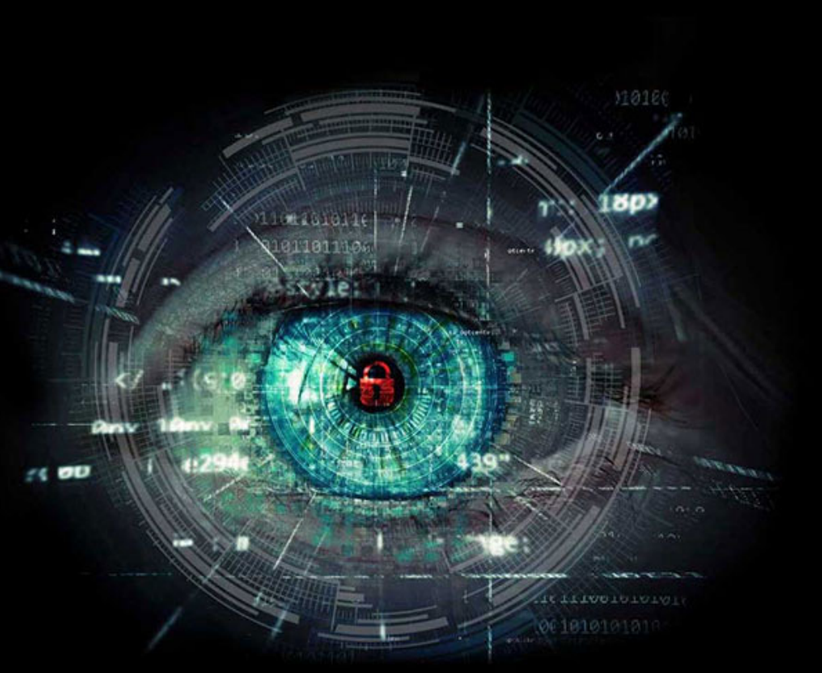

Cyber Security
0001
RMUTT

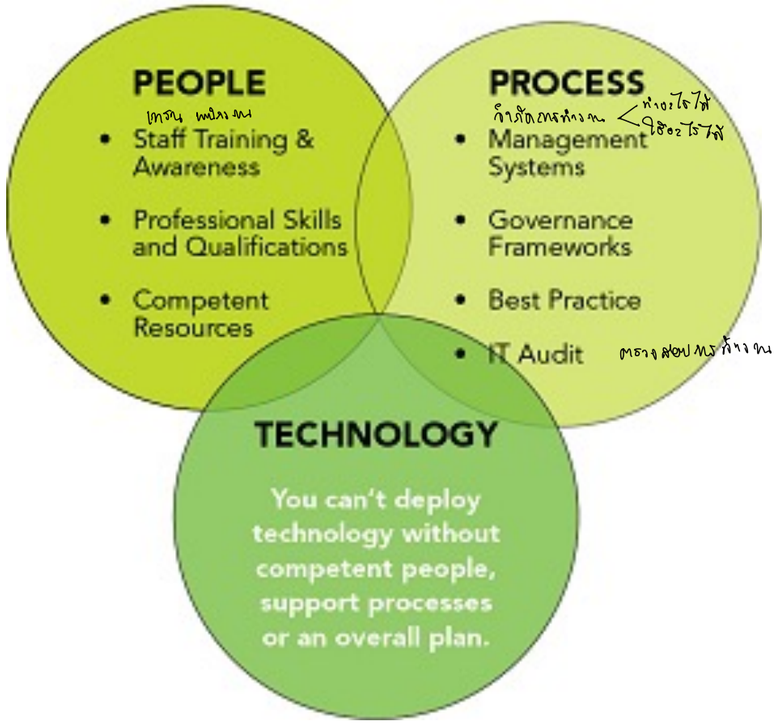
Agenda



1. Understanding core security goals
2. Introducing basic risk concepts
3. Exploring authentication concepts
4. Comparing authentication services
5. Authenticating RAS (Remote Access Service) Clients

CH1 Mastering Security Basics

Three pillars of cyber security



https://blog.itgovernance.co.uk/blog/three-pillars-of-cyber-security

จับต้องได้

Assets

จับต้องไม่ได้

Tangible Assets

Current Assets

cash
cash equivalents
accounts receivable
stock inventory
short-term investments

Fixed Assets

buildings
machinery
computer equipment
tools
furniture

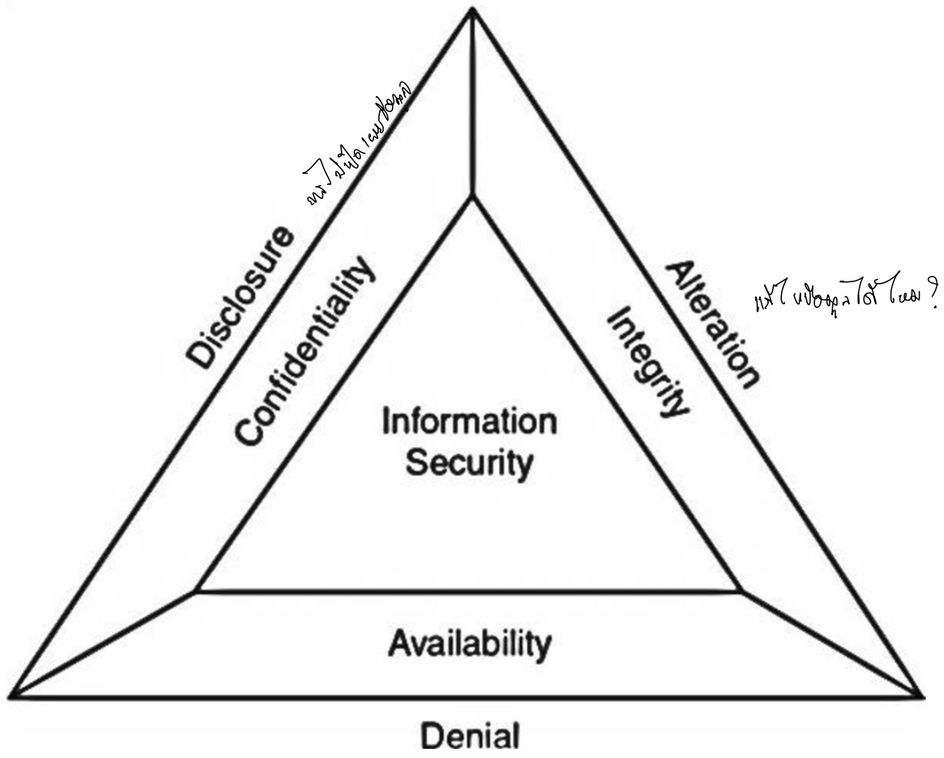
Intangible Assets

goodwill
patents
copyrights
trademark
brand recognition
business methodologies

Confidentiality , Integrity , Availability (CIA)

