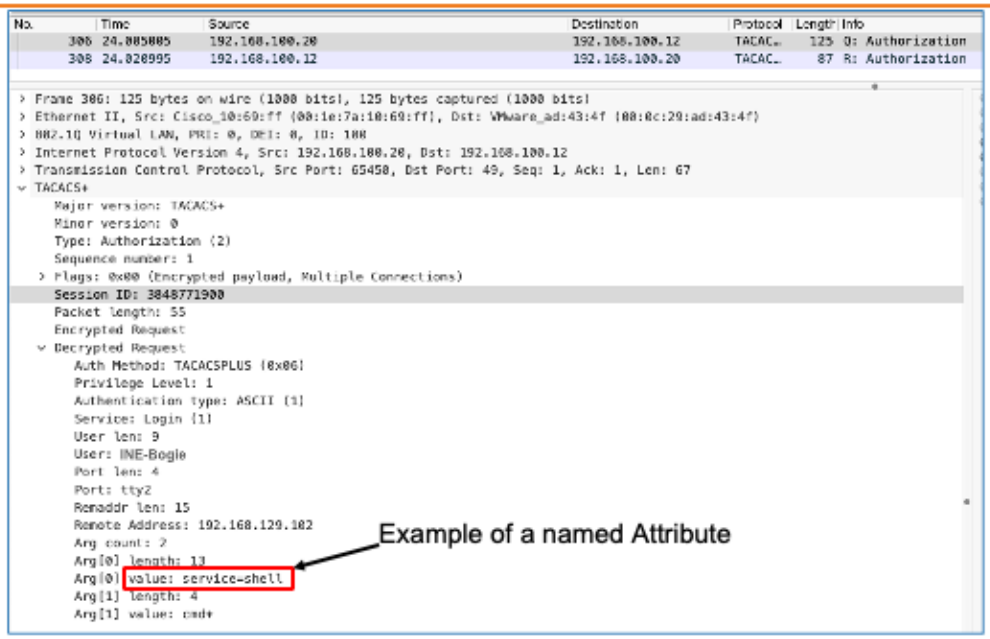
TACACS+ Attributes

- TACACS+ performs its AAA functions with AV (Attribute/Value) pairs
  - Attributes are named rather than numbered, Values are strings
    - E.g. *service=shell*
- Full Attribute List
  - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-mt/sec-usr-tacacs-15-mt-book/sec-usr-tacacs-att-value-pairs.html

Table 1 **Supported TACACS+ Authentication and Authorization AV Pairs**

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes	yes	yes	yes	yes	yes	yes
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.	yes	yes	yes	yes	yes	yes	yes
addr-pool=x	Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip. Note that **addr-pool** works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the **ip-local pool** command to declare local pools. For example: ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20 You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.	yes	yes	yes	yes	yes	yes	yes

TACACS+ Example



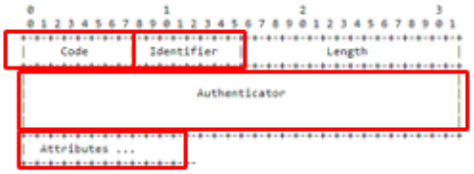
Radius

- Remote Authentication Dial In User Service
- Protocol designed to carry Authentication, Authorization and Accounting information
- IETF Standard Protocol
  - Originally defined in RFC 2058. Updated multiple times since then (see RFC 2865)
- Bundles Authentication/Authorization
- Transported by UDP (ports 1812/1813 or 1645/1646)
- Supports multiple authentication methods such as PAP, CHAP and EAP

Carried by UDP port 1812 (Authentication) and 1813 (Accounting)
…
Originally was UDP 1645 (Authentication) and 1646 (Accounting).
-
Original intent behind radius was to protect the Data Plane. Dialup users had to pass Radius Authentication/Authorization before being granted access to the Data Plane. Although it CAN protect the Management Plane…that is not its forte nor original purpose.

RADIUS Header

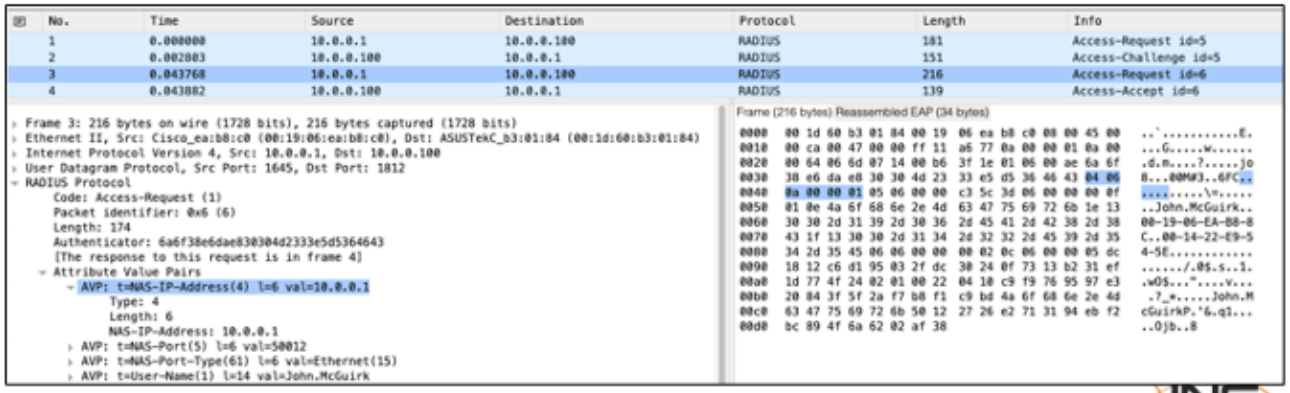
- RADIUS Header consists of 5 fields



- Code (identifies RADIUS packet type)
  - Access-Request, Access-Accept, Access-Reject, Access-Challenge
  - Accounting-Request, Accounting-Response
- Identifier (request-reply matching)
- Authenticator – Secret password/key shared between NAS and authentication server
- Attributes (AAA data)

RADIUS Attributes

- RADIUS exchanges client-server information using Attributes
  - Attributes in the TLV format allow Radius to carry different types of data
- Most of the 255 main attributes are IETF-predefined
  - See RFC2865, Section-5



RADIUS & TACACS+ Comparison

- RADIUS vs TACACS+
  - Primary Purpose : network access (R) <-> device administration (T)
  - Transport : UDP 1812/1813 or 1645/1646 (R) <-> TCP 49 (T)
  - Security : user password (R) <-> entire payload encryption (T)
  - Protocol Design : auth + auth (R) <-> separate AAA functions (T)
  - Standardization : industry standard (R) <-> Cisco proprietary (T)
  - EAP Support : yes (R) <-> no (T)

Diameter

- Originally introduced in IETF RFC 6733
- More scalable and flexible than Radius or TACACS+
- While also used for AAA, Diameter is primarily implemented in telecommunications networks such as IMS networks, LTE, and mobile telephony.
- Utilizes TCP or SCTP for transport
- Like TACACS+, offers end-to-end security via encryption of packets using;
  - TLS (when transported using TCP)
  - Stream Control Transmission Protocol (SCTP) Adaptation Layer (also called, "DTLS over SCTP")

