CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Network Access Control (NAC) 802.1X

Chris Samayoa

Week 16 – 1st Lecture
5/3/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

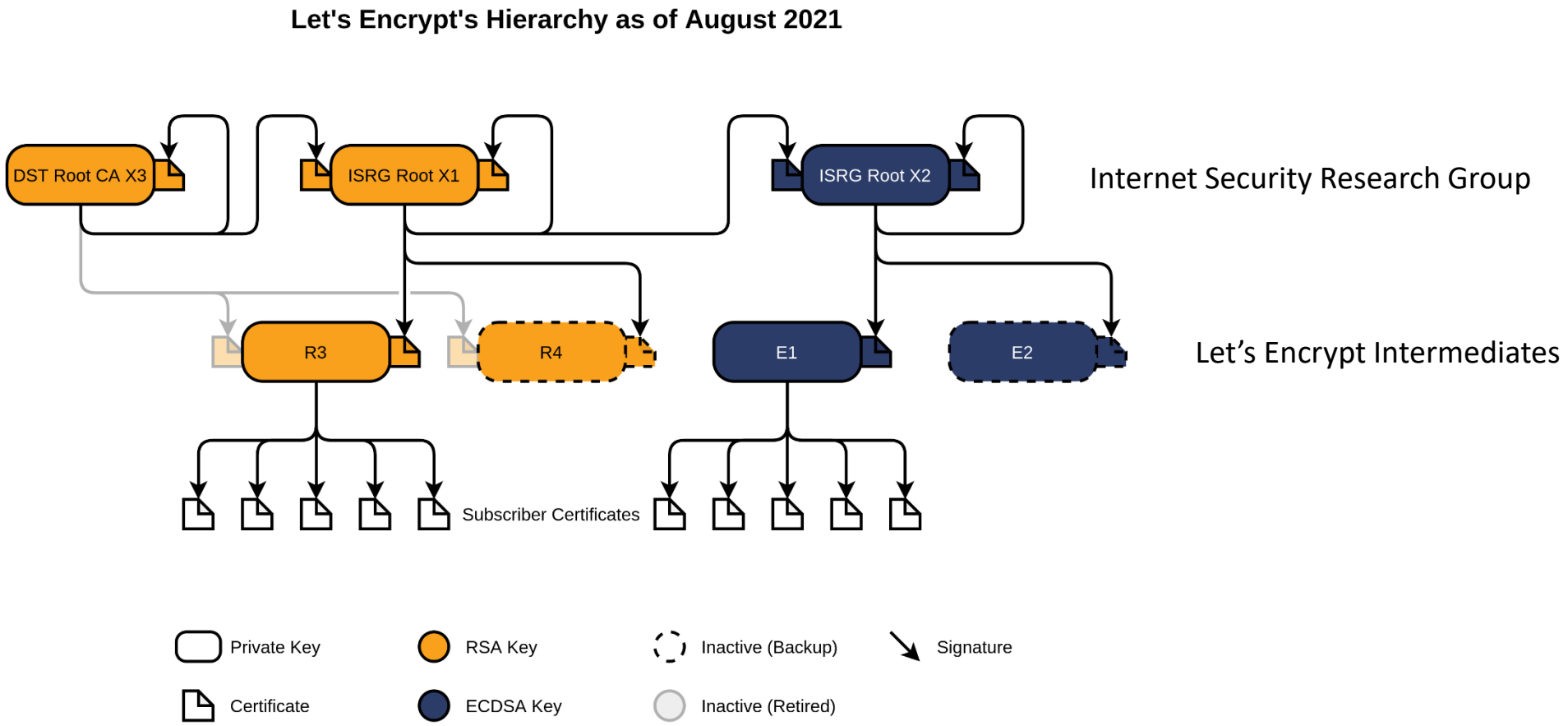
- Let's Encrypt
- NAC Overview
- Use Cases
  - Internal Workstations
  - Wireless / BYOD
  - IoT / Field Technology
- 802.1X
  - Common Vulnerabilities
  - EAP-TLS Mechanism
  - Automation
- Attribute-Based Access Control (ABAC)

Let's Encrypt

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Overview
  - Sponsorship allowed the creation of this nonprofit Certificate Authority (CA) for TLS certificates
    - Major sponsors: Mozilla, Cisco, Meta, AWS, and Chrome
  - Used by 260 million websites
  - API friendly for automated certificate renewals
    - 60 day renewal period recommended (90 day max)
  - Offers domain-validated certificates
    - Use web or DNS to validate ownership of domain using unique tokens
- Certbot
  - Popular Let's Encrypt client
    - Includes automated configurations for Apache and Nginx web services
  - Certificate creation: "sudo certbot --apache -d www.example.com"
  - Certificate renewal: "sudo certbot renew"
  - Easily use crontab to automate renewal process

Let’s Encrypt Chain of Trust



Source: https://letsencrypt.org/certificates/

Objectives

- Let's Encrypt
- NAC Overview
- Use Cases
  - Internal Workstations
  - Wireless / BYOD
  - IoT / Field Technology
- 802.1X
  - Common Vulnerabilities
  - EAP-TLS Mechanism
  - Automation
- Attribute-Based Access Control (ABAC)

NAC Overview

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Network Access Control (NAC) definition
  - Establish fine controls over how endpoint devices connect to a network and what resources they have access to
    - Base authorization on security policy
  - Core aspect is authentication and authorization
    - Software can also include additional tools such as antivirus, firewall, and vulnerability scanners
  - Creates auditable record of authorized and unauthorized resource requests
- Types of NAC
  - Pre-admission
    - Performs checks prior to allowing user/device on the network
  - Post-admission
    - Re-authenticates and checks for authorization when lateral movement on the network is requested

Source: https://www.techtarget.com/searchnetworking/definition/network-access-control

NAC Overview (cont'd)