- **Confidentiality**, it offers a high level of assurance that data, objects, or resources are restricted from unauthorized subjects. If a threat exists against confidentiality, unauthorized disclosure could take place.
- **Integrity**, it offers a high level of assurance that the data, objects, and resources are unaltered from their original protected state.
- **Availability**, it offers a high level of assurance that the data, objects, and resources are accessible to authorized subjects.

Confidentiality , Integrity , Availability (CIA)



Asset in relation to the CIA Triad

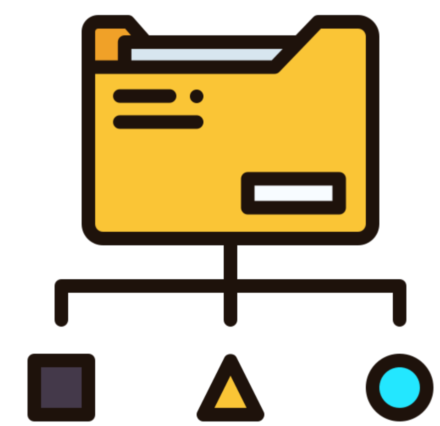
	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

การจัดการชั้นความลับ

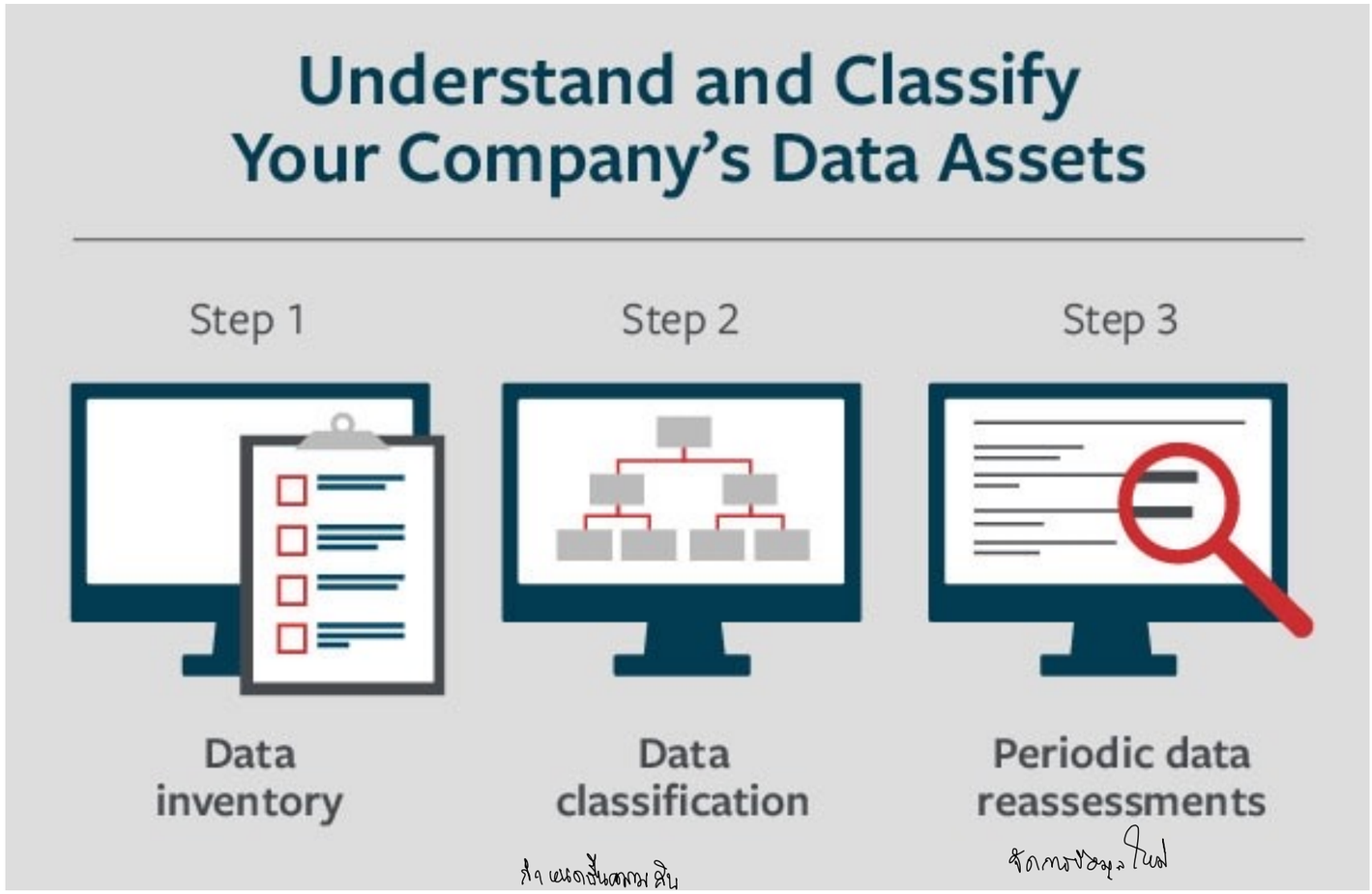
Data Classification

Data classification is an essential component of any data security and compliance program, particularly if your company keeps large amounts of data. It lays the groundwork for your data security strategy by helping you in determining where you keep ความสำคัญชั้นความลับ sensitive and regulated data, both on-premises and in the cloud. Furthermore, data classification enhances user productivity and decision-making while reducing storage and maintenance costs by removing unnecessary data. การจัดการในการเก็บข้อมูล

อะไรที่ไม่สำคัญต่อ Bussiness ก็ไม่ต้องเก็บ



Data Classification



Data Classification

Step 1: Data Inventory

Determine the type of data you store.