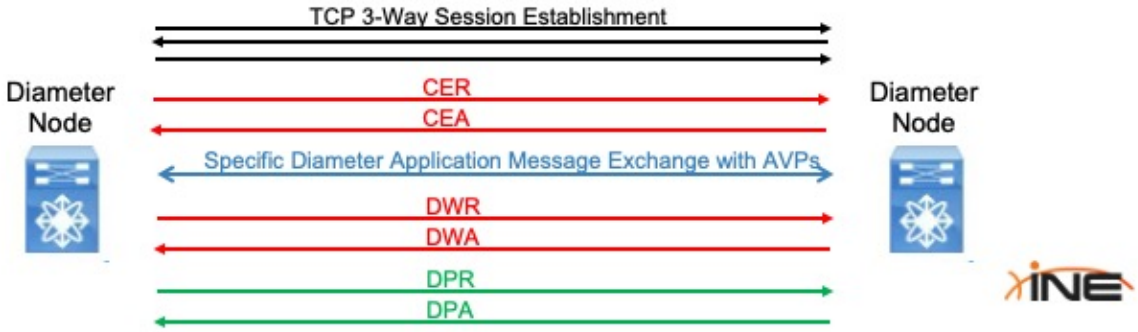
- SCTP = Stream Control Transmission Protocol. A reliable transport protocol like TCP but with added functionality such a multi-homing which allows an association to span multiple IP addresses at each endpoint. This provides redundancy; if one path fails, SCTP can continue communication over an alternate path without disrupting the connection.

Diameter Applications

- Diameter is extensible because it utilizes different applications.
- Diameter base protocol handles;
  - Reliable transport
  - Message delivery
  - Error handling
- Diameter base protocol works with various Diameter applications to extend its services such as:
  - Diameter Network Access Server Application (RFC 4005)
  - Diameter Base Accounting (RFC 6733)
  - Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072)

Diameter Message Exchange Overview

- Diameter messages consist of Requests and Answers
- Diameter messages fall into four categories:
  - Capabilities Exchange (CER and CEA)
  - Application specific messages using AVPs (Attribute-Value Pairs)
  - Diameter Watchdog (DWR and DWA)
  - Disconnect Peer (DPR and DPA)

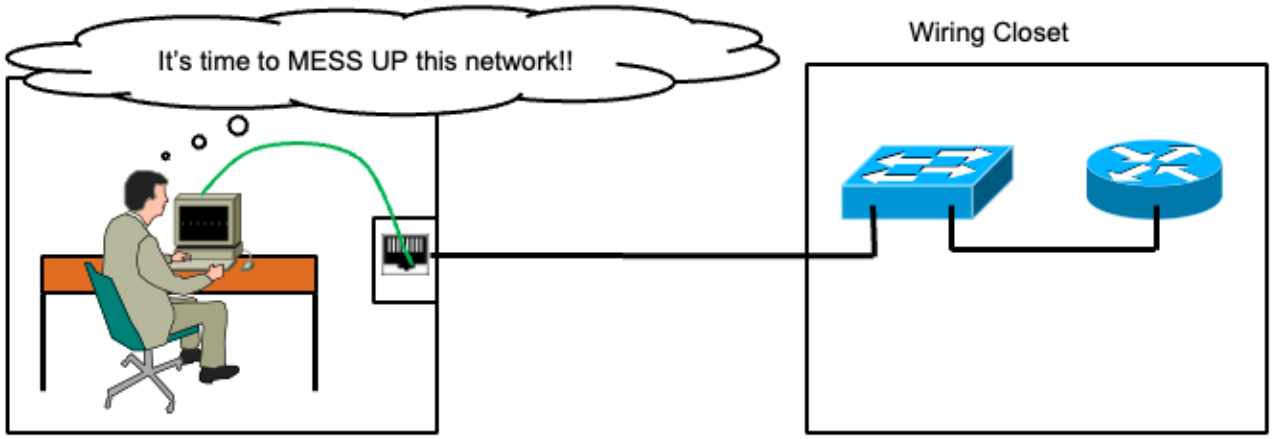


Thank you for watching!

Introduction to Port-Based Security

- Technical controls used to implement access controls can be applied against several different kinds of objects:
  - File access and manipulation
  - Database access and manipulation
  - Physical device access (buildings, safes, secured data centers, etc)
- When the network itself is considered the Object, access controls can be applied against it to restrict network access and what actions can take place on that network.
- Port-based security is a method of access control that;
  - Is applied *against network access ports*
  - Forces identification and authentication of potential network users
  - Can also implement authorization policies for authenticated users

Anyone can connect to the network!



You're In!!

- By default, routers and switches do not perform security checks against any device that connects to them
- Routers and switches will forward any frame/packet received on an interface if:
  - The appropriate protocol is enabled on the ingress interface
  - The appropriate forwarding tables or trees exist

Limiting Switch Access

- Port Security can be used to limit access to switchports
- Not available on dynamic ports
- What can be secured?
  - Maximum quantity of learned, dynamic MAC addresses can be limited
  - Static, authorized MAC addresses can be pre-configured
  - Combination of both options above

Port Security will work on a trunk as long as DTP is not in-use.
-
A secure port cannot be:
Destination port for SPAN
Port-channel
Private VLAN port

Basic Configuration

- Port Security can be enabled with a single interface-level command;
  - Switch>*enable*
  - Switch#*configure terminal*
  - Switch(config)#*interface gigabit0/0*
  - Switch(config-if)#**switchport port-security**
  - Switch(config-if)#end
- What are the defaults with this one command?
  - Port is allowed to learn a single MAC only
  - First MAC learned is assumed to be an authorized MAC
  - Subsequent MACs learned on the same port will cause a security violation

Optional Configurations

- Allow pre-defined quantity of MACs
  - (config-if)#switchport port-security maximum <1-1536>
- Pre-configure known, authorized MACs
  - (config-if)#switchport port-security mac <address>
- Apply aging timer to authorized MACs
  - (config-if)#switchport port-security aging time <1-1440 mins>
  - (config-if)#switchport port-security aging type <absolute | inactivity>