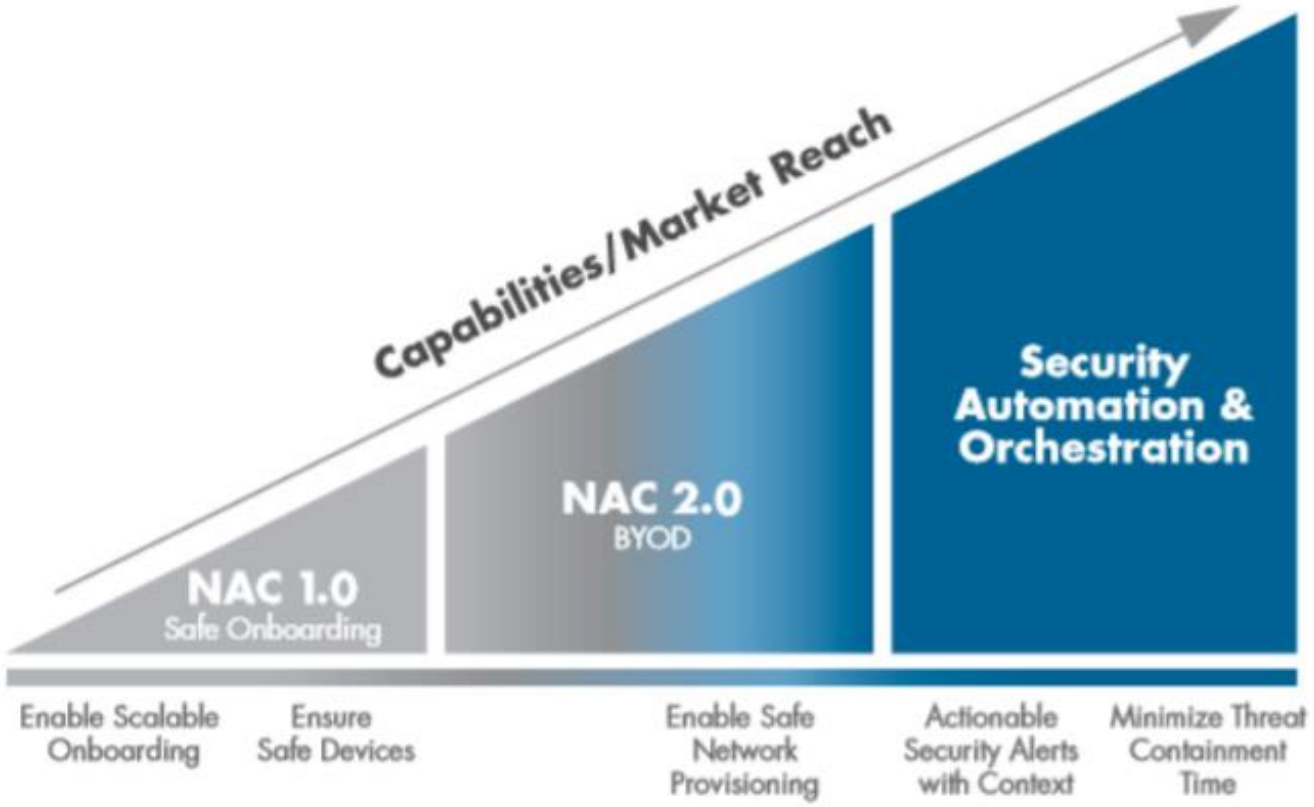
- Network Access Server
  - Centralized authentication/authorization server that determines access to network resources
    - VPN
    - Network load balancing
    - Network resource management
- Common use cases
  - Bring your own device (BYOD)
  - Access for non-employees
  - IoT
  - Incident response
- Capabilities
  - Limit / prevent unauthorized access to data
  - Block network access from non-compliance devices / users
  - Manage policy for connected network devices
  - Recognize and block malicious activity
  - Integrate with central monitoring solutions

Source: https://www.techtarget.com/searchnetworking/definition/network-access-control

Objectives

- Let's Encrypt
- NAC Overview
- Use Cases
  - Internal Workstations
  - Wireless / BYOD
  - IoT / Field Technology
- 802.1X
  - Common Vulnerabilities
  - EAP-TLS Mechanism
  - Automation
- Attribute-Based Access Control (ABAC)

Evolution of NAC



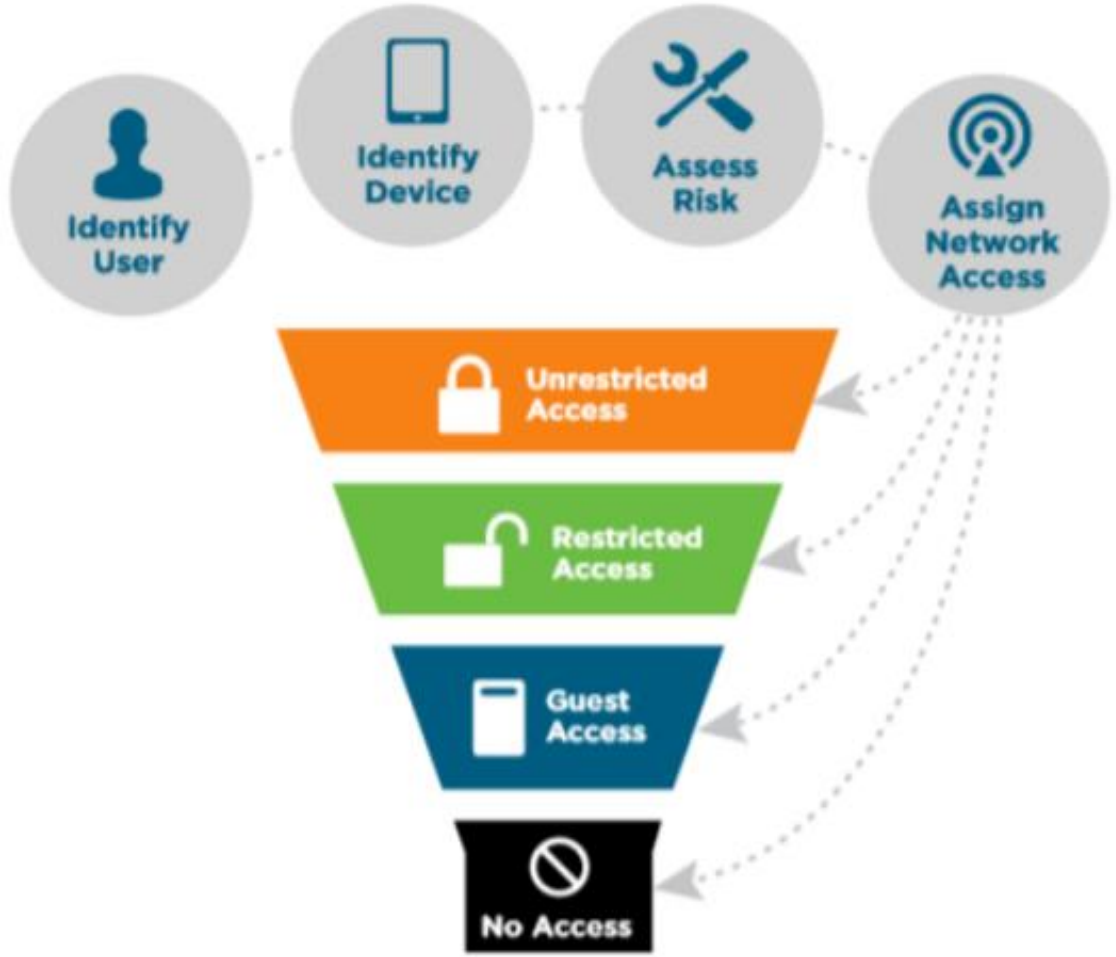
"Network access control is the act of keeping unauthorized users and devices out of a private network.“ - VMware

- Access Control
  - Local
  - External
- Compliance Enforcement
- Device / User Identification
- FAR Clause 52.204-21(b)(1)(i) - “Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).”
- Principle of Least Privilege

Source: The SANS Institute

Workstations

- "NAC 1.0"
- Company Owned
- Wired LAN Devices
- Easier to Manage
  - Complete administrative control



Source: The SANS Institute

Wireless / BYOD

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- “NAC 2.0”
- Laptops
- Cell Phones
- Remote Connections / VPN
- Enforce Compliance

CIS Control 1: Inventory and Control of Hardware Assets			Applicability	
Sub-Control	Control Title	Control Description	Included?	Justification
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	•	This Sub-Control helps to ensure that IoT devices that are never intended to be connected to the enterprise network, or only connected to an internal network, are still properly tracked.
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	•	This can present a variety of challenges for IoT devices, as the hardware asset information can drastically change from manufacturer to manufacturer. It can be difficult to standardize field formats as well. Broadly, it is best to collect whatever hardware asset information is available.
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	•	Unknown IoT devices connected to enterprise networks and systems should be quickly investigated and removed.
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	•	It is unlikely that this will be possible for most IoT devices, but if the capability is available, it should be enabled. Note that 802.1x does not work on many IoT devices that do not support supplicant software. Network-level authentication can cause reliability issues if not strictly maintained.
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	•	It is unlikely that this will be possible for many IoT devices, but if the capability to store and utilize certificates within an authentication protocol is available, it should be enabled.