- **Personally Identifiable Information:** Often referred to as PII, this information may include such things as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, medical records and Social Security numbers. It also may include gender, age, date of birth, city of birth or residence, driver's license number, and phone numbers.
- **Customer information:** This may include payment information such as payment card numbers and verification codes, billing and shipping addresses, email addresses, phone numbers, and purchasing history, among other data.
- **Intellectual property:** This may include proprietary and sensitive business information such as financial records, product designs, human resource records and internal correspondence and reports. It also can include intellectual property of others with whom you have a business relationship, including customers and vendors.

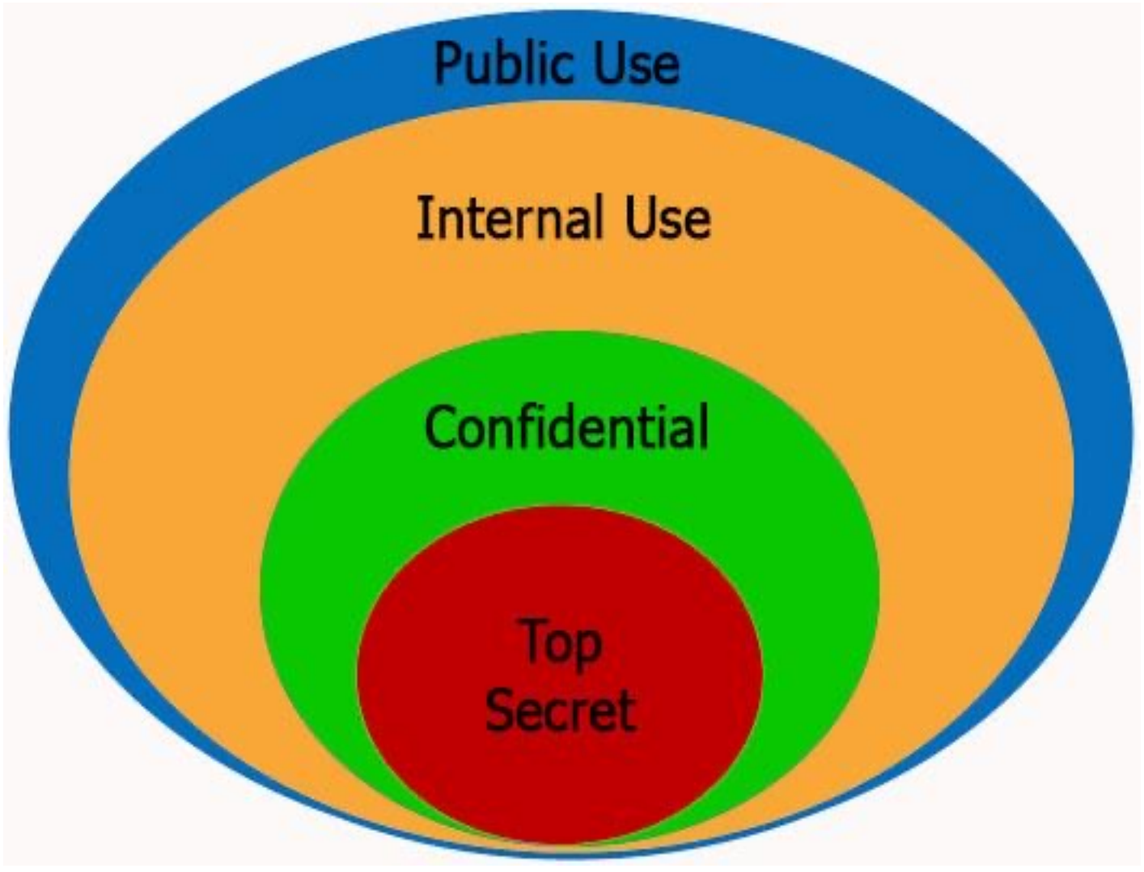
Data Classification

Step 2: Data Classification

Classify and labeling the data and establish access privileges based on type and level of confidentiality.

- **Restricted (highly sensitive):** This classification applies to the most sensitive business information intended strictly for use within your company. Its unauthorized disclosure could harm your company, business partners, vendors and/or customers in the short and long term.
- **Confidential (sensitive):** This classification applies to information about or belonging to customers, employees and information that your company is obligated to protect. This can also apply to information about your own company.
- **Internal use only:** This classification applies to sensitive information that is generally accessible by a wide internal audience and is intended for use only within your company. While its unauthorized disclosure to outsiders should be against policy and may be harmful to your company, the unlawful disclosure of the information is generally not expected to impact your company, employees, business partners, vendors and the like.
  Public (general): Information that is generally available or is intended for distribution outside your company.