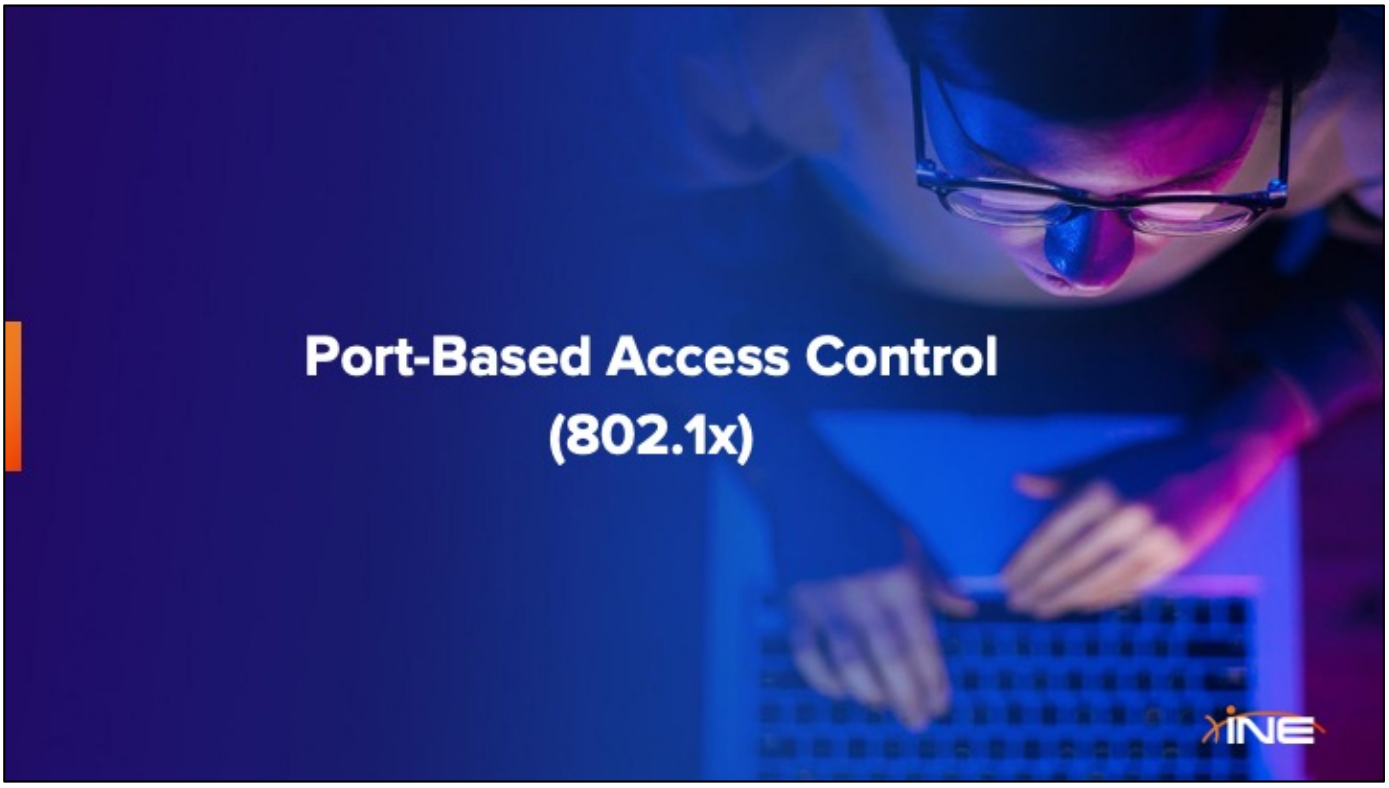
Port-Security Violations

- If a violation occurs, you have three options with regards to the response:
  - Shutdown (default)
  - Protect
  - Restrict

```
interface FastEthernet0/1
 switchport access vlan 22
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 001a.6c30.8faa vlan access
```

Protect doesn't give you syslogs or ANY indication that there has been a violation. ALL it does is silently discard the offending frames.

Thank you for watching!



Port Security – Pros and Cons

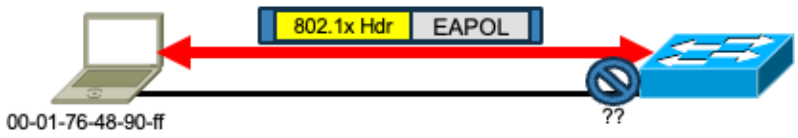
- What could Port Security do?
  - Allow only a specific MAC to associate with a port
  - Allow only a finite number of MACs to associate with a port
  - Any combination of the two above
  - Authenticate a device (MAC Address)
  - End-Device did not participate in the process
- What it could NOT do
  - Authenticate a user (shared PC for example)
  - Assign a dynamic policies (ie. VLANs, ACLs, etc) based on login credentials
  - Periodically Re-Authenticate
- *802.1x* was designed to overcome these shortcomings

802.1x Terminology

- As an IEEE protocol, 802.1x introduces some terminology you need to know;

IEEE Terms	Normal People Terms
Supplicant	Client
Authenticator	Network Access Device
Authentication Server	AAA/RADIUS Server

Default Security of 802.1x

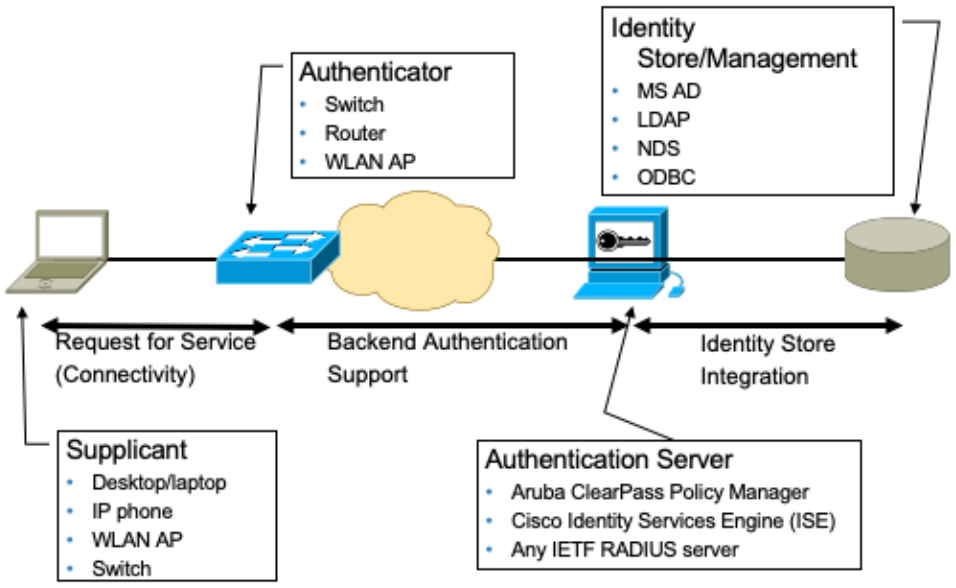


- Before 802.1x authorization, MAC address of end-station is unknown
- Before 802.1x authorization, spanning-tree is not in a forwarding state for the switch port
- Before 802.1x authorization, no traffic can be processed by switch CPU with the exception of EAPOL
- 802.1x state machine directly reliant on link state of port

Default Security of 802.1x

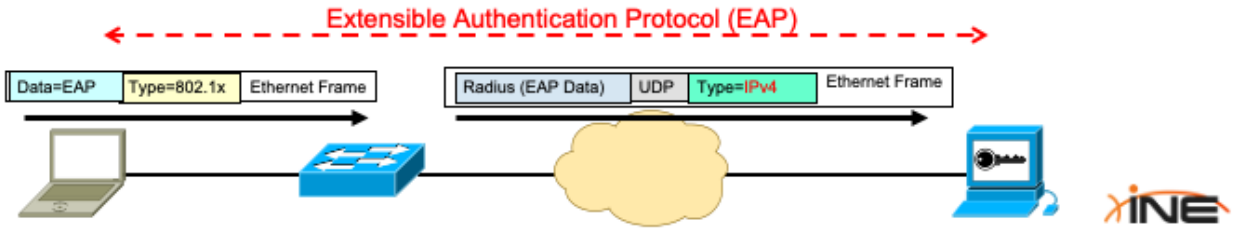
- Single-auth mode
- Authenticated session bound to MAC address used to authorize the port
- After 802.1x authorization, MAC address of end-station is the only one allowed on the port
- The operation ensures the validity of the authenticated session
- Network cannot be compromised by non-802.x client or a non-authenticated 802.1x client seen on the wire

802.1x Port Access Control Model



30,000-foot View

- EAP: Authentication Protocol between PC and AAA Server
  - EAP cannot be carried natively on the wire
  - EAP must be encapsulated inside of something else.
- Between client and "Authenticator" EAP is carried inside 802.1x
- Between Authenticator and AAA Server EAP is carried inside Radius.

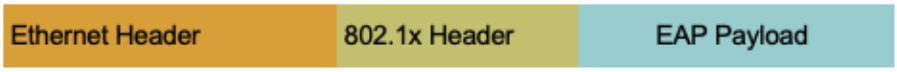


What Is EAP?

