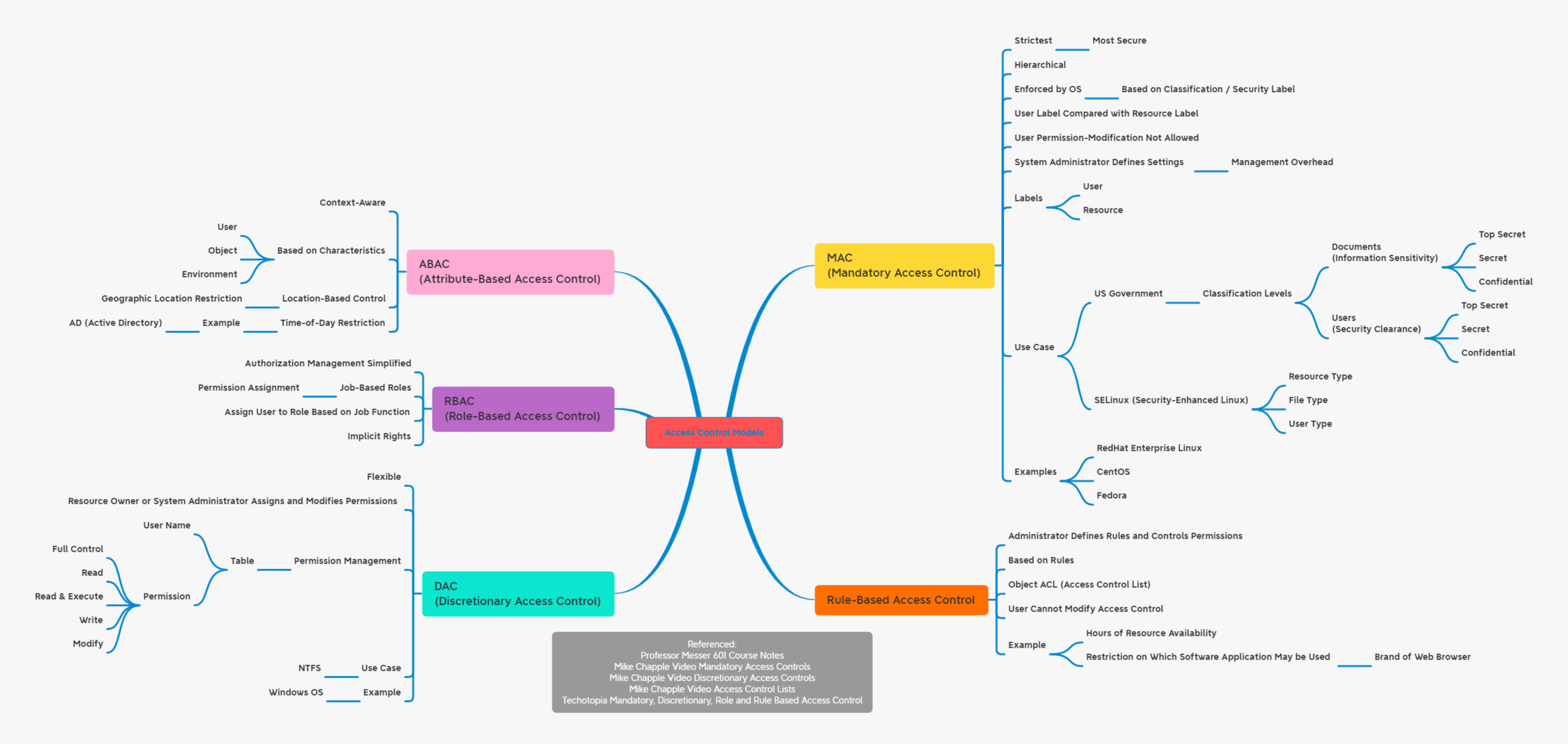
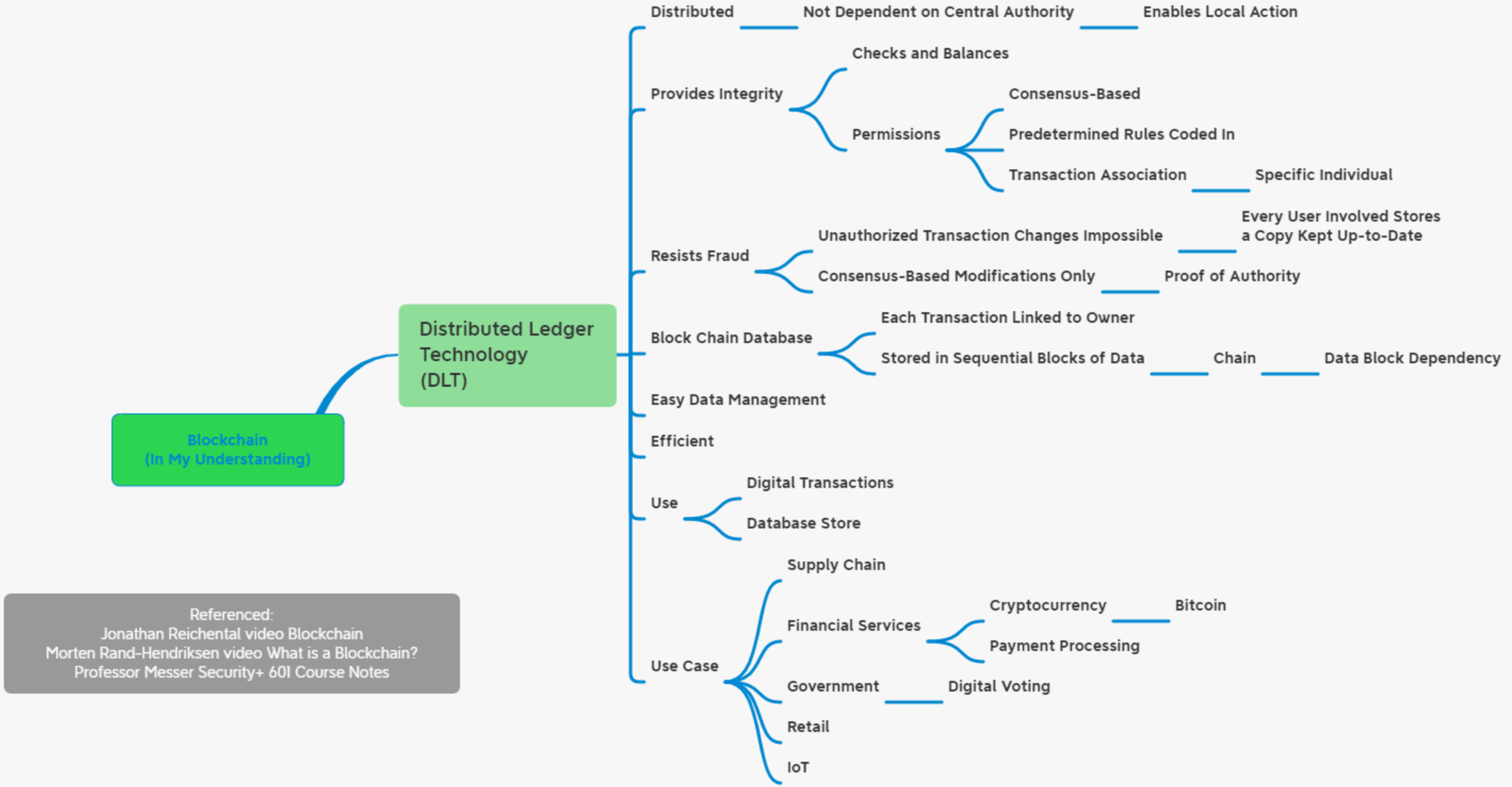
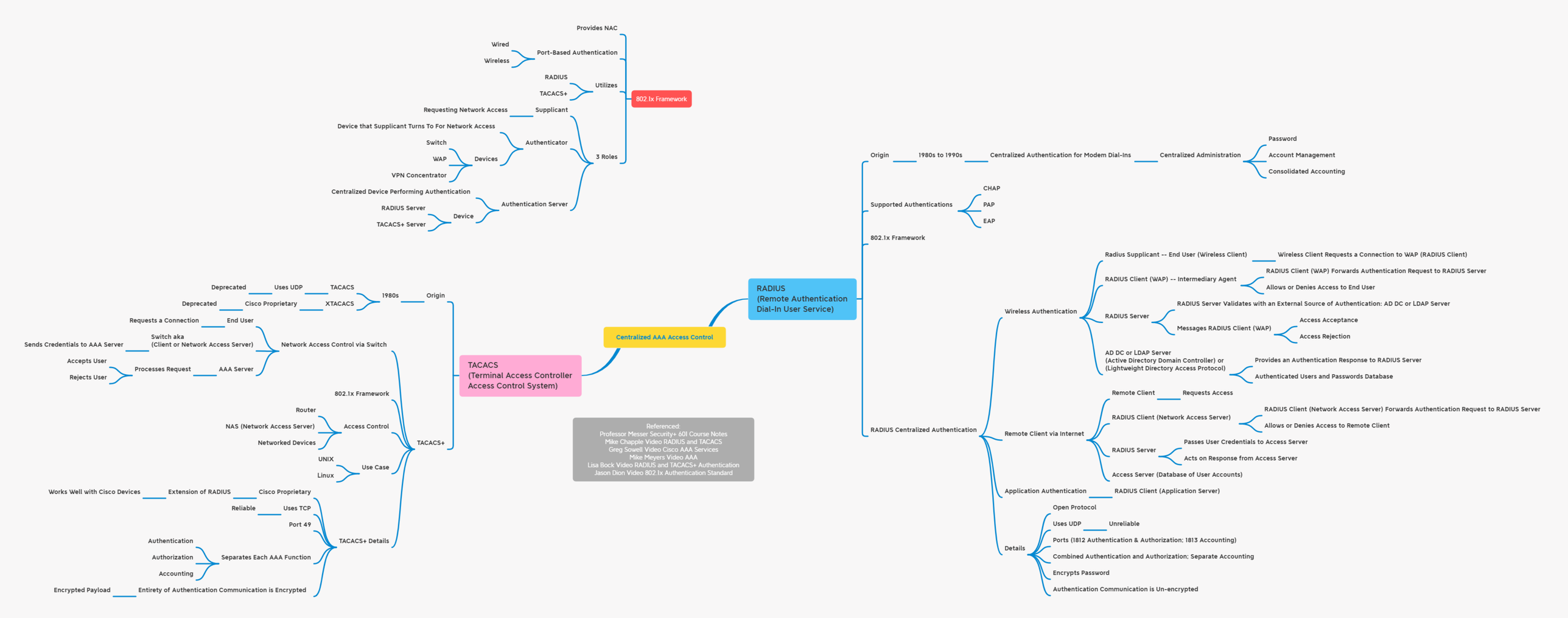
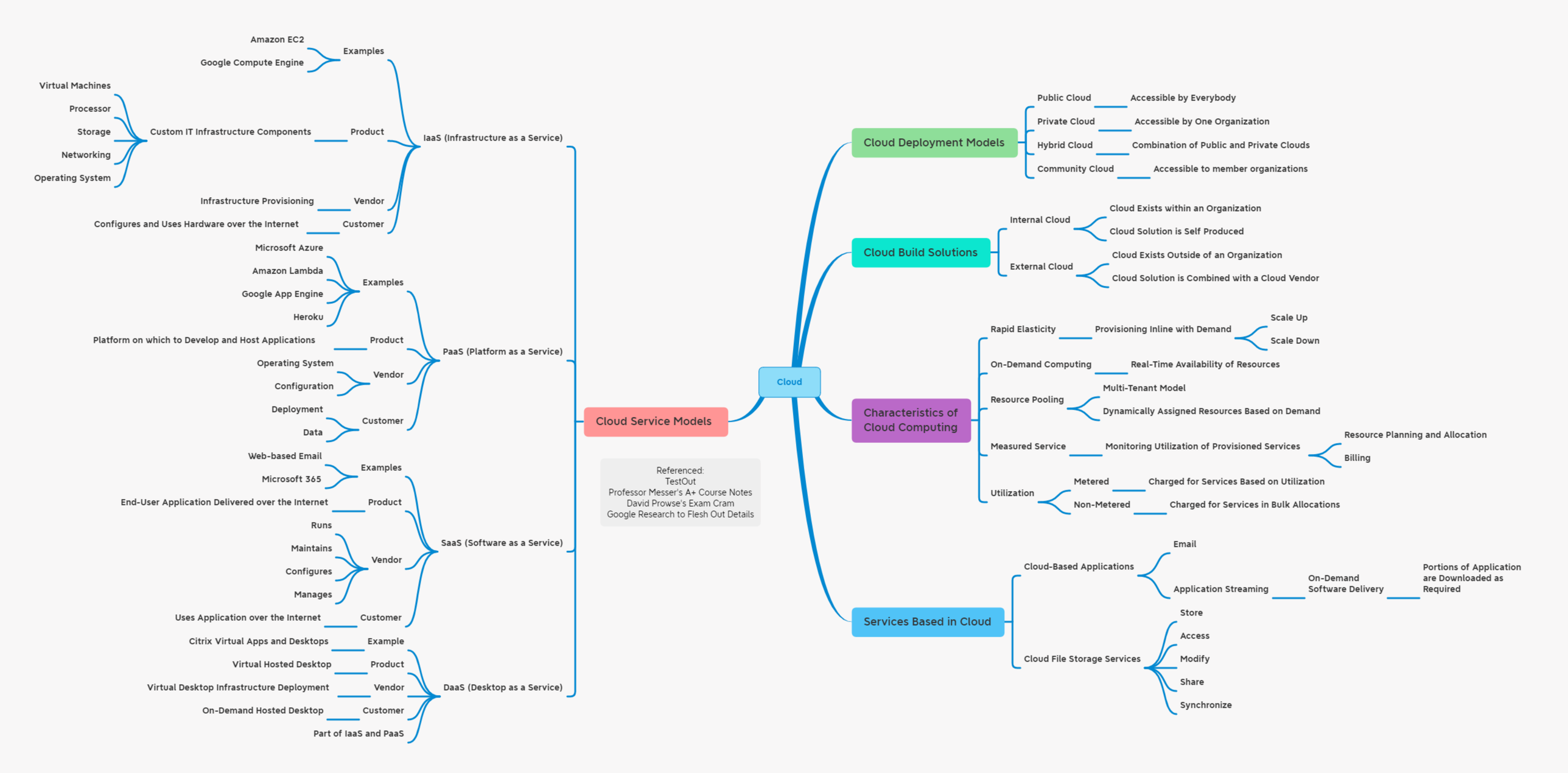