CIS Control 1

CIS

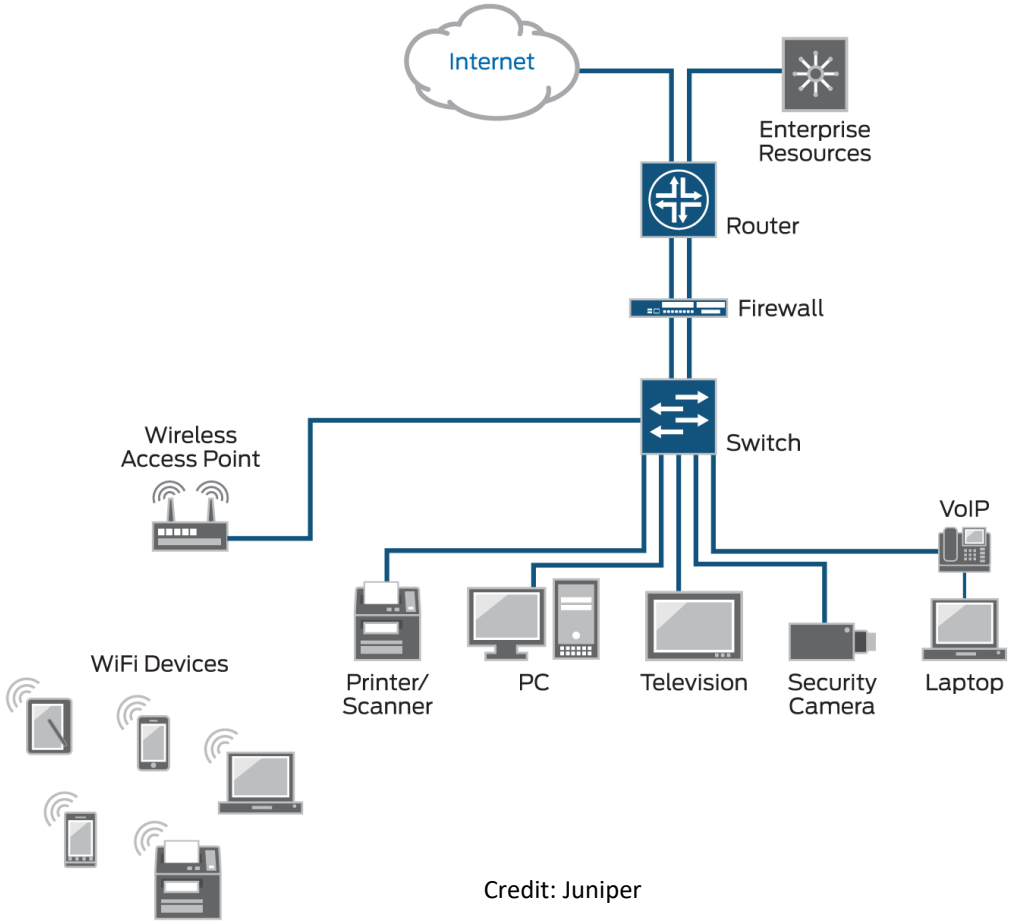
CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Center for Internet Security (CIS)
  - Publish best practices to protect against cyber threats
  - https://www.cisecurity.org/controls/cis-controls-list
  - Non-profit that runs the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- 18 Defined Controls

Inventory and Control of Enterprise Assets	Inventory and Control of Software Assets
Data Protection	Secure Configuration of Enterprise Assets and Software
Account Management	Access Control Management
Continuous Vulnerability Management	Audit Log Management
Email and Web Browser Protections	Malware Defenses
Data Recovery	Network Infrastructure Management
Network Monitoring and Defense	Security Awareness and Skills Training
Service Provider Management	Application Software Security
Incident Response Management	Penetration Testing

Internet of Things

- "NAC 3.0" / Security Automation and Orchestration
- Non-traditional layer 3 devices
  - Printers
  - VoIP Phones
  - Cameras
- Unlikely to enforce device compliance
- Automated onboarding essential
- Poor NAC support



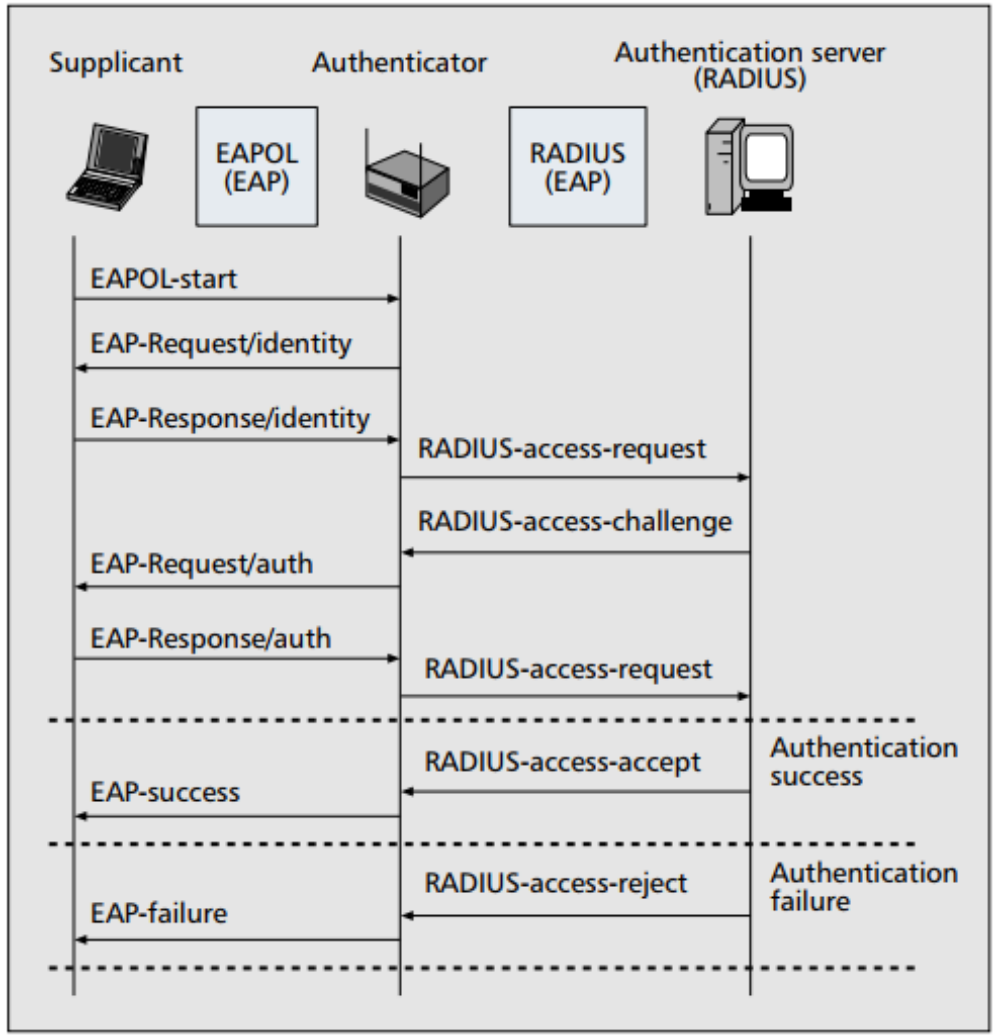
Credit: Juniper

Objectives

- Let's Encrypt
- NAC Overview
- Use Cases
  - Internal Workstations
  - Wireless / BYOD
  - IoT / Field Technology
- 802.1X
  - Common Vulnerabilities
  - EAP-TLS Mechanism
  - Automation
- Attribute-Based Access Control (ABAC)