- EAP—the Extensible Authentication Protocol
- A flexible transport protocol used to carry arbitrary authentication information—not the authentication method itself
- Rose out of need to reduce complexity of relationships between systems and increasing need for more elaborate and secure authentication methods
- Typically runs directly over data-link layers such as PPP or IEEE 802 media

What Does It Do?

- Transports authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- A switch or access point becomes a conduit for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry EAP information
- Establishes and manages connection; allows authentication by encapsulating various types of authentication exchanges; EAP messages can be encapsulated in the packets of other protocols, such as 802.1x or RADIUS
- Three forms of EAP are specified in the standard
  - EAP-MD5—MD5 hashed username/password
  - EAP-OTP—one-time passwords
  - EAP-GTC—token-card implementations requiring user input

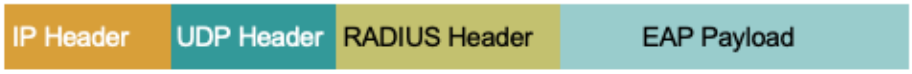


IEEE 802.1x

- Standard set by the IEEE 802.1 working group
- Is a framework designed to address and provide **port-based** access control using authentication
- Primarily 802.1x ***is an encapsulation method for EAP over IEEE 802 media***—EAPOL (EAP over LAN) is the key protocol
  - Layer 2 protocol for transporting authentication messages (EAP) between supplicant (user/PC) and authenticator (switch or access point)
  - Assumes a secure connection
- Actual enforcement is via MAC-based filtering and port-state monitoring

How Is RADIUS Used Here?

- RADIUS acts as the transport for EAP, from the authenticator (switch) to the authentication server (RADIUS server)
- RFC for how RADIUS should support EAP between authenticator and authentication server—RFC 3579



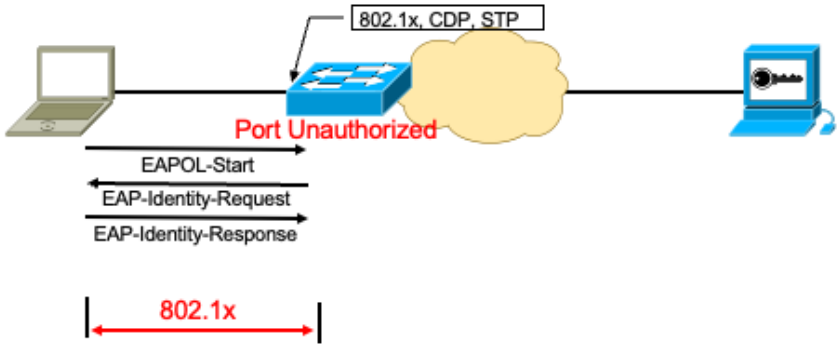
- RADIUS is also used to carry policy instructions back to the authenticator in the form of AV pairs

- Usage guideline for 802.1x authenticators use of RADIUS RFC 3580

UDP Ports for Radius: 1812 = Authentication and Authorization / 1813 = Accounting

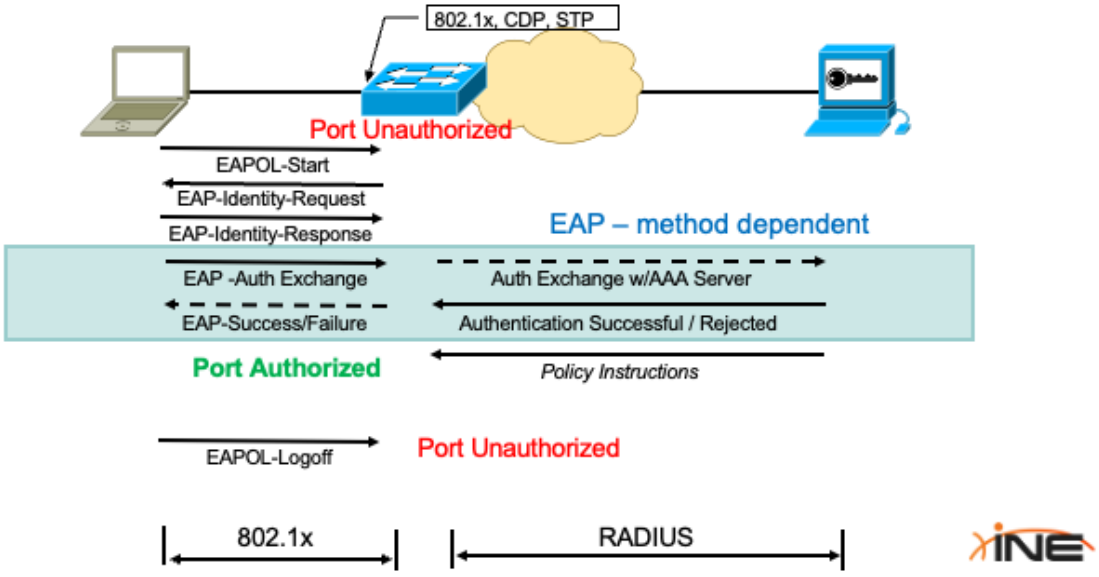
Some older implementations used 1645 and 1646

A Closer Look...



- NOTE: All 802.1x frames sent to/from Supplicant to/from Authenticator use the reserved Destination MAC of 01-80-C2-00-00-03.
- Switches NOT configured for 802.1x will not forward these frames because they fall into the reserved 802.1d MAC range for BPDUs.
- They will be sent to the CPU and dropped.

A Closer Look...



Thank you for watching!

What Are Network ACLs?

- ACL = Access Control List
- A basic form of access control implemented within network infrastructure devices
- Inspect one or more headers of an Ethernet frame or IP packet to determine if network access can be granted.
- Can be considered a form of ABAC (Attribute-Based Access Control).
- Implemented at various layers of the OSI Model
  - Layer-2 ACLs
  - Layer-3 ACLs
  - Layer-4 ACLs

Layer-2 Access-Lists

- Operate at the OSI Data Link Layer
- Consist of one or more ACEs (Access Control Entries)
- Each ACE will typically inspect source or destination MAC addresses within a frame to determine a forward-or-drop action
- Can also inspect;
  - Class of Service (802.1p bits)
  - Ether-Type
  - 802.1ad DEI
- Can inspect and act upon traffic flowing through a device but not traffic originated by the device.

- 802.1ad is a method of stacking multiple VLAN tags within a single Ethernet frame (also called queue-in-queue). The DEI (Drop Elligibility Indicator) is a bit that can be set to indicate a frame is eligible to be dropped during times of network congestion.