Access Control Models
MAC
(Mandatory Access Control)
Strictest
Most Secure
Hierarchical
Enforced by OS
Based on Classification / Security Label
User Label Compared with Resource Label
User Permission-Modification Not Allowed
System Administrator Defines Settings
Management Overhead
Labels
User
Resource
Use Case
US Government
Classification Levels
Documents
(Information Sensitivity)
Top Secret
Secret
Confidential
Users
(Security Clearance)
Top Secret
Secret
Confidential
SELinux (Security-Enhanced Linux)
Resource Type
File Type
User Type
Examples
RedHat Enterprise Linux
CentOS
Fedora
ABAC
(Attribute-Based Access Control)
Context-Aware
Based on Characteristics
User
Object
Environment
Location-Based Control
Geographic Location Restriction
Time-of-Day Restriction
Example
AD (Active Directory)
RBAC
(Role-Based Access Control)
Authorization Management Simplified
Job-Based Roles
Permission Assignment
Assign User to Role Based on Job Function
Implicit Rights
DAC
(Discretionary Access Control)
Flexible
Resource Owner or System Administrator Assigns and Modifies Permissions
Permission Management
Table
User Name
Permission
Full Control
Read
Read & Execute
Write
Modify
Use Case
NTFS
Example
Windows OS
Rule-Based Access Control
Administrator Defines Rules and Controls Permissions
Based on Rules
Object ACL (Access Control List)
User Cannot Modify Access Control
Example
Hours of Resource Availability
Restriction on Which Software Application May be Used
Brand of Web Browser
Referenced:
Professor Messer 601 Course Notes
Mike Chapple Video Mandatory Access Controls
Mike Chapple Video Discretionary Access Controls
Mike Chapple Video Access Control Lists
Techotopia Mandatory, Discretionary, Role and Rule Based Access Control