802.1X Protocol

- Port-based NAC
- Main Components:
  - Supplicant
  - Authenticator
  - Authorization Server
- Utilizes Extensible Authentication Protocol (EAP)
- RADIUS Authentication
  - Allows for auditing
- Enforces Least Privilege Principle
  - Per Subject / User

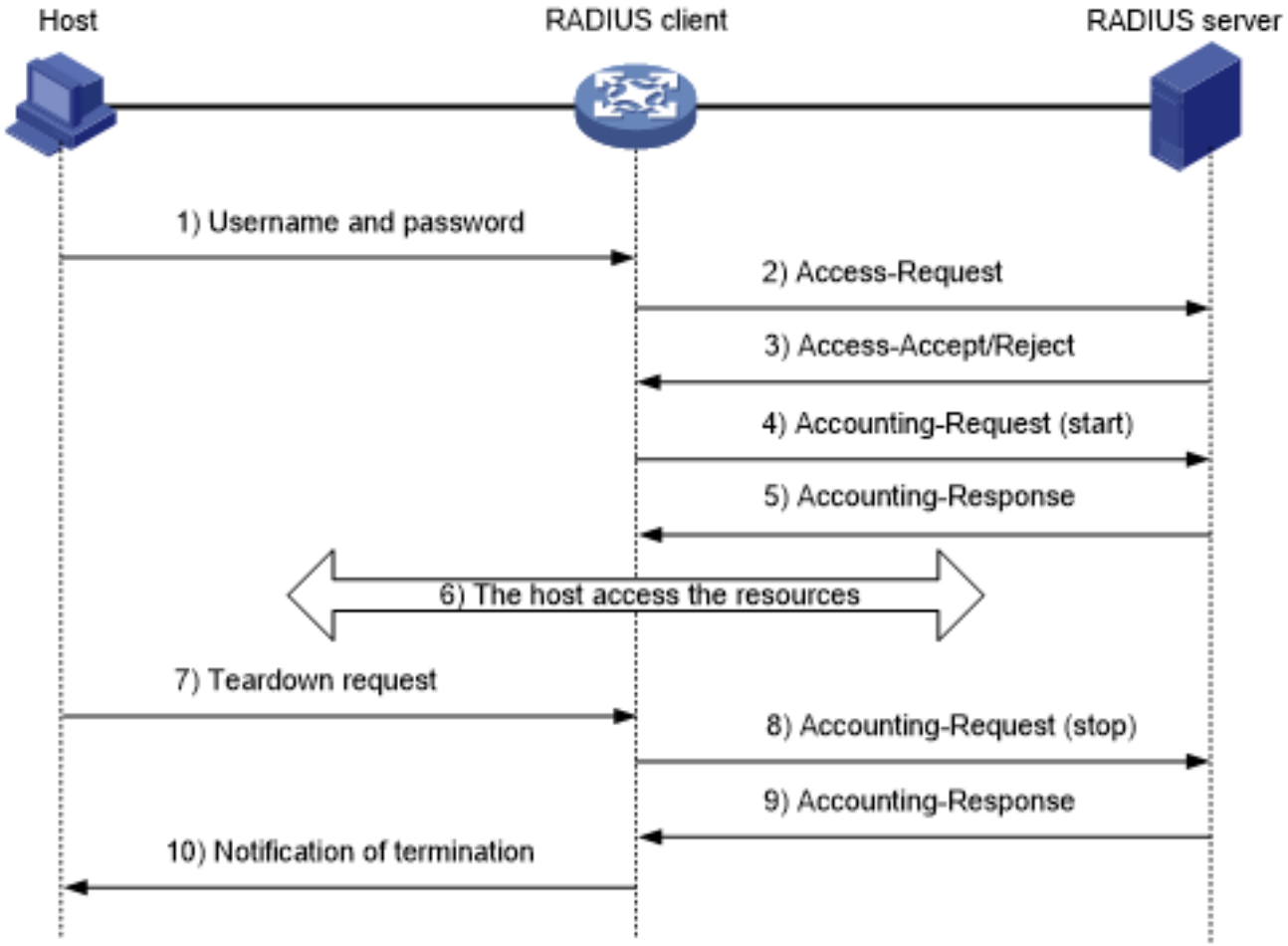


Credit: Chen, et al.

Definitions

- Supplicant
  - Subject requesting access
  - Device and software
- Authenticator
  - Pass-through device (e.g. router, access point)
  - Policy Enforcement Point (PEP)
- Authorization Server
  - Policy Decision Point (PDP)
  - e.g. RADIUS
- EAP (Extensible Authentication Protocol)
  - Authentication framework
  - Authentication initiated by the server (authenticator)
- RADIUS (Remote Authentication Dial-In User Service)
  - RADIUS Client = Networking device used to authenticate users
  - RADIUS Server = Central database of user profiles used to authenticate and authorize access