Examples of Layer-2 Access Lists

Cisco IOS-XR

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
```

Cisco IOS-XE

```
(config)#mac access-list extended macext5
(config-ext-macl)#permit any host 0000.0000.0009
(config-ext-macl)#permit any host 0000.0000.0010
(config-ext-macl)#permit any host 0000.0000.0011
(config-ext-macl)#permit any host 0000.0000.0012
```

- In many Cisco platforms, MAC/Layer-2 ACLs can only be used to inspect frames that are NOT carrying IPv4 or IPv6 packets.
- Some platforms allow you to apply a mask against the MAC address (so you can match on a range of addresses) while other platforms only support the “any” or “host” commands which only allow matching on a single, specific MAC address.

Layer-3 Access-Lists

- Operate at the OSI Network Layer
- Consist of one or more ACEs (Access Control Entries) processed sequentially.
  - Each ACE will typically inspect a source and/or destination IPv4/IPv6 address within a packet to determine a forward-or-drop action
  - Can also inspect IP protocol value
- Can inspect and act upon traffic flowing through a device but not traffic originated by the device.

Examples of Layer-3 Access Lists

```
ip access-list standard prevention
 remark Do not allow user1 subnet through
 deny 172.22.0.0 0.0.255.255
 remark Allow Main subnet
 permit 172.25.0.0 0.0.255.255
```

```
ipv6 access-list acl1
 permit ipv6 host 2001:DB8:0:4::2/32 any
 deny ipv6 10:10:10:10::1/64 20:20:20:20::1/64 log-input
 permit ipv6 any any log
```

Layer-4 Access-Lists

- Operate at the OSI Transport Layer
- Consist of one or more ACEs (Access Control Entries) processed sequentially.
- Each ACE will typically inspect a source and/or destination TCP/UDP port number within a packet to determine a forward-or-drop action
- Often will also incorporate Layer-3 IP address information

- The “Layer” of an ACL (such as Layer-2 ACL, Layer-3 ACL or Layer-4 ACL) doesn’t typically mean that the ACL can ONLY inspect data at that layer, but often means that the layer specified in the name is the HIGHEST Layer (in the OSI Reference Model) that the ACL can inspect.
- For example in Cisco devices, if you wish to utilize a Layer-4 ACL you must still populate something in the Layer-3 IPv4/IPv6 destination fields of the ACL…even if it’s something generic like the keyword, “any”.

Examples of Layer-4 ACLs

```
ip access-list extended marketing-group
 permit tcp any 172.26.0.0 0.0.255.255 eq telnet
```

```
IPv6 access list Virtual-Access2
    permit tcp host 2001:DB8:1::32 eq bgp host 2001:DB8:2::32 eq 11000 sequence 1
    permit tcp host 2001:DB8:1::32 eq telnet host 2001:DB8:2::32 eq 11001 sequence 2
```

Common Caveats of Access Control Lists

- Access control lists must be applied to a layer-3 routed interface or they will have no effect
  - Router(config)#interface GigabitEthernet0/0
  - Router(config-if)#***ip access-group 101 in***
- Network based (Layer-2, Layer-3 or Layer-4) ACLs typically have the following caveats when implemented on Cisco devices:
  - ACEs are processed sequentially until a match is found
  - No further processing of ACEs takes place after a match is found
  - If no match is found the default action is "deny"
- Most ACLs can be configured as "named" or "numbered" ACLs
- Named ACLs are easier to edit

VLAN Maps

- Network-based Layer-3 and Layer-4 access control lists can only inspect traffic that is being routed between subnets.
- VLAN maps allow one to control the forwarding of traffic;
  - That is switched within a single VLAN
  - That is routed between VLANs
- VLAN maps utilize Layer-2, Layer-3 or Layer-4 ACLs but the application of the ACL is done within a VLAN...not on a routable interface.
- Within some platforms VLAN maps can also;
  - Redirect traffic to an interface of your choice
  - Capture traffic and send copies of packets to a "Capture port"

VLAN Map Example

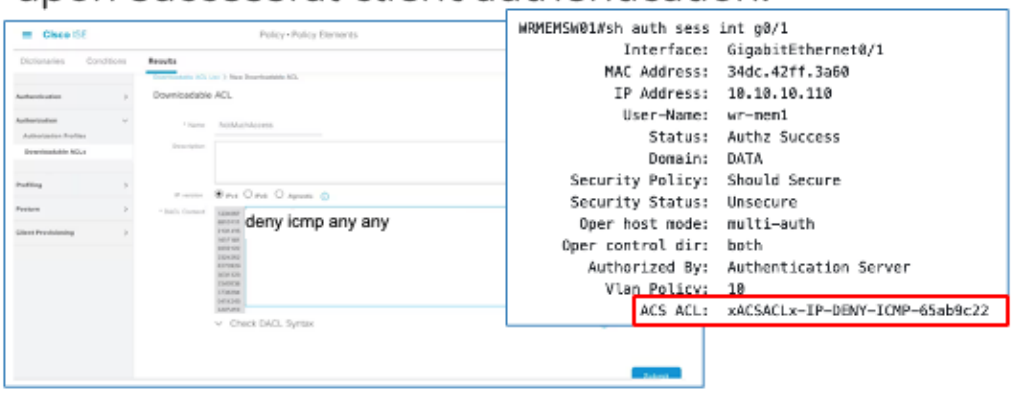
```
// Define access list
Router(config)# ip access-list extended cisco_acl
Router(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 any
Router(config-ext-nacl)#exit

//Define VLAN Access map
Router(config)# vlan access-map cisco 10
Router(config-access-map)# match ip address cisco_acl
Router(config-access-map)# action forward
Router(config-access-map)# exit