Data Classification

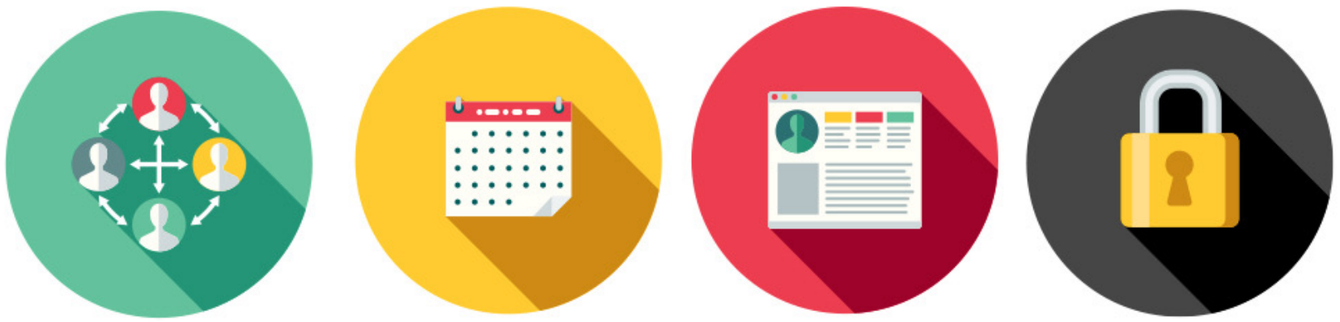


Data Classification

SECURITY LEVEL 01	**Public** Any business data that is easily accessible by the public and cannot cause any significant damageto your brand, financial loss, or put your partners, clients, and employees in peril.	Social media feeds, press releases, information on your website.
SECURITY LEVEL 02	**Private (Internal)** Information that can be used and shared within the company. Disclosure of the following information may cause loss of competitive advantage and mbarrassment.	Project documents, policy guides, internal emails.
SECURITY LEVEL 03	**Confidential** Outbreak of the following business data may lead to financial loss and harm a company, its employees, customers, and partners.	Customer information, contracts, state identification numbers, employee contracts.
SECURITY LEVEL 04	**Restricted** Highly sensitive business data that if disclosed may lead to permanent damage.	Business plans, disclosed annual reports, intellectual property, and trade secrets.

https://softengi.com/blog/three-steps-to-classify-your-financial-data/

Data Classification



PUBLIC

Data that can be freely shared with anyone

Examples:

- Directories
- Press releases
- Mission statements

INTERNAL

Data shared within the organization

Examples:

- Work schedules
- Budgets
- Project plans
- Strategies
- Business processes

CONFIDENTIAL

Data shared with select internal individuals as needed for their jobs

Examples:

- Some regulated data (personal identifiable information, protected health information, HIPAA)
- Personnel records
- Financials

RESTRICTED

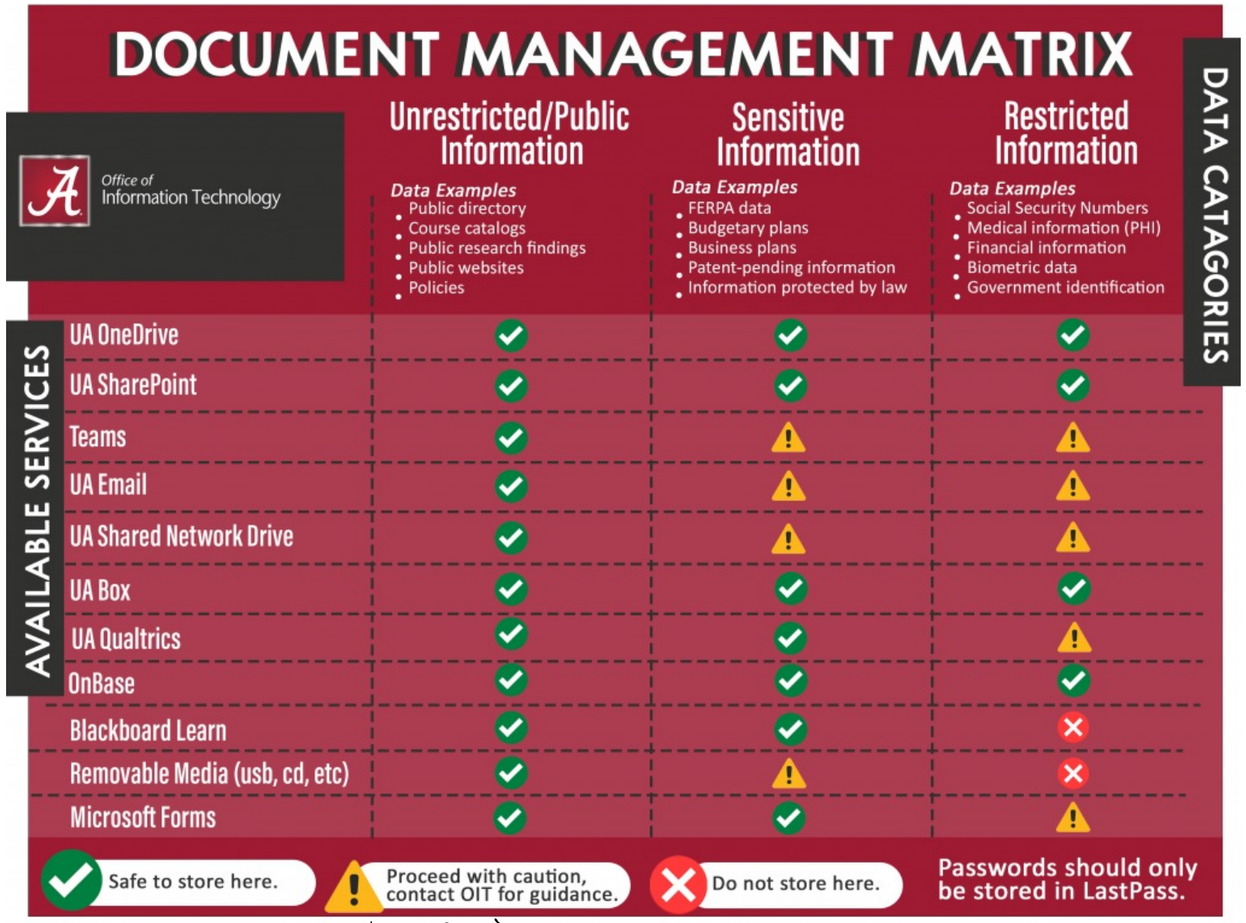
Data that is highly sensitive

Examples:

- Passwords
- Some highly regulated data
- Merger/acquisition plans
- Critical intellectual property

https://www.sfmagazine.com/articles/2021/december/the-critical-first-step-to-data-security/?psso=true

Data Classification



Data Classification

EMAIL & Attachments	Confidential/ Proprietary	Private	Sensitive	Public
Encrypted with AES 256	☑	☑	☑	
Remain Encrypted Except when Viewed	☑	☑		
Sent Only to Recipients within the Organization	☑	☑		
Cannot be Saved	☑			
Cannot be Copied and Pasted	☑			
Cannot be Printed	☑			
Cannot be Sent in Cleartext	☑	☑	☑	