Blockchain
(In My Understanding)
Distributed Ledger Technology (DLT)
Distributed
Not Dependent on Central Authority
Enables Local Action
Provides Integrity
Checks and Balances
Permissions
Consensus-Based
Predetermined Rules Coded In
Transaction Association
Specific Individual
Resists Fraud
Unauthorized Transaction Changes Impossible
Every User Involved Stores a Copy Kept Up-to-Date
Consensus-Based Modifications Only
Proof of Authority
Block Chain Database
Each Transaction Linked to Owner
Stored in Sequential Blocks of Data
Chain
Data Block Dependency
Easy Data Management
Efficient
Use
Digital Transactions
Database Store
Use Case
Supply Chain
Financial Services
Cryptocurrency
Bitcoin
Payment Processing
Government
Digital Voting
Retail
IoT
Referenced:
Jonathan Reichental video Blockchain
Morten Rand-Hendriksen video What is a Blockchain?
Professor Messer Security+ 601 Course Notes


802.1x Framework
Provides NAC
Port-Based Authentication
Wired
Wireless
Utilizes
RADIUS
TACACS+
3 Roles
Supplicant
Requesting Network Access
Authenticator
Device that Supplicant Turns To For Network Access
Devices
Switch
WAP
VPN Concentrator
Authentication Server
Centralized Device Performing Authentication
Device
RADIUS Server
TACACS+ Server
Centralized AAA Access Control
TACACS
(Terminal Access Controller
Access Control System)
Origin
1980s
TACACS
Uses UDP
Deprecated
XTACACS
Cisco Proprietary
Deprecated
Network Access Control via Switch
End User
Requests a Connection
Switch aka
(Client or Network Access Server)
Sends Credentials to AAA Server
AAA Server
Processes Request
Accepts User
Rejects User
TACACS+
802.1x Framework
Access Control
Router
NAS (Network Access Server)
Networked Devices
Use Case
UNIX
Linux
TACACS+ Details
Cisco Proprietary
Extension of RADIUS
Works Well with Cisco Devices
Uses TCP
Reliable
Port 49
Separates Each AAA Function
Authentication
Authorization
Accounting
Entirety of Authentication Communication is Encrypted
Encrypted Payload
RADIUS
(Remote Authentication
Dial-In User Service)
Origin
1980s to 1990s
Centralized Authentication for Modem Dial-Ins
Centralized Administration
Password
Account Management
Consolidated Accounting
Supported Authentications
CHAP
PAP
EAP
802.1x Framework
RADIUS Centralized Authentication
Wireless Authentication
Radius Supplicant -- End User (Wireless Client)
Wireless Client Requests a Connection to WAP (RADIUS Client)
RADIUS Client (WAP) -- Intermediary Agent
RADIUS Client (WAP) Forwards Authentication Request to RADIUS Server
Allows or Denies Access to End User
RADIUS Server
RADIUS Server Validates with an External Source of Authentication: AD DC or LDAP Server
Messages RADIUS Client (WAP)
Access Acceptance
Access Rejection
AD DC or LDAP Server
(Active Directory Domain Controller) or
(Lightweight Directory Access Protocol)
Provides an Authentication Response to RADIUS Server
Authenticated Users and Passwords Database
Remote Client via Internet
Remote Client
Requests Access
RADIUS Client (Network Access Server)
RADIUS Client (Network Access Server) Forwards Authentication Request to RADIUS Server
Allows or Denies Access to Remote Client
RADIUS Server
Passes User Credentials to Access Server
Acts on Response from Access Server
Access Server (Database of User Accounts)
Application Authentication
RADIUS Client (Application Server)
Details
Open Protocol
Uses UDP
Unreliable
Ports (1812 Authentication & Authorization; 1813 Accounting)
Combined Authentication and Authorization; Separate Accounting
Encrypts Password
Authentication Communication is Un-encrypted
Referenced:
Professor Messer Security+ 601 Course Notes
Mike Chapple Video RADIUS and TACACS
Greg Sowell Video Cisco AAA Services
Mike Meyers Video AAA
Lisa Bock Video RADIUS and TACACS+ Authentication
Jason Dion Video 802.1x Authentication Standard


Cloud
Cloud Service Models
IaaS (Infrastructure as a Service)
Examples
Amazon EC2
Google Compute Engine
Product
Custom IT Infrastructure Components
Virtual Machines
Processor
Storage
Networking
Operating System
Vendor
Infrastructure Provisioning
Customer
Configures and Uses Hardware over the Internet
PaaS (Platform as a Service)
Examples
Microsoft Azure
Amazon Lambda
Google App Engine
Heroku
Product
Platform on which to Develop and Host Applications
Vendor
Operating System
Configuration
Customer
Deployment
Data
SaaS (Software as a Service)
Examples
Web-based Email
Microsoft 365
Product
End-User Application Delivered over the Internet
Vendor
Runs
Maintains
Configures
Manages
Customer
Uses Application over the Internet
DaaS (Desktop as a Service)
Example
Citrix Virtual Apps and Desktops
Product
Virtual Hosted Desktop
Vendor
Virtual Desktop Infrastructure Deployment
Customer
On-Demand Hosted Desktop
Part of IaaS and PaaS
Referenced:
TestOut
Professor Messer's A+ Course Notes
David Prowse's Exam Cram
Google Research to Flesh Out Details
Cloud Deployment Models
Public Cloud
Accessible by Everybody
Private Cloud
Accessible by One Organization
Hybrid Cloud
Combination of Public and Private Clouds
Community Cloud
Accessible to member organizations
Cloud Build Solutions
Internal Cloud
Cloud Exists within an Organization
Cloud Solution is Self Produced
External Cloud
Cloud Exists Outside of an Organization
Cloud Solution is Combined with a Cloud Vendor
Characteristics of Cloud Computing
Rapid Elasticity
Provisioning Inline with Demand
Scale Up
Scale Down
On-Demand Computing
Real-Time Availability of Resources
Resource Pooling
Multi-Tenant Model
Dynamically Assigned Resources Based on Demand
Measured Service
Monitoring Utilization of Provisioned Services
Resource Planning and Allocation
Billing
Utilization
Metered
Charged for Services Based on Utilization
Non-Metered
Charged for Services in Bulk Allocations
Services Based in Cloud
Cloud-Based Applications
Email
Application Streaming
On-Demand Software Delivery
Portions of Application are Downloaded as Required
Cloud File Storage Services
Store
Access
Modify
Share
Synchronize

Computer Malware

Signs
- System Performance
- Pop-Ups
- Running Programs
- File Duplication
- File Creation
- File Deletion
- File Corruption

Operation
- Replication
- Residency
- Evasion
  - Antivirus
  - Antimalware

Effects
- Infection
- Modification
- Deletion
- Encryption
- Extraction
  - Transmit Covertly
- Resource Consumption

Methods
- Email
  - Attachment
- Web
  - Website
  - Advertisement
- File
- Removable Media
  - USB
- Network

Purpose
- Harm
- Elevated Access Control
- Extract
  - Passwords
  - Data
    - Logging Keystrokes
- Corrupt
- Command and Control
- Residency
- Reproduce

Locations
- Memory
- Registries
- Macros

Referenced:
Google
Exam Cram Security+ 601
Professor Messer Course Notes 601
Blog: Comodo Antivirus: What is a Computer Virus?