//Apply VACL to VLAN 10 to 20
Router(config)# vlan filter cisco vlan-list 10-20
```

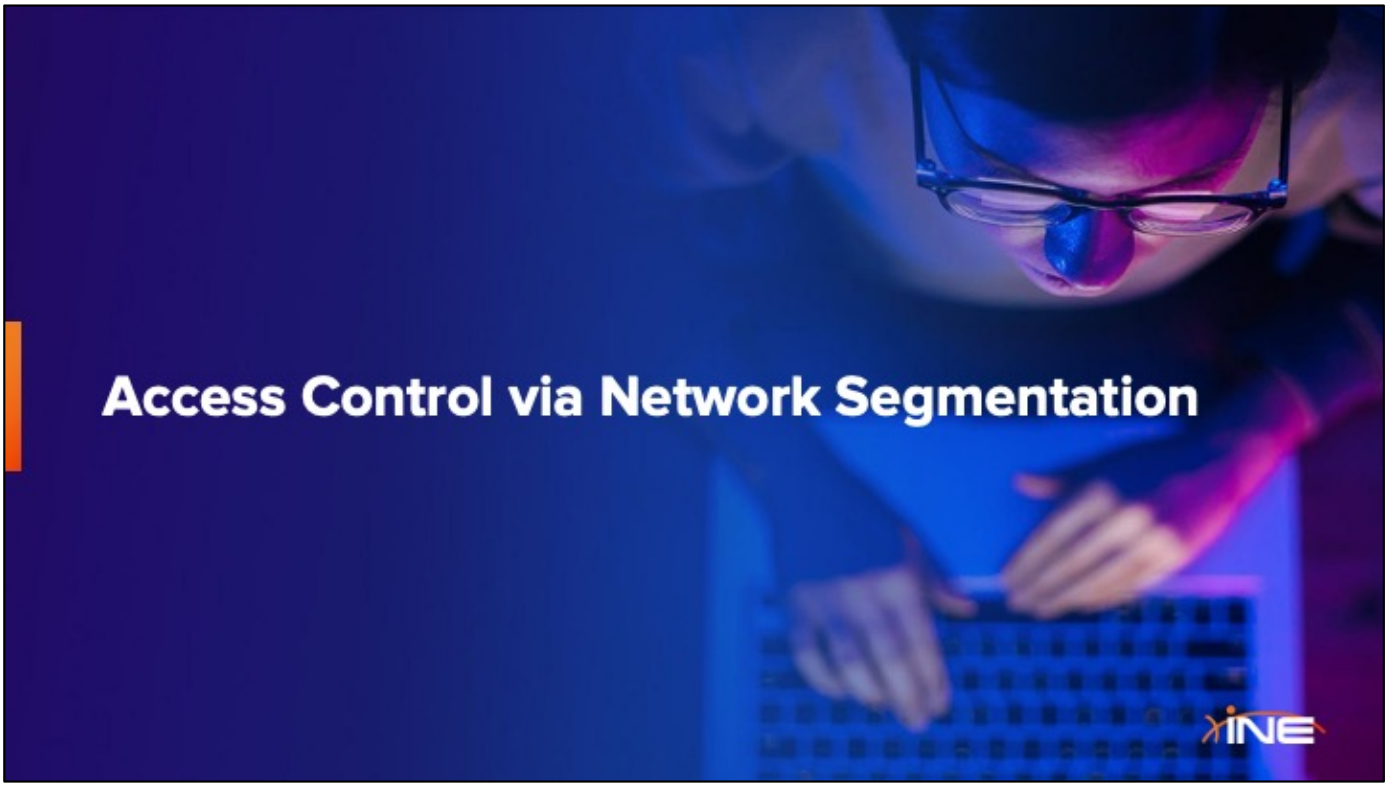
dACLs

- dACL = Downloadable Access Control List
- ACLs configured on an external controller (such as ISE or a WLC) and downloaded to the network device (Switch) upon successful client authentication.



- The benefit of downloadable ACLs is that, for mobile devices (like laptops or tablets) you don't have to manually configure the ACL on every device the user could possibly connect to. Instead, as a user moves to a new network device and authenticates via 802.1x the downloadable ACL is dynamically pushed to the port on that device where the user is connected.
- The name of the ACL shown in the output of "show authentication session" is automatically generated by the Cisco IOS device (router or switch). It will not match the descriptive name you configured on your authentication server.

Thank you for watching!

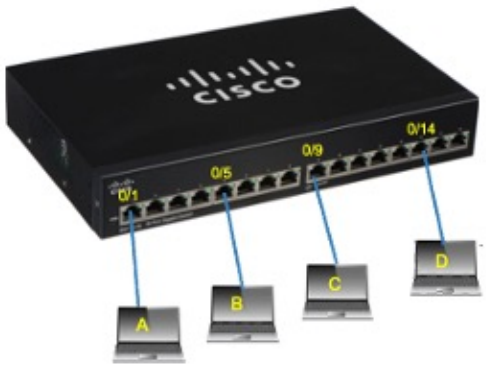


What is Network Segmentation

- Access control via network segmentation is the process of;
  - Dividing a network into different logical groups
  - Devising and implementing access control policies that dictate traffic flow between network segmentation groups
- Various methods exist to support this including;
  - VLANs (with and without VLAN Maps)
  - Private VLANs
  - Firewall DMZs and Zones
  - Cisco TrustSec

Segmentation Using VLANs

- VLAN = Virtual Local Area Network
- Logical method of grouping Layer-2 switchports on a local switch into different broadcast domains
- Traffic must be routed to pass between VLANs



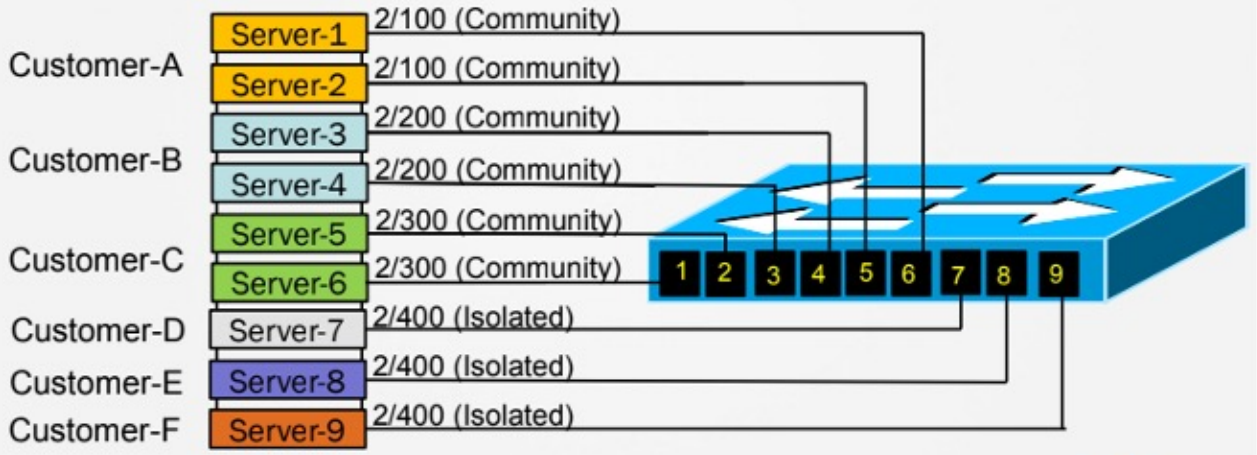
- Segmentation of broadcasts is automatic when VLANs are implemented
- Segmentation of unicast traffic is automatic if no router exists that is within the VLAN

IntraVLAN Traffic Segmentation

- Methods exist to implement network-based access control policies on bridged (intra-VLAN) traffic;
  - VLAN Maps (ie. VLAN Access Lists or "VACLs")
  - Private VLANs
- Private VLAN Concepts
  - Each PVLAN port is associated with two VLANs (one primary VLAN and one secondary VLAN)
  - Secondary VLANs configured for Private VLANs consist of two sub-types:
    - Community PVLANs
    - Isolated PVLANs
  - Promiscuous ports provide an egress point for the PVLAN

Private VLAN Operation

» Primary VLAN-2 (SVI for VLAN-2 = 2.2.2.1/24)



An Introduction to Firewalls

- Firewall Placement:

- Firewall functionality – To allow specific, trusted traffic between networks & deny unwanted traffic from crossing network boundaries

Firewall Stateful Packet Filtering

- Many firewalls enforce network segmentation via stateful packet filtering.
- Firewall remembers the “state” of outgoing connections
- Relies on a stateful database
- Traffic initiated from outside/untrusted interfaces denied
- Easy to implement and configure
- Firewall is transparent to end users

Per User Network Segmentation

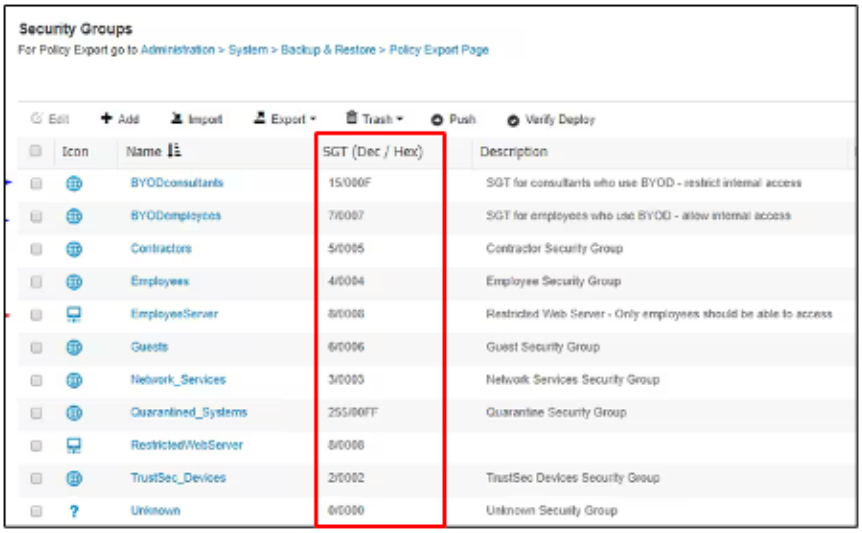
- Previously mentioned methods of network segmentation restrict network access by:
  - Pre-planned, static geographic network restrictions (eg, VLANs & Firewalls)
  - Segmentation based on static device addressing (eg Network-Based Access-Lists)
- Is it possible to segment the network based on user identity and role?
  - A user's IP address could change...and it wouldn't matter