RADIUS Process



Source: https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485047943.htm

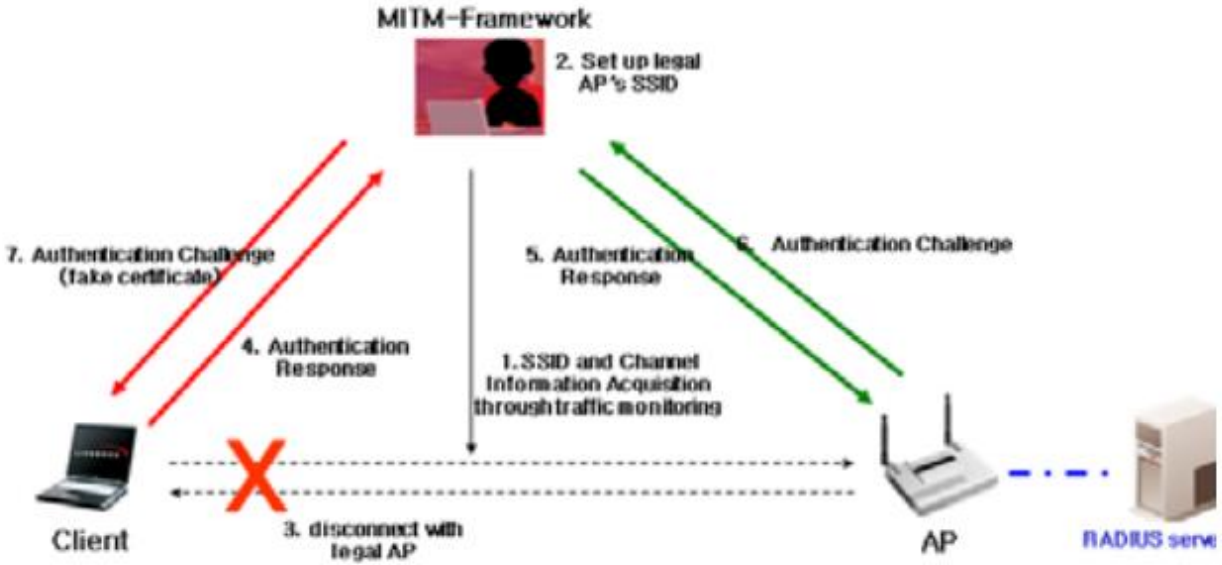
Common EAP Mechanisms

	EAP-MD5 (RFC 1321)	EAP-TLS (RFC 2716)	EAP-TTLS (Internet draft)	PEAP (Internet draft)
Server authentication	No	Public key (certificate)	Public key (certificate)	Public key (certificate)
Supplicant authentication	Password hash	Public key (certificate or smart card)	Certificate, EAP, or non-EAP protocols	Certificate or EAP protocols
Mutual authentication	No	Yes	Yes	Yes
Dynamic key delivery	No	Yes	Yes	Yes
Basic protocol architecture	Challenge/response	Establish TLS session and validate certificates for both client and server	1. Establish TLS between client and TTLS server 2. Exchange attribute-value pairs between client and server	1. Establish TLS between client and PEAP server 2. Run EAP exchanges over TLS tunnel
Server certificate	No	Required	Required	Required
Client certificate	No	Required	Optional	Optional
Protection of user identity	No	No	Yes, protected by TLS	Yes, protected by TLS

Source: Chen, et al.

Vulnerabilities

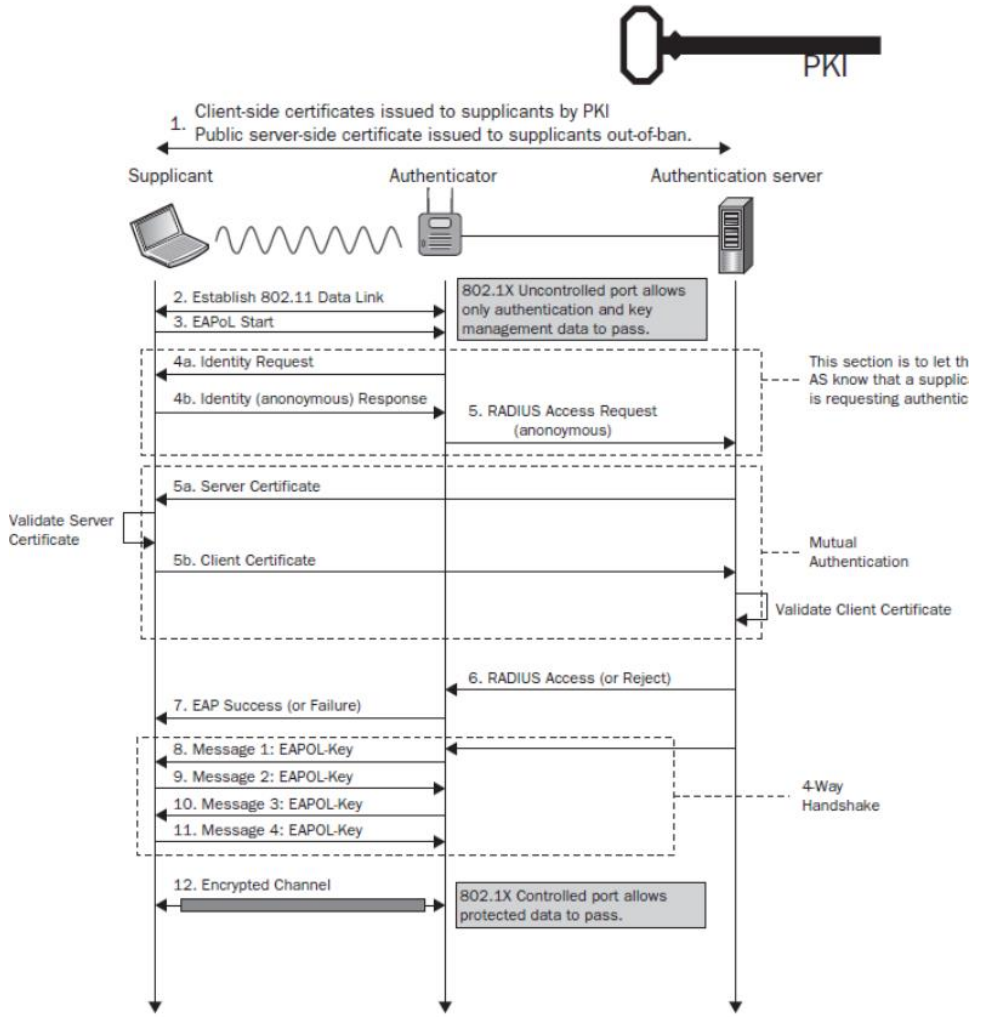
- Man-in-the-middle attacks
  - Need Mutual Authentication
- EAP-PEAP MSCHAPv2
  - Encryption mechanism compromised
- EAP-TTLS
  - Credentials sent in cleartext
- Potential for stolen certificates



Credit: Chen, et al.

EAP-TLS - Process

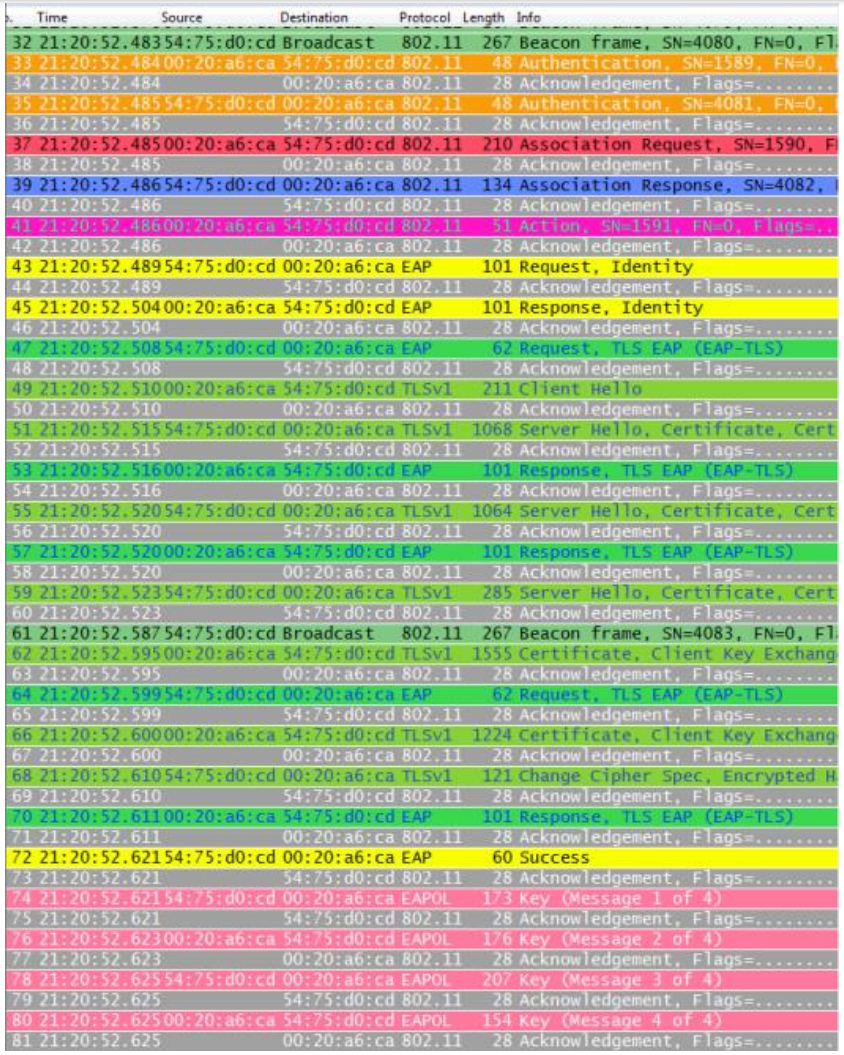
- Certificate distribution
- EAPoL used between Supplicant and Authenticator
- Mutual authentication
- Use of RADIUS for authorization
- Encrypted communication