Types
- Crypto-Malware
  - Ransomware
- Trojans
  - Remote Access Trojan (RAT)
  - Keylogger
  - Backdoor
  - Trojan Horse
- Worms
- Potentially Unwanted Programs (PUPs)
  - Spyware
  - Adware
  - Cryptomining
- Command and Control
  - Bot (Robot)
  - Botnet (Zombie Army)
- Logic Bombs
- Root Kit
  - Covert Installation
  - Backdoor
  - Command and Control
- Virus
- Keylogger

Classification
- Armored
  - Difficult to Reverse Engineer
- Stealth
  - Avoids Detection
    - Moves
    - Renames
- Non-Resident
  - Memory
  - Attached to File
- Resident
  - Memory Implantation
  - Fileless
- Multipartite
  - Boot Sector
  - Executables
- Polymorphic
  - Alters Signature Upon Replication
    - Evades Detection
  - Changes Code
  - Keeps Function
- Spacefiller
  - Lives in File Cavities
  - File Size Remains Intact
- Boot Sector
  - Master Boot Record
- Boot Record
  - System Area
    - USB Drives
    - Diskette
      - DOS Boot Sector
    - Hard Drive
      - Master Boot Record
- Script
  - Malicious Website Code
- Macro
  - Macro Language Commands
  - Insert Malicious Code into Macro Sequence
  - Launch Virus
- Overwrite
  - Overwrite Files
    - Insert Code
      - Spread
- File Infectors
  - Attached To
    - .com
    - .exe
    - script
  - Infect Programs Executed and Load

Cryptographic Algorithms

One Way

ONE WAY ONLY ⟶

Hashing

File Integrity Check

- CRC32
- MD5
- SHA Family
- HMAC
- RIPEMD

Password Hashing Algorithms

- Argon2
- Bcrypt
- PBKDF2
- Scrypt

Two Way

Encryption

Key

Symmetric

Secret Key
(1 Key that is Shared by 2)

- Block
  - Block Encryption
    - DES
    - 3DES
    - AES
    - Blowfish
    - Twofish
    - IDEA
  - Cipher Modes
    - ECB
    - CBC
    - CTM
    - GCM
- Stream
  - RC4

Asymmetric

Public Key
(Public & Private Keys)

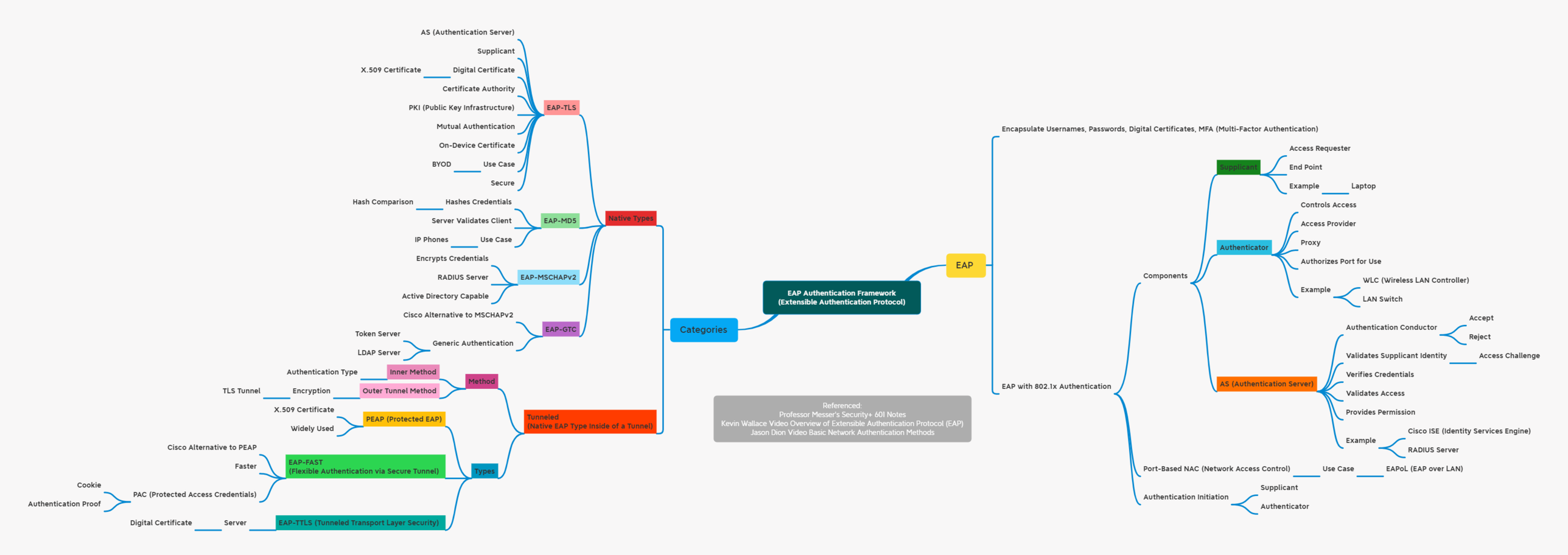
- RSA (Rivest Shamir Adleman)
- ECC (Elliptic Curve Cryptography)
- DHE (Diffie-Hellman Ephemeral)
- ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)

Keyless Cipher

- Shift
- Substitution
  - Caesar
- Transposition
  - Reil Fence
- Polyalphabetic
- Nomenclator

- Cryptography
  - Symmetric Cryptography
    - Block Cipher
      - Block Cipher Algorithms
        - DES
          - 1970s
          - Federal Encryption Standard
            - Deprecated
            - Insecure
          - Method: Substitution & Transposition Functions
          - Operates on 64 Bit Blocks
          - 56 Bit Key
        - 3DES
          - 1990s
          - Temporary Workaround
            - Phasing Out
            - Not Recommended — Weak
          - Uses DES Algorithm 3 Times
          - Operates on 64 Bit Blocks
          - Key Options
            - Keys 1, 2, 3 Are Different
              - 112 Bit Key
              - Strong
            - Key 1 Equals Key 3 — 80 Bit Key
            - All Three Keys Are Equal
              - Insecure as DES
              - Backwards Compatible with DES
        - Blowfish
          - 1993
          - Not Secure
          - Method: Substitution & Transposition Functions
          - Operates on 64 Bit Blocks
          - Key Length Options — Between 32 Bits and 448 Bits
        - Twofish
          - 1998
          - Secure
          - Method: Substitution & Transposition Functions
          - Operates on 64 Bit Blocks
          - Key Length Options
            - 128 Bit Key
            - 192 Bit Key
            - 256 Bit Key
        - AES (Advanced Encryption Standard)
          - 2001
          - Secure — All Key Lengths
          - Current US Federal Government Standard
          - Method: Substitution & Transposition Functions
          - 128 Bit Blocks
          - Key Length Options
            - 128 Bit Key
            - 192 Bit Key
            - 256 Bit Key
      - Block Cipher Modes
        - ECB Mode (Electronic Codebook)
          - Confidentiality
          - Same Key Applied to Blocks
        - CBC Mode (Cipher Block Chaining)
          - Confidentiality
          - IV for First Block
          - XOR with Previous Block
        - CTR Mode (Counter)
          - Confidentiality
          - Acts Similar to Stream Cipher
        - GCM Mode (Galois/Counter Mode)
          - Variant of CTR Mode
          - Confidentiality
          - Galois Authentication
          - Efficient
          - Use Case
            - Wireless
            - IPsec
            - SSH
            - TLS
    - Stream Cipher
      - RC4
        - 1987
        - Unsecure
        - Uses
          - WEP, WPA
          - SSL, TLS
        - Pseudo-random Stream of Bits
        - Selected Initialization Key
        - Same Key Created by Sender and Receiver
        - Key Length Options — Between 40 Bits and 2048 Bits
  - Asymmetric Cryptography
    - Key Exchange Algorithms (Key Agreement Protocols) For Sharing of Symmetric Key
      - No Encryption
      - No Authentication
      - 1976
        - DH Algorithm (Diffie-Hellman)
        - ECDH Algorithm (Elliptic Curve Diffie-Hellman)
    - PGP Framework (Pretty Good Privacy) Based on PKI (Public Key Infrastructure) Can Use DH or RSA Algorithms
      - 1991
      - Key Pair
      - Combination of Symmetric and Asymmetric Cryptography
      - Encryption Process
        - Random Symmetric Key Created by Sender
        - Data Encrypted with Random Key by Sender
        - Random Key Encrypted with Recipient's Public Key by Sender
      - Decryption Process
        - Random Key is Decrypted with Private Key by Recepient
        - Decrypt Data with Random Key by Recepient
      - Example
        - GnuPG
        - GPG
    - RSA Algorithm (Rivest, Shamir, Adleman)
      - 1977
      - Based on Key Length — Secure
      - Slow
      - Public Key Cryptography System
      - Prime Factorization — Factoring Prime Numbers
      - 2 Large Prime Numbers — User Chooses Key Pair
        - Keys are Derived
          - Shareable — Public
          - Keep Confidential — Private
      - Sender Encrypts with Recipient's Public Key
      - Recipient Decrypts with Recipient's Private Key
      - Key Length Options — Between 1024 Bits and 4096 Bits
      - Use Case
        - Initial Secure Channel — Exchange Symmetric Key — Encryption via Symmetric Key
    - ECC (Elliptic Curve Cryptography)
      - 2004
      - Uses Curves — Elliptic Curve Discrete Logarithm
      - Smaller Keys
      - Can Be Attacked by Quantum Computing
    - Quantum Cryptography — Quantum Mechanics