  - A user could connect to any portion of the network and still be required to comply with network segmentation rules

Segmentation Using Cisco TrustSec

- Next-generation segmentation for simplified access control
- Access Controls are defined based on roles/context rather than IP addresses (i.e. "Security Groups")
- Each Security Group is assigned a tag ("Security Group Tag") for identification & filtering
- Filtering policy is defined through Security Group ACLs (SGACLs)
  - Source SGT, destination SGT, action & protocol
  - Enforcement performed at egress
- The policy is scalable, "follows a user" and does not depend on the network topology

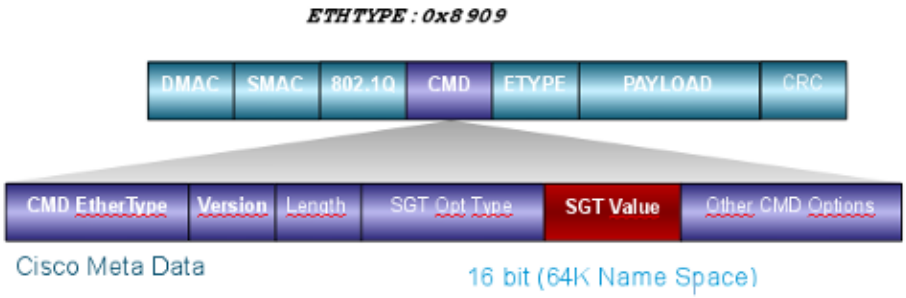
Example of Security Group Tags

- Below we see some Security Groups and their associated Tag values on the Cisco ISE:



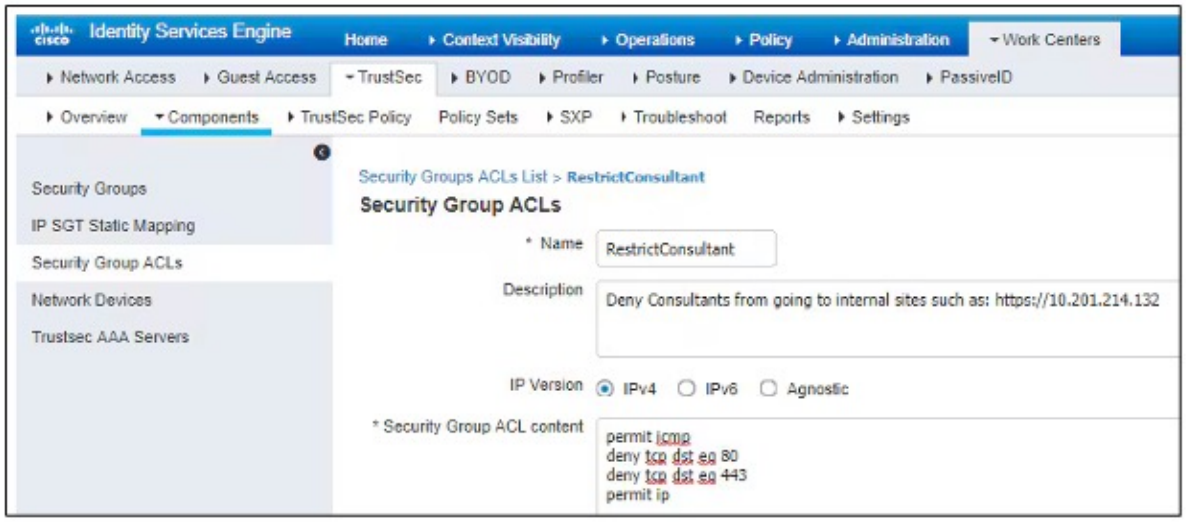
SGT Frame Placement

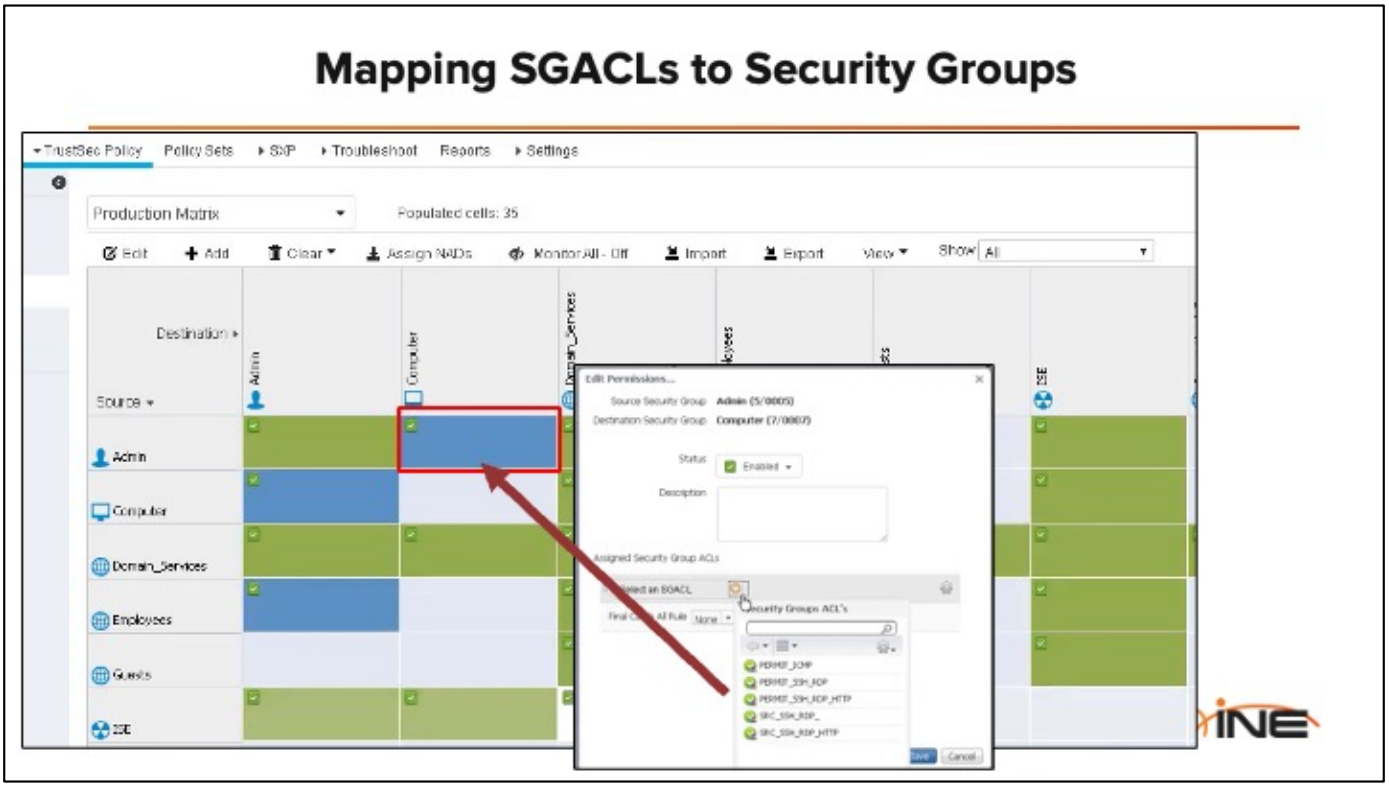
- Network devices within the TrustSec cloud come in two forms:
  - Devices capable of applying Security Group Tags in hardware
  - Devices that cannot send/receive SGTs but can logically apply tagging and SGACL rules in software
- Hardware-applied SGTs take the following format:



- CMD in this context stands for the “Cisco Meta Data” field.
- For network access devices that support the role of 802.1x Authenticator but don’t have the ability to add SGTs to Ethernet frames (no hardware ability) they can learn remote IP-to-SGT mappings as well as the full list of SGACLs (Security Group Access Control Lists) from ISE (or another TrustSec router) via the SXP (Security-group eXchange Protocol).

Creating TrustSec SGACLs

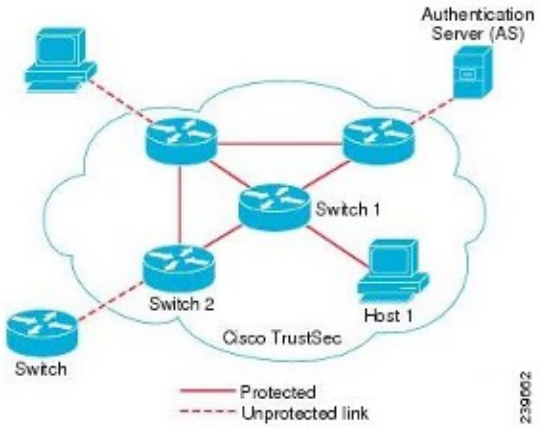




- In Cisco ISE you can have the names of your SGACLs display in each cell of the matrix. In this example the names have been hidden.
- In this example, a green cell has simply been given a “permit IP” default SGACL. If it were red that would mean it has a “Deny IP” rule applied.
- Cells that are in blue are cells in which specific, user-configured SGACLs have been applied.

Other Features of TrustSec

- Cisco TrustSec offers two additional (optional) features:
  - Authenticated Infrastructure (using 802.1x peer to peer authentication)
  - Encrypted Communications (using 802.1AE MACSec)



Graphic courtesy of Cisco ISE User Guide

Thank you for watching!

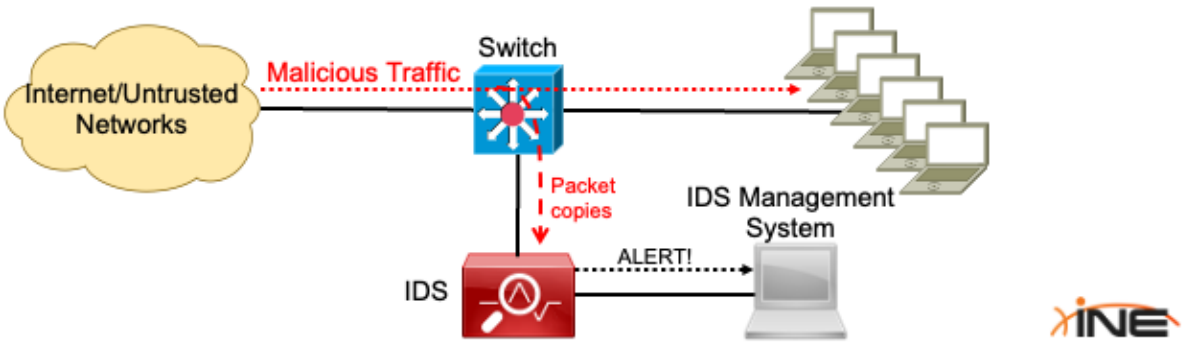
Intrusion Detection & Prevention

- Intrusion Detection controls can be technical, physical or administrative
- IDS and IPS systems are a form a technical controls
  - *IDS* = Intrusion Detection System
  - *IPS* = Intrusion Prevention System
- The main purpose of both IDS and IPS systems is to spot malicious activity via packet inspection which can produce an event...which subsequently generates an action.
- Can be network-based or host-based

- An Administrative Control aimed at Intrusion Detection might be a section of a newhire employee training class that concentrates on how to spot (and prevent) unbadged people from gaining entry into the office building. They could teach things like, “Ensure that you never hold the door open for anyone. Everyone needs a badge to enter the building. If you spot an unbadged person walking around call Security”.
- Both IPS and IDS systems are programmed with complex rulesets which allow them to determine if a packet is considered malicious or not.

Network-Based IDS Placement