Credit: Nayarisi (CWNE #153)

EAP-TLS – Packet Capture

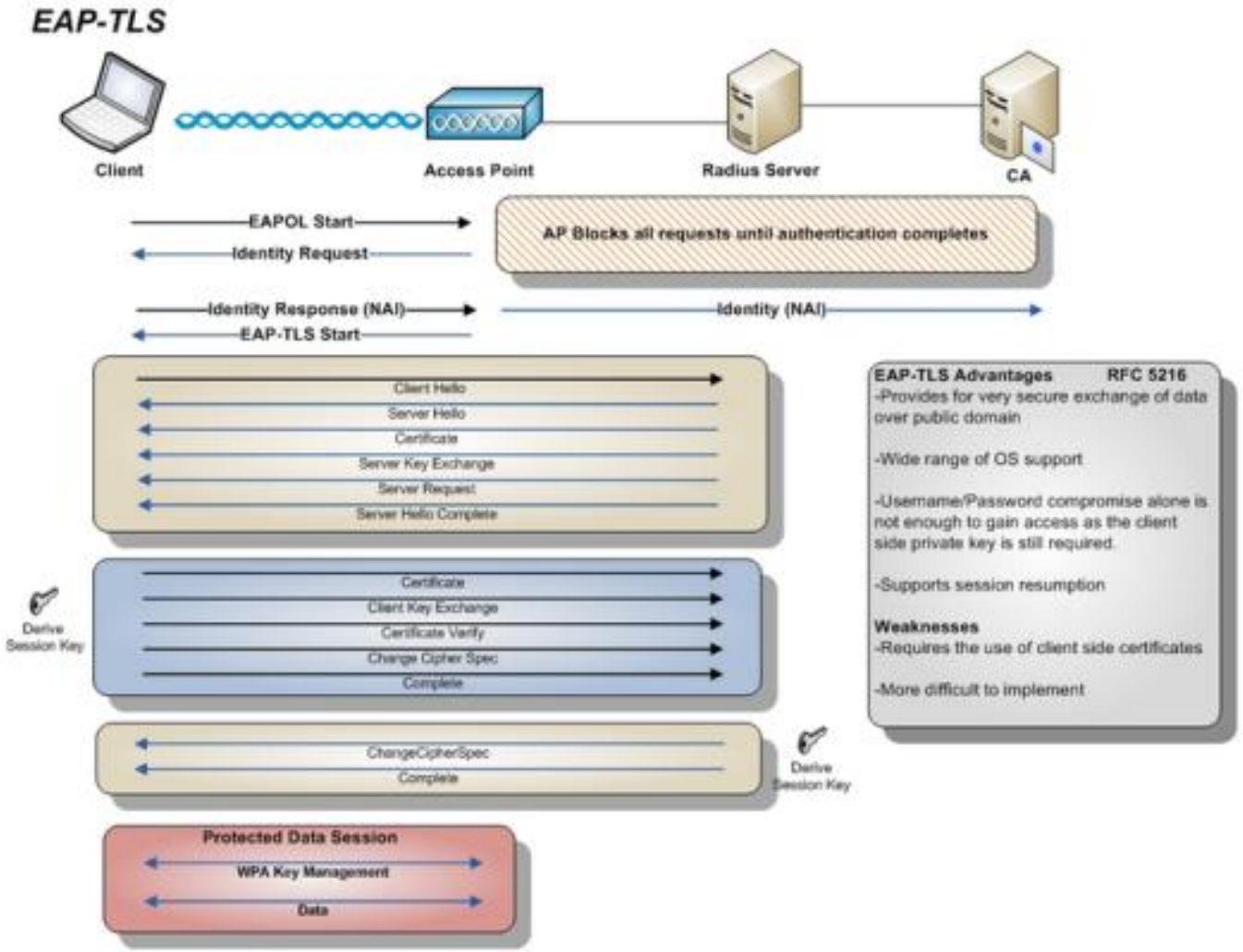
- Supplicant MAC starts with 00:20:a6:ca
- Identity of client not protected
  - Optional to have TLS handshake performed prior to client identity being established
  - Default is client identity sent in cleartext



	Time	Source	Destination	Protocol	Length	Info
32	21:20:52.483	54:75:d0:cd	Broadcast	802.11	267	Beacon frame, SN=4080, FN=0, Fl
33	21:20:52.484	00:20:a6:ca	54:75:d0:cd	802.11	48	Authentication, SN=1589, FN=0,
34	21:20:52.484		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
35	21:20:52.485	54:75:d0:cd	00:20:a6:ca	802.11	48	Authentication, SN=4081, FN=0,
36	21:20:52.485		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
37	21:20:52.485	00:20:a6:ca	54:75:d0:cd	802.11	210	Association Request, SN=1590, Fl
38	21:20:52.485		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
39	21:20:52.486	54:75:d0:cd	00:20:a6:ca	802.11	134	Association Response, SN=4082,
40	21:20:52.486		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
41	21:20:52.486	00:20:a6:ca	54:75:d0:cd	802.11	51	Action, SN=1591, FN=0, Flags=..
42	21:20:52.486		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
43	21:20:52.489	54:75:d0:cd	00:20:a6:ca	EAP	101	Request, Identity
44	21:20:52.489		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
45	21:20:52.504	00:20:a6:ca	54:75:d0:cd	EAP	101	Response, Identity
46	21:20:52.504		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
47	21:20:52.508	54:75:d0:cd	00:20:a6:ca	EAP	62	Request, TLS EAP (EAP-TLS)
48	21:20:52.508		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
49	21:20:52.510	00:20:a6:ca	54:75:d0:cd	TLSv1	211	Client Hello
50	21:20:52.510		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
51	21:20:52.515	54:75:d0:cd	00:20:a6:ca	TLSv1	1068	Server Hello, Certificate, Cert
52	21:20:52.515		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
53	21:20:52.516	00:20:a6:ca	54:75:d0:cd	EAP	101	Response, TLS EAP (EAP-TLS)
54	21:20:52.516		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
55	21:20:52.520	54:75:d0:cd	00:20:a6:ca	TLSv1	1064	Server Hello, Certificate, Cert
56	21:20:52.520		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
57	21:20:52.520	00:20:a6:ca	54:75:d0:cd	EAP	101	Response, TLS EAP (EAP-TLS)
58	21:20:52.520		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
59	21:20:52.523	54:75:d0:cd	00:20:a6:ca	TLSv1	285	Server Hello, Certificate, Cert
60	21:20:52.523		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
61	21:20:52.587	54:75:d0:cd	Broadcast	802.11	267	Beacon frame, SN=4083, FN=0, Fl
62	21:20:52.595	00:20:a6:ca	54:75:d0:cd	TLSv1	1555	Certificate, Client Key Exchang
63	21:20:52.595		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
64	21:20:52.599	54:75:d0:cd	00:20:a6:ca	EAP	62	Request, TLS EAP (EAP-TLS)
65	21:20:52.599		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
66	21:20:52.600	00:20:a6:ca	54:75:d0:cd	TLSv1	1224	Certificate, Client Key Exchang
67	21:20:52.600		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
68	21:20:52.610	54:75:d0:cd	00:20:a6:ca	TLSv1	121	Change Cipher Spec, Encrypted H
69	21:20:52.610		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
70	21:20:52.611	00:20:a6:ca	54:75:d0:cd	EAP	101	Response, TLS EAP (EAP-TLS)
71	21:20:52.611		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
72	21:20:52.621	54:75:d0:cd	00:20:a6:ca	EAP	60	Success
73	21:20:52.621		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
74	21:20:52.621	54:75:d0:cd	00:20:a6:ca	EAPOL	173	Key (Message 1 of 4)
75	21:20:52.621		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
76	21:20:52.623	00:20:a6:ca	54:75:d0:cd	EAPOL	176	Key (Message 2 of 4)
77	21:20:52.623		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....
78	21:20:52.625	54:75:d0:cd	00:20:a6:ca	EAPOL	207	Key (Message 3 of 4)
79	21:20:52.625		54:75:d0:cd	802.11	28	Acknowledgement, Flags=.....
80	21:20:52.625	00:20:a6:ca	54:75:d0:cd	EAPOL	154	Key (Message 4 of 4)
81	21:20:52.625		00:20:a6:ca	802.11	28	Acknowledgement, Flags=.....