Referenced:
Professor Messer Security+ 601 Course Notes
Professor Messer Security+ 501 Course Notes
Mike Chapple Videos Symmetric Cryptography
Mike Chapple Videos Asymmetric Cryptography
Mike Chapple Videos Key Management
Wikipedia


EAP Authentication Framework
(Extensible Authentication Protocol)
EAP
Encapsulate Usernames, Passwords, Digital Certificates, MFA (Multi-Factor Authentication)
EAP with 802.1x Authentication
Components
Supplicant
Access Requester
End Point
Example
Laptop
Authenticator
Controls Access
Access Provider
Proxy
Authorizes Port for Use
Example
WLC (Wireless LAN Controller)
LAN Switch
AS (Authentication Server)
Authentication Conductor
Accept
Reject
Validates Supplicant Identity
Access Challenge
Verifies Credentials
Validates Access
Provides Permission
Example
Cisco ISE (Identity Services Engine)
RADIUS Server
Port-Based NAC (Network Access Control)
Use Case
EAPoL (EAP over LAN)
Authentication Initiation
Supplicant
Authenticator
Categories
Native Types
EAP-TLS
AS (Authentication Server)
Supplicant
X.509 Certificate
Digital Certificate
Certificate Authority
PKI (Public Key Infrastructure)
Mutual Authentication
On-Device Certificate
BYOD
Use Case
Secure
EAP-MD5
Hash Comparison
Hashes Credentials
Server Validates Client
IP Phones
Use Case
EAP-MSCHAPv2
Encrypts Credentials
RADIUS Server
Active Directory Capable
EAP-GTC
Cisco Alternative to MSCHAPv2
Generic Authentication
Token Server
LDAP Server
Tunneled
(Native EAP Type Inside of a Tunnel)
Method
Inner Method
Authentication Type
Outer Tunnel Method
Encryption
TLS Tunnel
Types
PEAP (Protected EAP)
X.509 Certificate
Widely Used
EAP-FAST
(Flexible Authentication via Secure Tunnel)
Cisco Alternative to PEAP
Faster
PAC (Protected Access Credentials)
Cookie
Authentication Proof
EAP-TTLS (Tunneled Transport Layer Security)
Digital Certificate
Server
Referenced:
Professor Messer's Security+ 601 Notes
Kevin Wallace Video Overview of Extensible Authentication Protocol (EAP)
Jason Dion Video Basic Network Authentication Methods

- Fog Computing
  - Extends Cloud Continuum
  - Decentralized Cloud
  - Distributed Model
  - Hardware and Software Solution
  - Horizontal: IoT Device Integration
    - Analytics
      - Anomaly Detection
      - Failure Prediction
      - Optimization
      - Machine Learning
    - Interoperability
  - Vertical: IoT Interconnection Across Domains
    - Sharing
      - Resource
      - Data
      - Service
  - End-to-End Security
- Fog
  - Fog Processing
    - Local-Level Intelligence
    - Reduced Bandwidth
      - Local Control, Collection, Processing, Analysis of Sensor Data
      - Partial Data Upload to the Cloud
    - Scalable
    - Low Latency
      - Real-Time Data Analysis and Monitoring
      - Time-to-Response
      - Time-to-Action
      - Mission-Critical Decision
    - Efficiency
    - Security
      - Data Remains Local — Privacy
      - Vulnerability in IoT
  - Use Case
    - Smart Phone Facial Recognition
    - Jet Engine Sensor
  - Application
    - Industrial Automation
    - Smart Cities
    - Oil and Gas
    - Transportation
    - Material and Goods
    - Agriculture
- Fog Computing
  - Geographically Accessible
  - Centralized Resources
- Cloud
  - Distant
  - Big Data Analytics
  - Connectivity

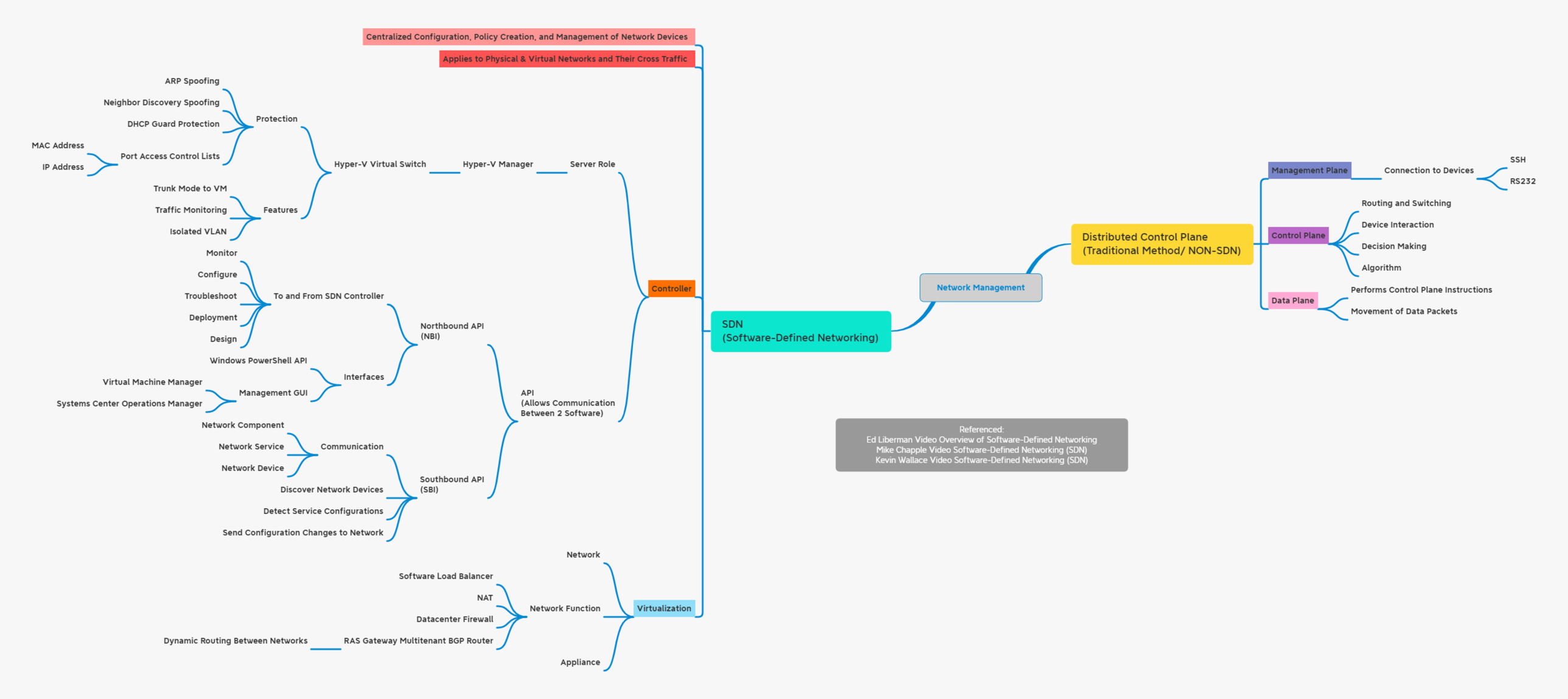
Referenced:
Google
Article: Medium: Primer on Edge Computing by Arin Dey
Mike Chapple Security+ 601 Videos
Lisa Bock Securing the IoT: Introduction Video
Barton Poulson Edge Computing and Fog Computing Video
Nebbiolo Technologies PDF Fog vs Edge Computing