- *IDS* systems typically operate in "promiscuous mode"
  - Placed outside of the packet forwarding path
  - Receive and inspect copies of the original packet
  - Can't directly interact with malicious packets but can alert other devices to do so.



- IDS and IPS systems are sometimes generically referred to as "sensors".

Network-Based IPS Placement

- *IPS* systems typically operate in "inline mode"
  - Placed along the packet forwarding paths of packets
  - Can intercept and inspect packets flowing through a network
  - Malicious packets can be immediately discarded
  - May induce packet forwarding delay

- Originally, IDS and IPS systems were unique appliance one could purchase and install within your network.
- The next evolution was to create appliances that could operate in either IDS or IPS modes to provide more flexibility (depending on the license you purchased for the device).
- The current evolution of IPS and IDS is to incorporate these functions within "next generation" Firewalls such as the Cisco Firepower 4100 Firewall.

IPS/IDS Methods of Detection

- Signature-Based
  - Rely on a comprehensive database of signatures, which are patterns or characteristics known to be indicative of malicious activity.
  - This database is regularly updated to include new threat signatures.
- Policy-Based
  - Focus on monitoring and controlling the flow of traffic according to a set of rules or policies defined by the network administrator, rather than relying solely on known signatures of malicious activities.

IPS/IDS Methods of Detection

- Anomaly-Based
  - Detects unusual patterns that do not conform to expected behavior, essentially learning what normal traffic looks like and then identifying deviations.
- Reputation-Based
  - Utilizes a database of IP addresses, domains, and URLs known to be malicious, assigning reputation scores based on their history of behavior.
  - When network traffic involves these entities, the system evaluates the reputation score to decide whether to allow, block, or alert on the activity.

Categories of IDS/IPS Events

- Triggers that create events (or things that SHOULD have created a trigger but didn't) can be classified using the following terminology;
  - ***False Positive***: A trigger indicating a malicious event when in reality, nothing bad actually happened.
  - ***False Negative***: When a true malicious event happens but the IPS/IDS fails to recognize it or generate an event alert.
  - *True Positive*:
    - A verifiable and accurate alert signifying a malicious event
    - This is correct behavior when something bad is happening
  - *True Negative*:
    - Lack of any event reporting because nothing malicious is happening.
    - This is correct behavior during normal conditions.

Host-Based IDS and IPS

- Specialized software that interacts with a host's Operating System
- Usually sits between applications and the host's OS kernel and monitors applications calls to the kernel.
- Can utilize the same detection techniques (i.e. anomaly-based, signature-based, etc) as Network-Based IDS and IPS systems.
- Benefits:
  - More scalable than network-based systems
  - Can inspect encrypted packets after decrypted by the host
- Drawbacks
  - May negatively impact CPU performance.
  - Allows attacking packets to reach the host

Examples of Host-Based IPS/IDS

- Microsoft Defender

- Open Source Security (OSSEC)

Thank you for watching!