Credit: Nayarisi (CWNE #153)

Mutual Certificate Validation



Credit: Nayarisi (CWNE #153)

Need for Automation

- TLS certificate creation and distribution
- Policy compliance
- Increased usage of BYOD
- Increase in working remotely
  - Covid-19 effect
  - VPN connectivity
- IoT Devices
  - Many not compatible with 802.1X
  - Increased adoption among enterprise devices
  - Often positioned in non-secure areas

Sample – NAC Commercial Options

CALIFORNIA STATE UNIVERSITY LONG BEACH
College of Engineering

	Portnox Core	Cisco ISE	Bradford Networks Sentry
100% view of all devices on the network, or attempting to connect to the network	5, Core receives its information from the switches, any connection or attempted connection is known	3, Cisco depends on its supplicant	5, Sentry receives its information from the switches, any connection or attempted connection is known
Central management of the NAC solution	5, Screens are manageable, needed information is consolidated to one location	4, Screens are too busy, have to go through multiple layers to complete a single task	5, Screens are manageable, needed information is consolidated to one location
Ease of use through automation	5, Fully automatable	5, Fully automatable	5, Fully automatable
The solution cannot be labor intensive	5, Fully automatable, rules can trigger any event needed by the administrator	4, Fully automatable, ruleset is limited to what Cisco provides	5, Fully automatable, rules can trigger any event needed by the administrator
Granular rule enforcement and control	5, Rules are very granular. Management roles are very granular.	5, Rules are very granular. Management roles are very granular.	3, Rules are very granular. Management roles are limited.
Automatic onboarding of new systems and guests	5, Onboarding process is automatic.	4, Onboarding is automatic for known device types	5, Onboarding process is automatic.
Confirm compliance control of company owned equipment	5, all devices on the network are reported	4, all devices on the network that a license is available for are reported	5, all devices on the network are reported
Must be able to handle printers, IOT, BYOD, VoIP, etc.	5, All devices are handle by profiles. The profile feed is updated regularly.	4, All devices are handle by profiles. The profile feed is updated regularly. Requires additional licenses.	5, All devices are handle by profiles. The profile feed is updated regularly.
Scale from 1 to 5, with 5 being the best			

Credit: The SANS Institute

Need for 802.1X Capable IoT

- Security focused standards development
- Built-in support for 802.1X certificates
- Standardized API across manufacturers
  - Capable of handling auto-deployed client and server certificates
- Pre-enrollment mechanism
- Move beyond default security profiles to individual client authentication

NAC Summary

- Many components of NAC
  - All need to work together for comprehensive coverage
- Standardization for deployment/configuration of new network devices is key
  - Ad-hoc deployments complicate automation
- Trusted internal certificate authority is needed for EAP-TLS
  - Automated certificate deployment is needed (client and server)
  - Need to “auto-renew” certificates to avoid compromised certificates
- Current state of NAC for IoT devices is primarily profile based
  - Machine learning is helping to make this option more secure
- A well configured NAC includes auditable record keeping
  - Useful for auto-deployments, change management, and system recovery
- Points of Policy concept useful to consider when designing NAC workflow
  - Opens up path to use NAC increasingly for attribute-based authorizations

NAC References

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP – IEEE Computer Society, 2008

Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience – IEEE Radio Communications, December 2005

Federal Acquisition Regulation 52.204-21 (https://www.acquisition.gov/far/52.204-21-0)

Juniper – What is 802.1X Network Access Control (https://www.juniper.net/us/en/products-services/what-is/802-1x-network-access-control/)

MRN-CCIEW – CWSP – EAP TLS (https://mrncciew.com/2014/08/26/cwsp-eap-tls/)

PEAP-MSCHAPv2 Vulnerability Allows For Credential Theft (https://www.securew2.com/blog/peap-mschapv2-vulnerability)

The SANS Institute – Challenges to Implementing Network Access Control (https://www.sans.org/reading-room/whitepapers/access/challenges-implementing-network-access-control-37990)

VMware – Network Access Control (https://www.vmware.com/topics/glossary/content/network-access-control)

What is 802.1X? How Does it Work (https://www.securew2.com/solutions/802-1x)