IP Sec Authentication & Encapsulation Standard (As I Understand It)

- OSI Layer 3: Network Layer
- * For the Creation of this Mind Map, I Referenced the following eBooks.
  - Ian Neil's CompTIA Security+: SY0-601 Certification Guide
  - Martin Weiss's CompTIA Security+ SY0-601 Exam Cram
  - Professor Messer's CompTIA Security+ SY0-501 Course Notes
- Use Case
  - VPN (Secure Session between two Hosts on a Network)
- 2 Modes
  - Tunnel
    - L2TP/IPSec
    - Default Mode
    - Between Gateways
      - Router
      - Firewall
    - Uses AH or ESP Header
    - Asymmetric Key
    - Encryption
      - Header
      - Payload
    - Used Externally
  - Transport
    - Between End Points
      - Client/Server
      - Server/Server
      - Client/Client
      - RDP Session
    - Ecryption
      - Payload
    - Used with an Internal Network
- 2 Protocols: Component Characteristics
  - ESP
    - Data Confidentiality
      - Encryption of Data
      - Independently of other Services
    - Authentication of Sender of Data
    - Limited Traffic Flow Confidentiality
    - Data Integrity
    - Anti-Replay Protection
  - AH
    - Data Integrity
    - Authentication of Sender of Data
    - Nonrepudiation
    - Replay Attack Protection
    - Keyed-Hash Mechanism
    - No Confidentiality/Encryption
    - IP Header Fields May be Modified in Transit
- Protocols
  - AH (Authentication Header)
    - Hash of Packet (Confirms Packet Integrity)
      - MD5
      - SHA-1
      - SHA-2
    - Shared Key
  - ESP (Encapsulation Security Payload)
    - Header
    - Trailer
    - Integrity Check Value
    - Encryption of Data (Symmetric Encryption Using Block Cipher)
      - DES
      - 3DES
      - AES
    - Hash
      - MD5
      - SHA-1
      - SHA-2
  - IKE (Internet Key Exchange) Support
    - Key Management Standard
    - Allows for Separate Encryption Key Protocols
    - ISAKMP (Internet Security Association and Key Management Protocol)

- Controls
  - Layered Defense Mechanisms (In My Understanding)
    - Security Controls Categorized by their Nature
      - Technical
        - Implemented by IT Staff using Systems
      - Administrative/Managerial
        - Implemented by Management through Policies, Processes, and Procedures
          - Background Check
          - Security Awareness Training
          - Business Continuity Plan
            - Contingency Planning
            - Change Management
              - Improvement Initiatives
                - Efficiency
                - Effectiveness
      - Operational
        - Physical Controls (Outer Layer of Defense)
          - Facility Design
            - Layout
            - Doors
              - Access Badge
              - Mantrap
            - Fencing
            - Alarm
            - Guard
            - Gate
            - CCTV
            - Surveillance Systems
          - Data Access
            - Backup
            - Output
            - Mobile File Storage Device
        - Company Culture
          - Training
          - Physical Protection
          - Environmental Protection
          - Monitoring
          - Operating Procedures
    - Security Controls Categorized by their Function
      - Main
        - Deterrent
          - Implemented for Discouragement
        - Preventive
          - For Preventing an Occurrence
        - Detective
          - Identification After Occurrence
        - Corrective
          - Reactive Measures to Reduce Effect of or Restore to a Known Good State
      - Compensating
        - Risk Reduction Measures for Controlling a Weakness or Flaw Due to a Constraint
          - Existing
          - Potential

- Security Controls Categorized by their Function
  - * For the Creation of this Mind Map, I Referenced the following eBooks.
    - Darril Gibson's CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide
    - Dawn Dunkerley's Mike Meyers CompTIA Security+ Certification Passport, 6th Edition
    - Ian Neil's CompTIA Security+: SY0-601 Certification Guide
    - Marty Weiss's CompTIA Security+ SY0-601 Exam Cram
    - Professor Messer's CompTIA Security+ SY0-501 Course Notes
    - Professor Messer's CompTIA Security+ SY0-601 Course Notes
  - Deterrent (Implemented for Discouragement)
    - Network and System Security
      - Encryption
      - Antimalware
      - IDS
      - IPS
      - Firewall
      - Content Filter
      - Logical Access Controls
      - Data Classification
      - Least Privilege
    - Detection of Violation
      - Consequence
      - Punishment
    - Warning Signs
      - No Tresspassing
      - On Camera
    - Secure Coding Practices
      - Application Security
    - Motion Sensor
    - Lighting
    - Security Guard
    - Camera
    - Cable Lock
    - Screen Saver
    - Screen Filter
  - Preventive (For Preventing an Occurrence)
    - Administrative
      - Physical
        - Security Guard
        - Lock
      - Policies, Processes, Procedures
        - Access Control
          - Least Privilege
          - Separation of Duties
        - Change-Management
          - Change Advisory Board
        - Personnel
          - On-Boarding
            - Personnel Background Checks
          - Off-Boarding
            - Disabling User Accounts
          - Continuing Education
            - Security Awareness Training
        - Risk Controls
          - Identify Risks
          - Identify Mitigating Measures
        - Technical
          - IPS
          - Firewalls
          - Anti-Malware
          - Penetration Testing
          - Vulnerability Scanning
          - Operating System Hardening
  - Detective (Identification After Occurrence)
    - Technical
      - Audit Trails
        - Log Files
      - Intrusion Detection Systems
      - System Monitoring
      - Checksums
      - Anti-Malware
    - Physical
      - Physical Access
        - CCTV Surveilance
        - Motion Detector
        - Alarm
      - Environmental Controls
        - Fire Suppression
        - Temperature
    - Administrative
      - Security Audits
      - Mandatory Vacations
      - Rotation of Duties
      - Trend Analysis
  - Corrective (Reactive Measures to Reduce Effect of or Restore to a Known Good State)
    - Operating System Updates
    - Restoring from Backup
    - Mitigating a Vulnerability
    - Anti-Malware
    - Fire Suppression System
  - Compensating (Risk Reduction Measures for Controlling a Weakness or Flaw Due to a Constraint)
    - Risk-Based Standards
      - Backup Power
      - Alternate Site
    - When Separation of Duties is not Possible
      - Audit Trails
      - Transaction Logs
    - When Multi-factor Authentication is Not Yet Feasible
      - Username & Password


SDN
(Software-Defined Networking)
Network Management
Distributed Control Plane
(Traditional Method/ NON-SDN)
Management Plane
Connection to Devices
SSH
RS232
Control Plane
Routing and Switching
Device Interaction
Decision Making
Algorithm
Data Plane
Performs Control Plane Instructions
Movement of Data Packets
Controller
Centralized Configuration, Policy Creation, and Management of Network Devices
Applies to Physical & Virtual Networks and Their Cross Traffic
Hyper-V Virtual Switch
Hyper-V Manager
Server Role
Protection
ARP Spoofing
Neighbor Discovery Spoofing
DHCP Guard Protection
Port Access Control Lists
MAC Address
IP Address
Features
Trunk Mode to VM
Traffic Monitoring
Isolated VLAN
To and From SDN Controller
Monitor
Configure
Troubleshoot
Deployment
Design
Interfaces
Northbound API
(NBI)
Windows PowerShell API
Management GUI
Virtual Machine Manager
Systems Center Operations Manager
API
(Allows Communication
Between 2 Software)
Communication
Network Component
Network Service
Network Device
Southbound API
(SBI)
Discover Network Devices
Detect Service Configurations
Send Configuration Changes to Network
Virtualization
Network
Network Function
Software Load Balancer
NAT
Datacenter Firewall
RAS Gateway Multitenant BGP Router
Dynamic Routing Between Networks
Appliance
Referenced:
Ed Liberman Video Overview of Software-Defined Networking
Mike Chapple Video Software-Defined Networking (SDN)
Kevin Wallace Video Software-Defined Networking (SDN)