Data Classification

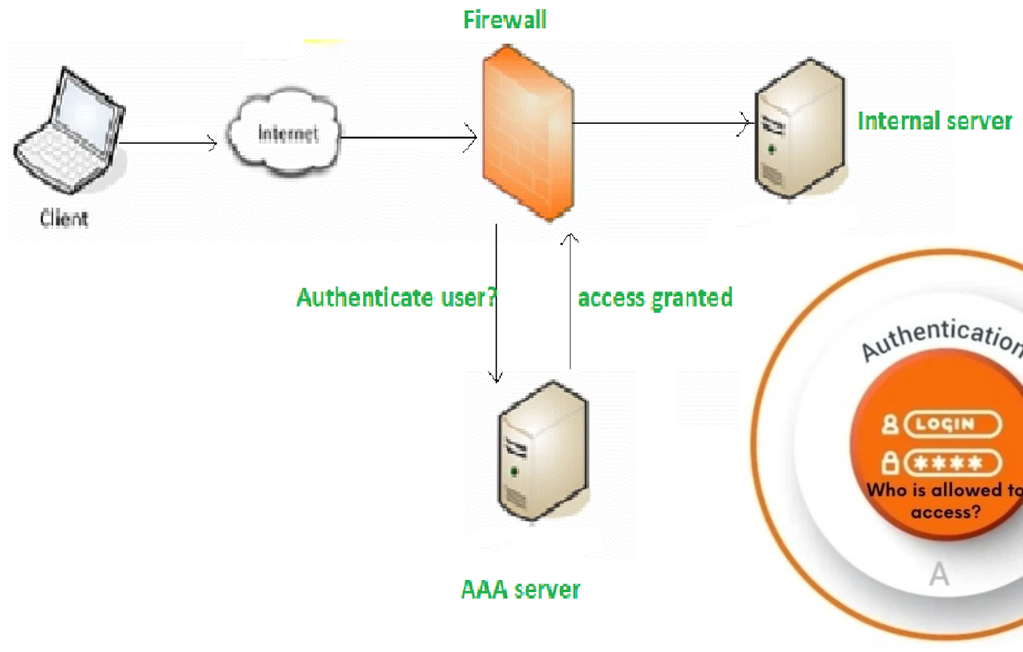
Step 3: Periodic Data Reassessments

Periodically reassess the classification of the data and who has permission to access it. An information retention policy should include guidance on what types of information should be retained, how long it should be retained and procedures for disposing or destruction of unneeded data. Audit all data and information that you store to be sure it is classified properly, and to determine if unneeded data may be destroyed.

Process Framework

AAA - Authentication, Authorization, Accounting

Authentication, Authorization, and Accounting (AAA) is a three-process framework used to manage user access, enforce user policies and privileges, and measure the consumption of network resources.



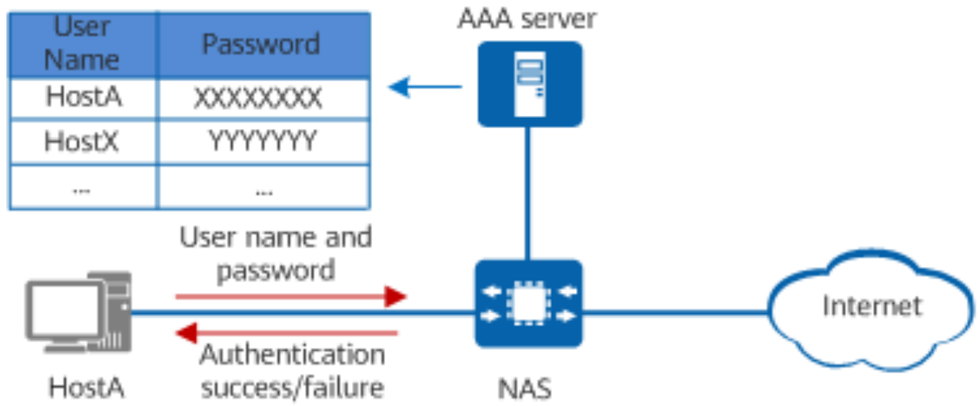
AAA - Authentication, Authorization, Accounting

Authentication (Who are you?)

Authentication: confirms the identities of users accessing the network and determines whether the users are authorized.

The AAA server compares a user's authentication credentials with those stored in a database. If the credentials match, the user passes identity authentication and is permitted access to the network. If the credentials do not match, the user fails identity authentication and is denied access to the network. The following lists the typical authentication credentials:

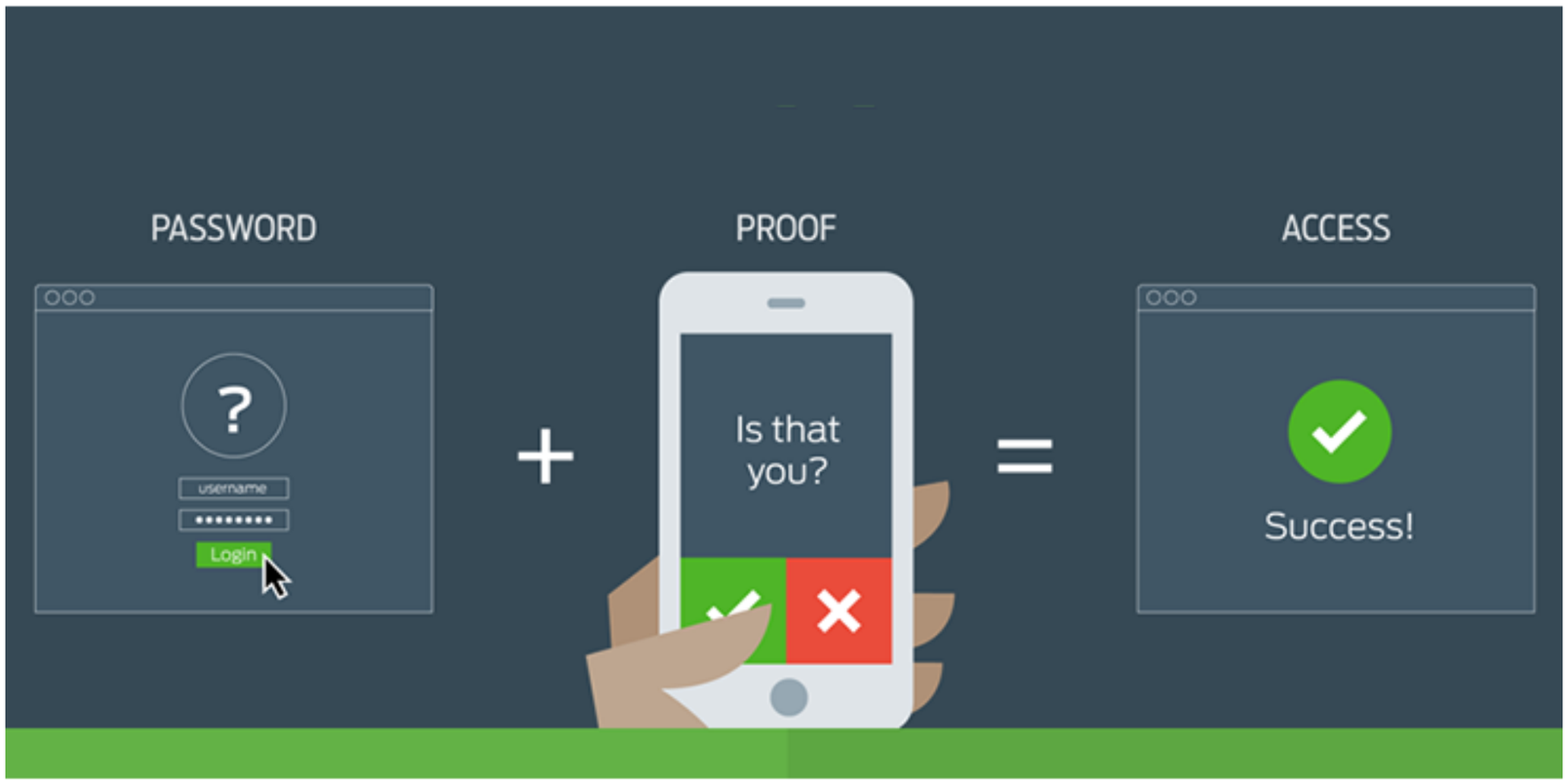
- Password
- Username and password
- Digital certificate
- Fingerprint
- Hardware and Software token



AAA - Authentication, Authorization, Accounting

AAA - Authentication, Authorization, Accounting

AAA - Authentication, Authorization, Accounting



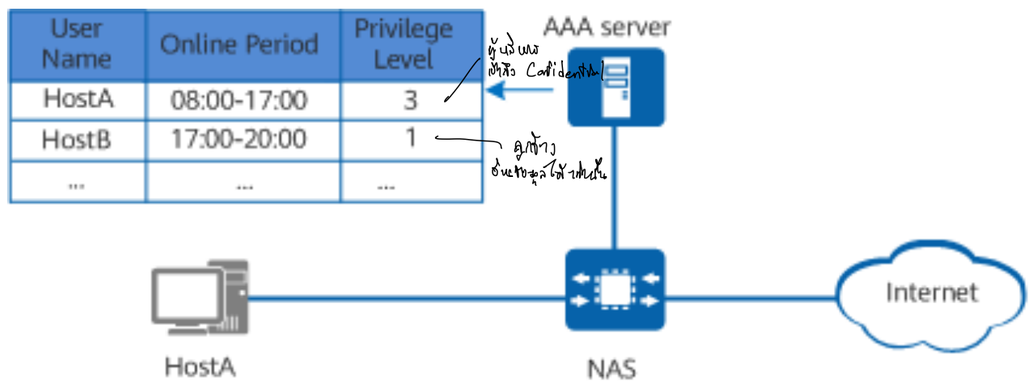
AAA - Authentication, **Authorization**, Accounting

Authorization (What you can do?)

Authorization: assigns differentiated rights to authorize users to use specific services.

After a user passes identity authentication, the following items are authorized to the user:

- Commands
- Resources
- Information
- Authorization follows the least privilege principle. That is, users are granted only the permissions required for executing required functions to prevent any accidental or malicious network behavior.

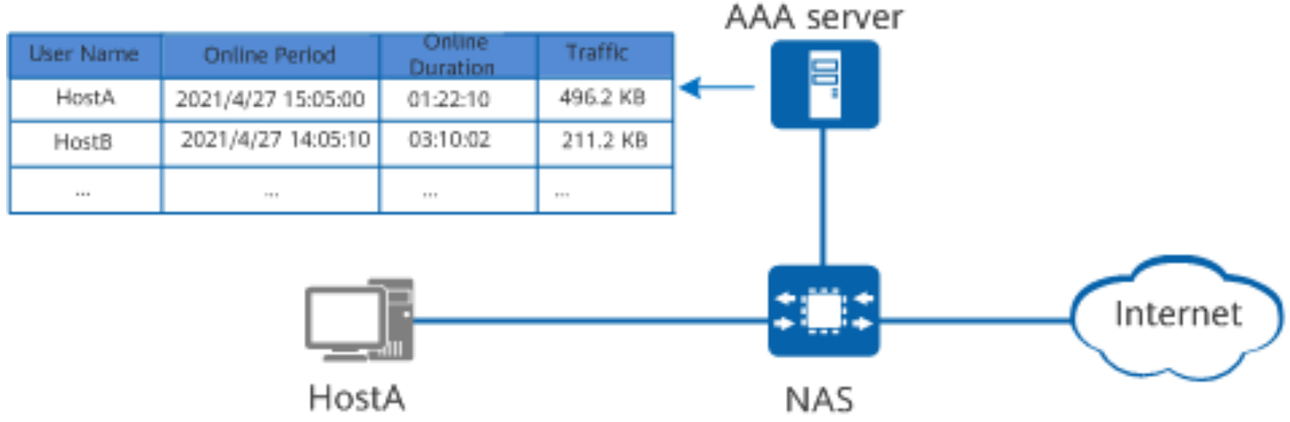


AAA - Authentication, Authorization, Accounting

Accounting

Accounting: records all the operations of a user during the network service process, including who, when, and what has been performed.