Objectives

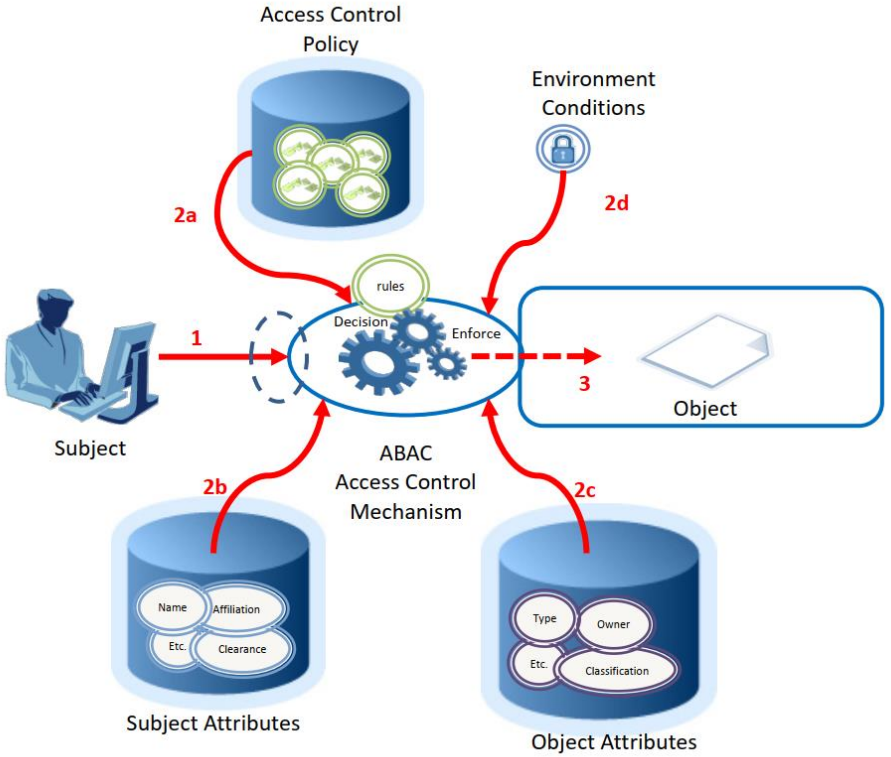
- Let's Encrypt
- NAC Overview
- Use Cases
  - Internal Workstations
  - Wireless / BYOD
  - IoT / Field Technology
- 802.1X
  - Common Vulnerabilities
  - EAP-TLS Mechanism
  - Automation
- Attribute-Based Access Control (ABAC)

ABAC

- Attribute Based Access Control (ABAC)
  - "Access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions."
  - Supports both Discretionary Access Control (DAC) and Mandatory Access Control (MAC)
- Components
  - Attributes: characteristics of the subject, object, and/or environmental conditions
  - Subject: human user or non-person entity (NPE)
  - Object: system resource for which access is managed by the ABAC system
    - e.g. devices, files, processes, networks, data, applications, etc.
  - Operation: execution of a function at the request of a subject upon an object
    - e.g. read, write, delete, copy, execute, or modify
  - Policy: representation of rules and/or relationships that determine if access should be allowed
  - Environmental Conditions: operational or situational context in which access requests occur
    - e.g. time, date, location, or threat level

Source: NIST SP 800-162

ABAC Model



1. Subject requests access to object
2. Access Control Mechanism evaluates a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to compute a decision
3. Subject is given access to object if authorized

Figure 2: Basic ABAC Scenario

Source: NIST SP 800-162

ABAC (cont'd)

- Important Terms
  - Natural Language Policy (NLP): Human-readable statements regarding access to enterprise objects
  - Digital Policy (DP): Access control rules written as machine executable code (used by an access control mechanism)
    - Built using subject/object attributes, operations, and environmental conditions
  - Metapolicy (MP): Policy for managing policies. Used to resolve conflicts between DPs or other MPs in complex use cases
- Access Control Mechanism (ACM) Function Points
  - Policy Decision Point (PDP): Computes access decisions by evaluating application DPs and MPs
  - Policy Enforcement Point (PEP): Enforces policy decisions in response to a subject requesting access to a protected object
    - PEP enforces decisions made by the PDP
  - Policy Information Point (PIP): Source of information for attributes assigned to subjects and objects
    - Provides data to the PDP to make decisions
  - Policy Administration Point (PAP): User interface for creating, managing, and testing DPs and MPs

ACM Example

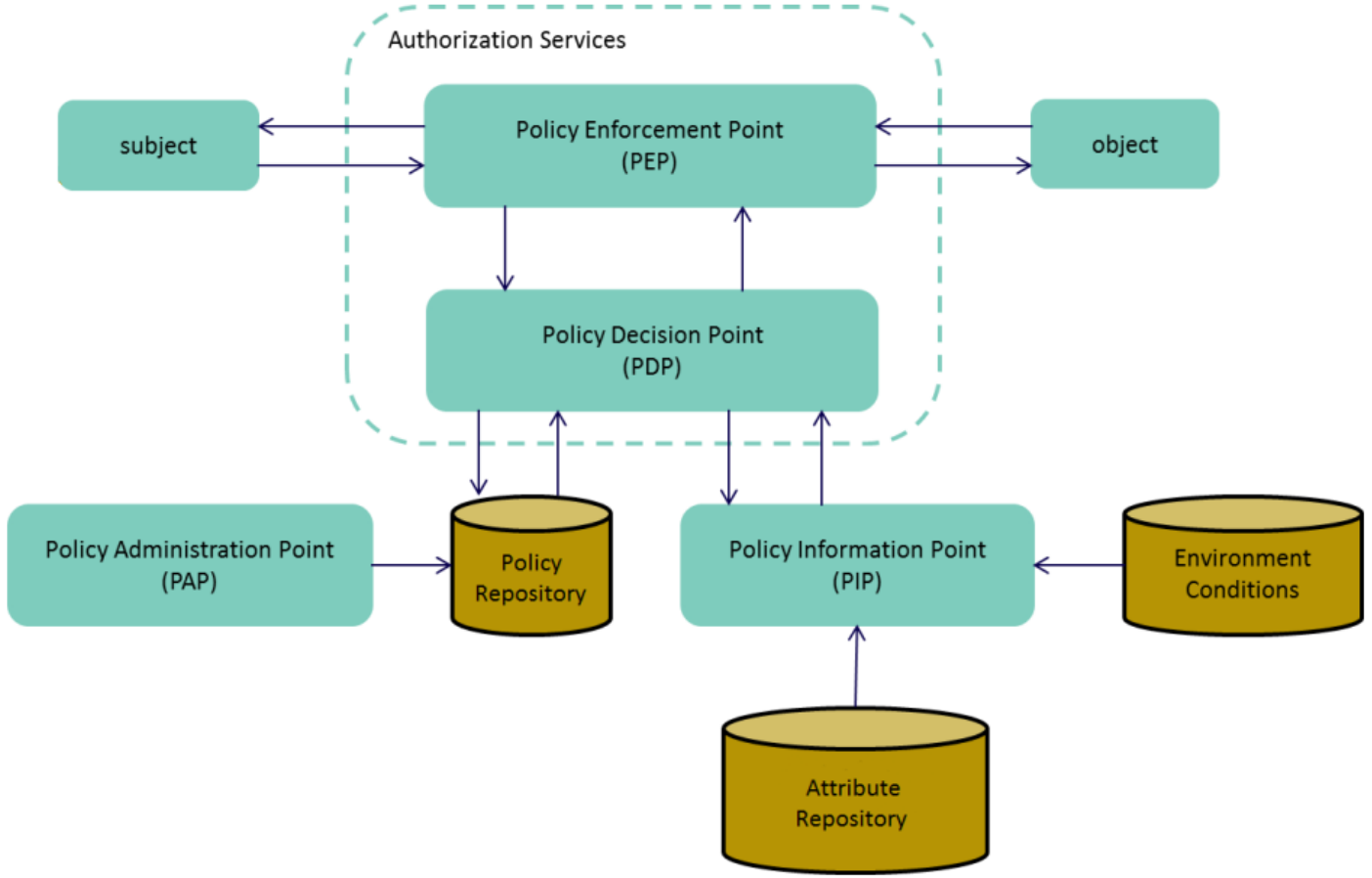


Figure 5: An Example of ACM Functional Points

Source: NIST SP 800-162