VPN (Virtual Private Network) Technologies

Access to Remote Protected Network Resources Through a Secure Tunnel Connection

- Communication
  - Authenticated
  - Encrypted
  - Encapsulated
  - Routed

Connectivity

- Client-to-Site
  - Client Connects from Outside of the Office to the Office Network
  - Use Case — Individual Connecting to Corporate Network — Gets an additional Corporate Network Internal IP address during Connection
- Site-to-Site
  - Use Case
    - Connecting two Subnets over the Internet — No Individual User Connections
    - Satellite Office Connection to the Main Office — Several Users at Each Location

Types

- Corporate — Connects One to a Network
- Commercial
  - Proxy Server
    - Allows for Identity to Stay Hidden — Web Browsing
    - Changes Location of Traffic
  - Fee for Service
  - Example — NordVPN
  - Use Case
    - Hide Identity
    - Testing of Site or Service for Global Customers

Connection Types

- Full VPN Tunnel
  - All Traffic Through Tunnel
- Split VPN Tunnel
  - Corporate Traffic Through Tunnel
  - Other Traffic Split From Tunnel

Provider

- Server
- Concentrator
  - Point of Access
    - Encrypts
    - Decrypts
  - Types
    - Hardware
    - Software
  - Multiple OS Support — Client Software
- Firewall
  - Provides IP Address
    - DHCP Server
    - IP Address Pool
  - Firewall VPNs
    - IPsec
      - Secures Connection
      - Modes
        - Transparent — Payload Encryption
        - Tunneling — Entire Packet Encryption
    - L2TP (Layer 2 Tunneling Protocol) — Secure — Combined with IPsec
    - PPTP (Point-to-Point Tunneling Protocol)
      - Tunnel with Encapsulated Data Packet
      - PPTP Encrypts
      - Not as Secure — Obsolete
    - SSL and TLS
      - Web Browser — Client
      - Is Not Blocked
    - Open VPN
      - Open-Source VPN
      - Custom
      - Based on SSL and TLS
    - SSH (Secure Shell)
      - Connects Two Devices Through a VPN Tunnel
      - PuTTY — Example

Client

- PPTP (Point-to-Point Tunneling Protocol)
  - Default
  - Routing and Remote Access Role
  - Less Secure — Obsolete
  - Not Supported by Apple
- IKEv2 (Internet Key Exchange 2)
  - IPsec-Based
  - No Re-authentication Required when Disconnected — Re-establishes Connection
  - Use Case
    - Slow Connections
    - Unreliable Connections
- L2TP (Layer2 Tunneling Protocol)
  - Lightweight
  - Preferred by Apple
  - Security
    - Certificate
    - Password
- SSTP (Secure Socket Tunneling Protocol)
  - Most Secure — Public Certificate
  - SSL/TLS over Port 443 — End-to-End VPN Tunnel
  - Support for a Variety of OS
    - Browser — No VPN Client — No Firewall Settings
    - Light Client
  - Not Supported by Apple
  - Does Not Support Site-to-Site
- DirectAccess
  - Microsoft — Through Group Policy
  - Do Not Use
- Windows 10 Always On VPN
  - Supports
    - Domain-Joined
    - Non-Domain-Joined
    - Cloud Integration
      - Azure
      - InTune
  - Connection Control is Based on Workstation
- HTML5 VPN
  - SSL/TLS — Through Web Browser
    - Web Cryptography
    - API
  - Reverse Proxy
  - No Installation of App

Referenced:
Professor Messer Security+ 601 Course Notes
Robert McMillen Video Intro to VPN Technologies
Scott Simpson Video Learning VPN
Scott Simpson Video Understanding VPN

Tokenization

Data Security

- Replacement of Pieces of Data for Security Purposes
  - Token
    - Is a Meaningless Placeholder Mapped to Data
    - Points Back to Data
  - Can Be Reversed through Tokenization System — Not Mathematically Reversible Without Original Key
- Primary Function — To Address Online Breach Dilemma — Online Fraud Prevention — Security
- Use Case — Payment Tokenization
  - Card Processing — Tokenization
    - Replace Primary Account Number with Token
    - Substitute a number for transaction purposes
  - Refund
  - Recurring Payment
- Examples
  - Apple Pay
  - Android Pay
  - Apps — eCommerce

Text

- Text Cleansing And Extraction
  - Component Elements
    - Words
    - Symbols
  - Standardize Format — Dates
  - Perform Language Conversion
  - Remove Extraneous Elements — Punctuation
  - Convert Abbreviations — Full Words
  - Convert Text Case — Lowercase
  - Remove URLs, Hashtags, Mentions
  - Remove Stop-Words
    - Meaningless Words — Articles in Grammar
    - Take Up Storage
    - Take Up Processing
  - Perform Stemming
    - Keep Base Word
    - Remove Word Derivatives
  - Perform Lemmatization
    - Get at Root Words
    - Meaningful
- Use Case — Machine Learning

Referened:
Professor Messer Security+ 601 Course Notes
Kumaran Ponnambalam Video Tokenization
Wikipedia Tokenization (Data Security)
Square Article: Payment Tokenization Explained

Wireless Encryption

WPA3 (WiFi Protected Access v3)

- 2020
- Packet Encryption: AES (Advanced Encryption Standard)
- Mode of Operation: GCMP (Galois Counter Mode Protocol)
- Key Exchange Process: SAE (Simultaneous Authentication of Equals), Dragonfly Key Exchange
- MIC (Message Integrity Check)
- Enterprise: 802.1X, RADIUS

WPA2 (Wi-Fi Protected Access v2)

- 2004
- Packet Encryption: AES (Advanced Encryption Standard)
- Mode of Operation: CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
- PSK (Pre-Shared Key)
- MIC (Message Integrity Check)
- Enterprise: 802.1X, RADIUS

WPS (Wi-Fi Protected Setup)

- 2007
- Automatic WPA2 Encryption Configuration
- Sets Up Personal Shared Key Automatically: 8-Digit Code
- Vulnerable

WEP (Wired Equivalent Privacy)

- 1997
- Packet Encryption: RC4
- Packet Integrity Check: CRC-32
- Initialization Vector: 24 Bit IV
- Shared Secret Key
- Fixed Key
- MIC (Message Integrity Check)
- Not Secure

WPA (Wi-Fi Protected Access)

- 2003
- Packet Encryption: RC4
- TKIP (Temporal Key Integrity Protocol)
- Per Packet Encryption Key Rotation
- Per Packet Key
- IV (Initialization Vector)
- PSK (Pre-Shared Key)
- MIC (Message Integrity Check)
- Enterprise: 802.1X, RADIUS
- Vulnerable

Referenced:
Professor Messer's Security+ 601 Notes
Mike Chapple Video Wireless Encryption
Mike Meyers Video Wireless Encryption
Mike Chapple Video WEP, WPA, WPA2
Cybarrior Blog Wireless Security protocols: WEP, WPA, WPA2 and WPA3
Wikipedia Wi-Fi Protected Access

Cryptographic Algorithms

Symmetric Block Encryption

	Key Size (Bit)	Methodology	Advantage	Disadvantage	Use Case
DES	56	64-Bit Block			Do Not Use
					Financial Transactions
3DES	56, 112, 168	DES Algorithm		Slow	Alternative to AES
		64-Bit Block		Multiple Pass Encryption/Decryption	
		3 Phases			
		Multiple Keys		Resource Intensive	
AES	128, 192, 256	128-Bit Block	Fast		Small Devices
			Efficient		USB Drive Encryption
		One Pass Encryption/Decryption	Less Resource Intensive		CCMP WPA2
			Strong		TLS
Blowfish	Between 32 and 448	64-Bit Block	Faster than AES-256		Replacement for DES
Twofish	Between 40 and 2048	128-Bit Block			
IDEA	128	64-Bit Block			Replacement for DES
					Financial
					Government
					Broadcasting
					Audio/Visual