Accounting records the used service type, start time, and data traffic to collect and record the network resource usage of the user for implementing time- or traffic-based accounting and network monitoring.



Risk

IT risk is basically any threat to your business data, critical systems and business processes. It is the risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an organization. IT risks have the potential to damage business value and often come from poor management of processes and events.

Categories of IT risks

IT risk spans a range of business-critical areas, such as:

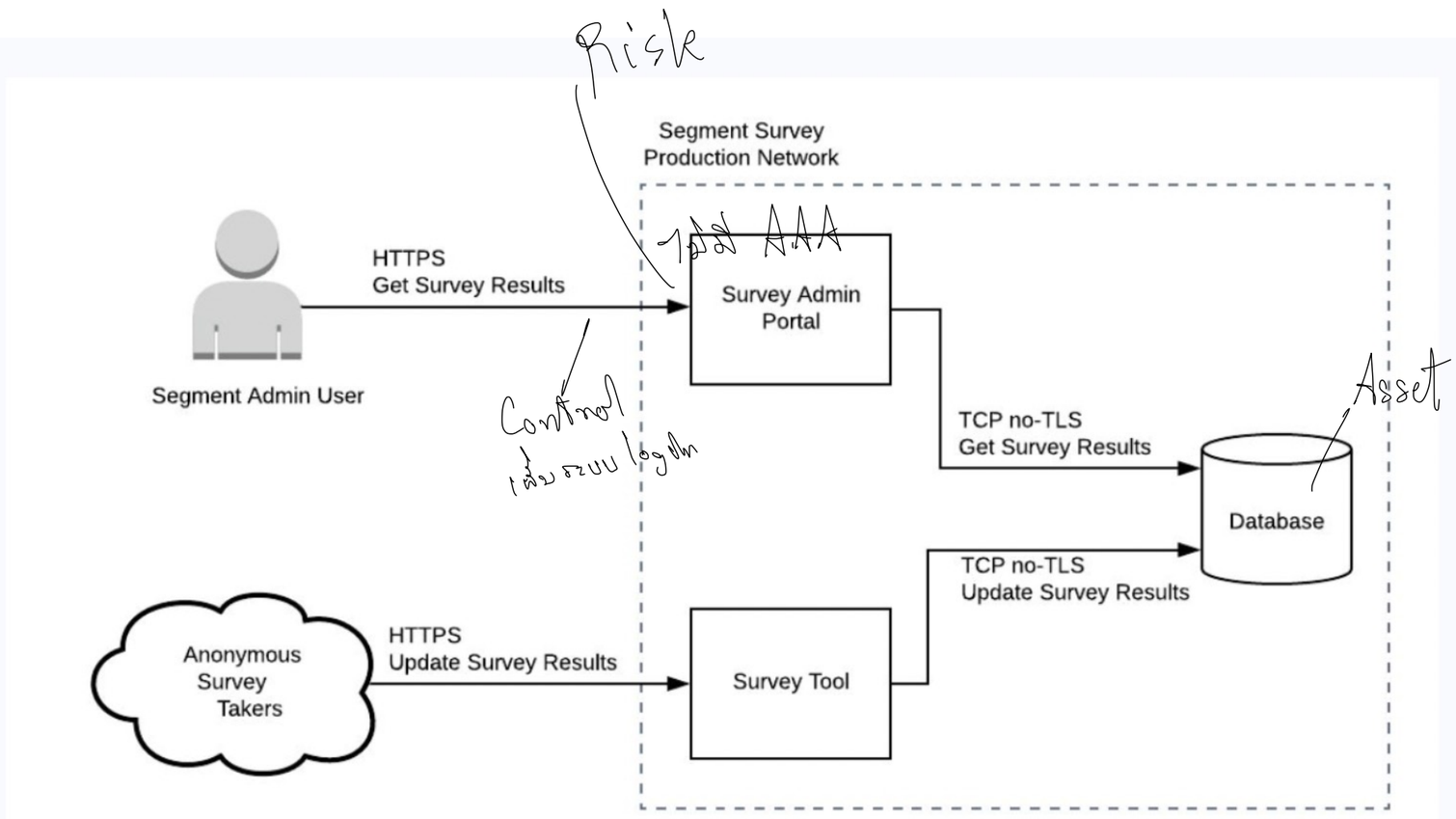
- Security - compromised business data due to unauthorized access or use
- Availability - inability to access your IT systems needed for business operations
- Performance - reduced productivity due to slow or delayed access to IT systems
- Compliance - failure to follow laws and regulations (data protection)