Cryptographic Algorithms

Block Cipher Modes

	Methodology	Advantage	Disadvantage	Use Case
ECB	Divide into Blocks		Weakness	Deprecated
	Encrypt Blocks		Same Key Per Block	
CBC	Combines Block with Previous Block		Inefficient	Symmetric Block Cipher
	IV for Randomness		Pipeline Delays	
	XOR Operation			
CTM	Block into Stream Cipher	Multiprocessing		Secure Mode of Operation
	IV & Counter			
	Different Key Per Block			
GCM	Counter Mode Operation	Efficient		Encryption / Decryption
				Authenticity
	Galois Mode Authentication	Performance		Integrity
				Confidentiality

Cryptographic Algorithms

Asymmetric Encryption

	Bit	Methodology	Advantage	Disadvantage	Use Case
RSA Rivest Shamir Adleman	2048	Prime Number Properties	Strong Security with Sufficient Key Size		Data Transmitted over Internet
		Based on Diffie-Hellman Static Key			Email
ECC Elliptic Curve Cryptography	Generates Key	Elliptical Curve	Less Resource Intensive		Low-Power Devices
					Small Wireless Devices
					Not Used by Gov Agencies
DHE Diffie-Hellman Ephemeral	Between 768 and 3072 Based on Group #s 1-15	Ephemeral Key		Negotiates for Strongest Supported Group	Sharing of Symmetric Key
	Higher Group # is More Secure				
ECDHE Elliptic Curve Diffie-Hellman Ephemeral	Generates Key Using ECC	Ephemeral Key		Negotiates for Strongest Supported Group	Sharing of Symmetric Key

Cryptographic Algorithms

File Integrity Check

	Output Size Bit	Algorithm	Functionality	Use Case
CRC32		Checksum	Detect Data Corruption	
MD5	128	Message Digest	Verify Data Integrity	Email
				File on Disk
			Detect Data Corruption	File Download
				Executable File
SHA Family	0 (160)	Digital Signature	Encryption	Detection of File Modification by Malware
	1 (160)		Data Integrity	HIDS
	2 (224, 256, 384, 512)			
	3 (224, 256, 384, 512)		Authenticity	Antivirus
HMAC	HMAC-MD5 (128)	Shared Secret Key for Randomness	Data Integrity	IPsec
	HMAC-SHA1 (160)		Authenticity	TLS
RIPEMD		Message Digest	Verify Data Integrity	

Cryptographic Algorithms

Password Hashing Algorithms

	Bit	Salt	Functionality	Use Case
Argon2		Salt	Key Derivation Function	Backend Server
		Secret Key		Cryptocurrency
Bcrypt		Salt	Blowfish Encryption	Unix/Linux Shadow Password File
PBKDF2	128, 256, 512	Salt	HMAC Function	WPA2
				Apple iOS
				Cisco OS
Scrypt		Salt	Key Derivation Function	Wallets
				Files
				App Passwords

Wireless Standards

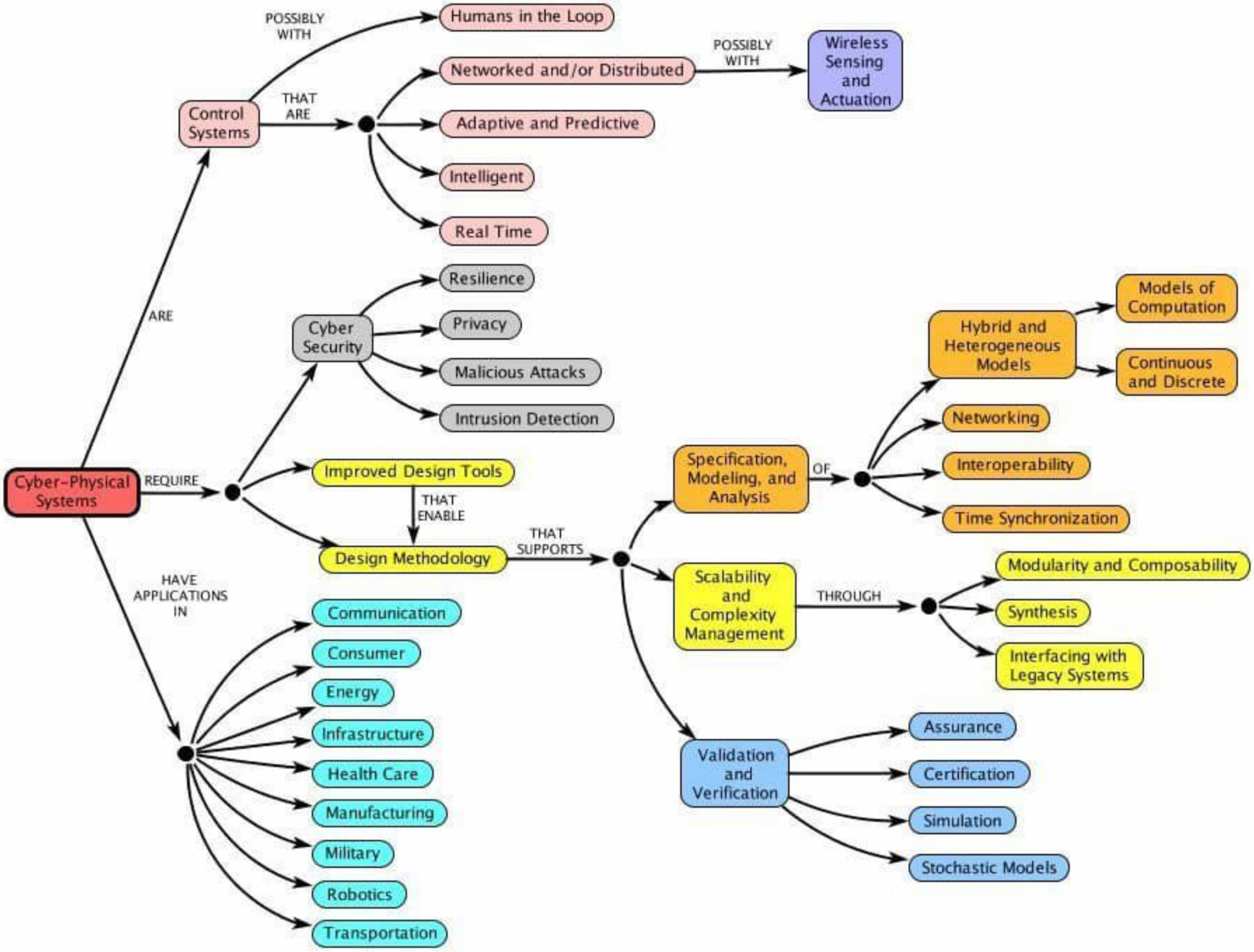
IEEE 802.11 Standard

	Frequency (GHz)	Streams (Up To)	Speed (Up To)	Channel Numbers (North America)	Channel Width (MHZ)	RF Modulation
802.11a	5	1	54 Mbps		20	CDMA, DSSS
802.11b	2.4	1	11 Mbps	1 through 11	20	CCK, DSSS
802.11g	2.4	1	54 Mbps	1 through 11	20	CCK, DSSS, OFDM
802.11n	2.4, 5	4 MIMO	150 x 4 = 600 Mbps	2.4: 1 through 11 5: 36, 40, 44, 48, 149, 153, 157, 161, 165	20, 40	CCK, DSSS, OFDM
802.11ac	5	8 MU-MIMO	866.7 x 8 = 6.933 Gbps	5: 36, 40, 44, 48, 149, 153, 157, 161, 165	20, 40, 80, 160	BPSK QPSK QAM

Cyber-Physical Systems - a Concept Map

See authors and contributors.

http://CyberPhysicalSystems.org



CISO MindMap 2020
What Security Professionals Really Do?