Risk example 1

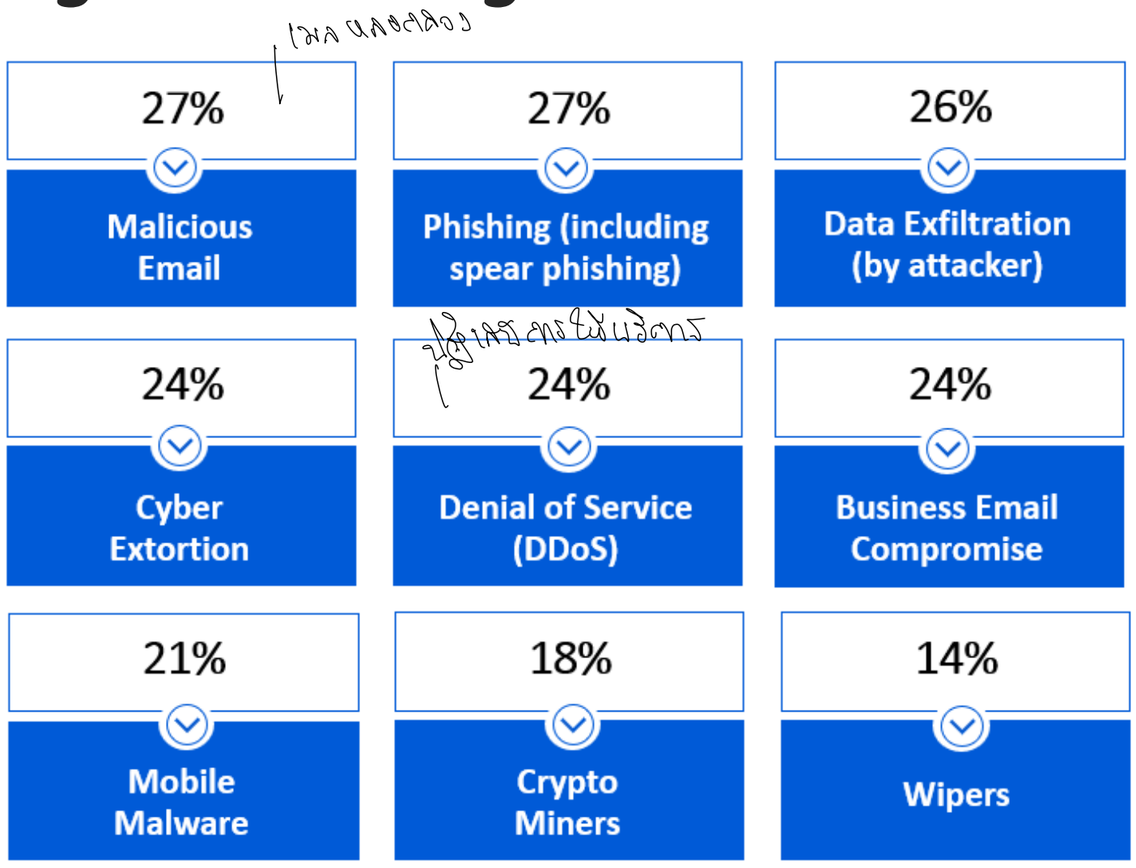
"**Risk** is probability of a **threat** causing harm, by exploiting a **vulnerability** in the absence of a **control** which **impacts** negatively on **assets** like individuals or an organization"

A person going to a shop during cloudy weather has the risk of getting wet. The clouds are the **threat** and the person himself is the **asset**. If he has a **control** like an umbrella then the risk of getting wet is mitigated. If he does not have an umbrella then he is **vulnerable** to get wet.

Risk example 2



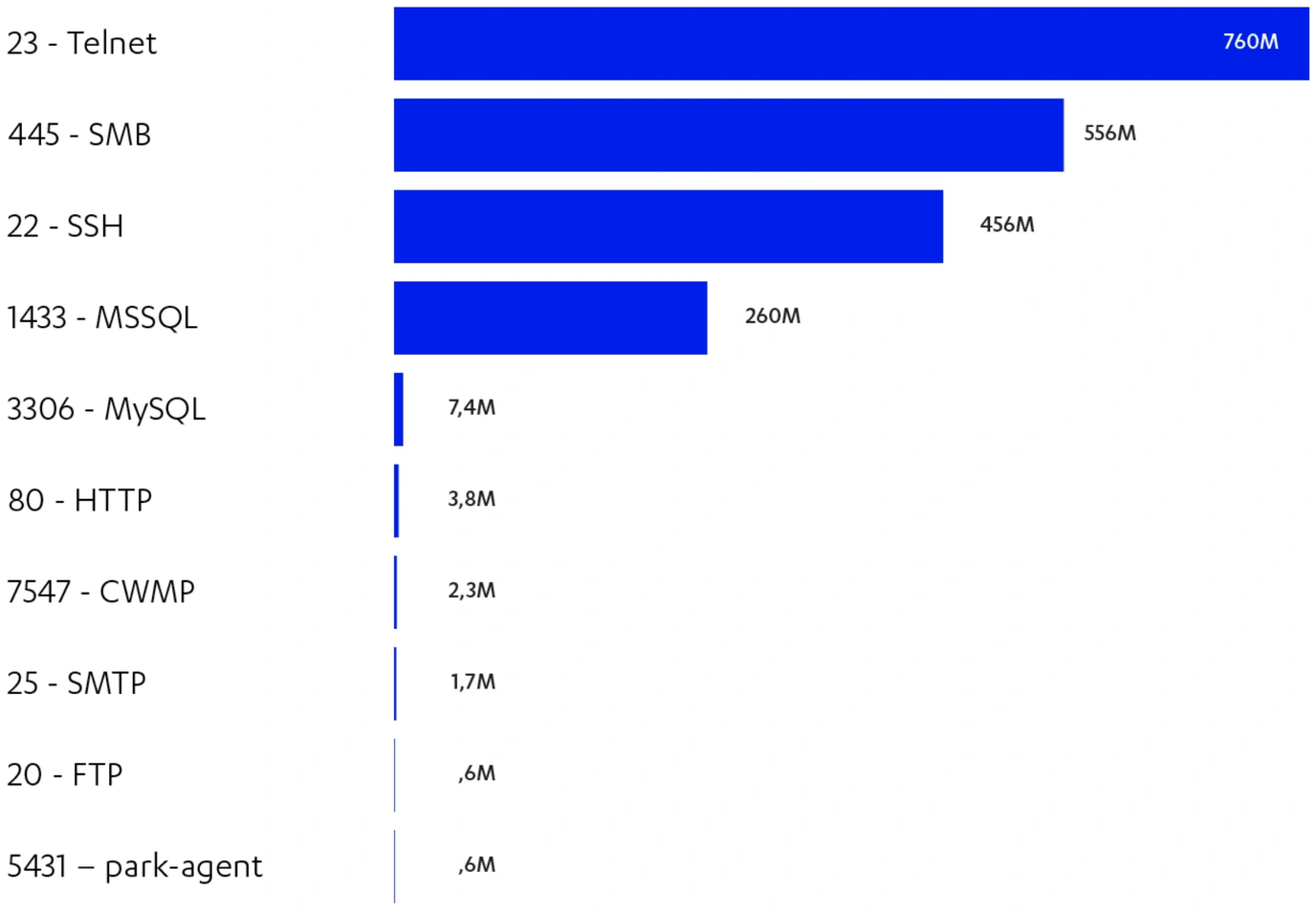
Top Cybersecurity thread trends 2023



Selection of non-ransomware cyberattacks experienced in the last year and the percentage of organizations that reported them

SOPHOS

TOP TCP PORTS TARGETED



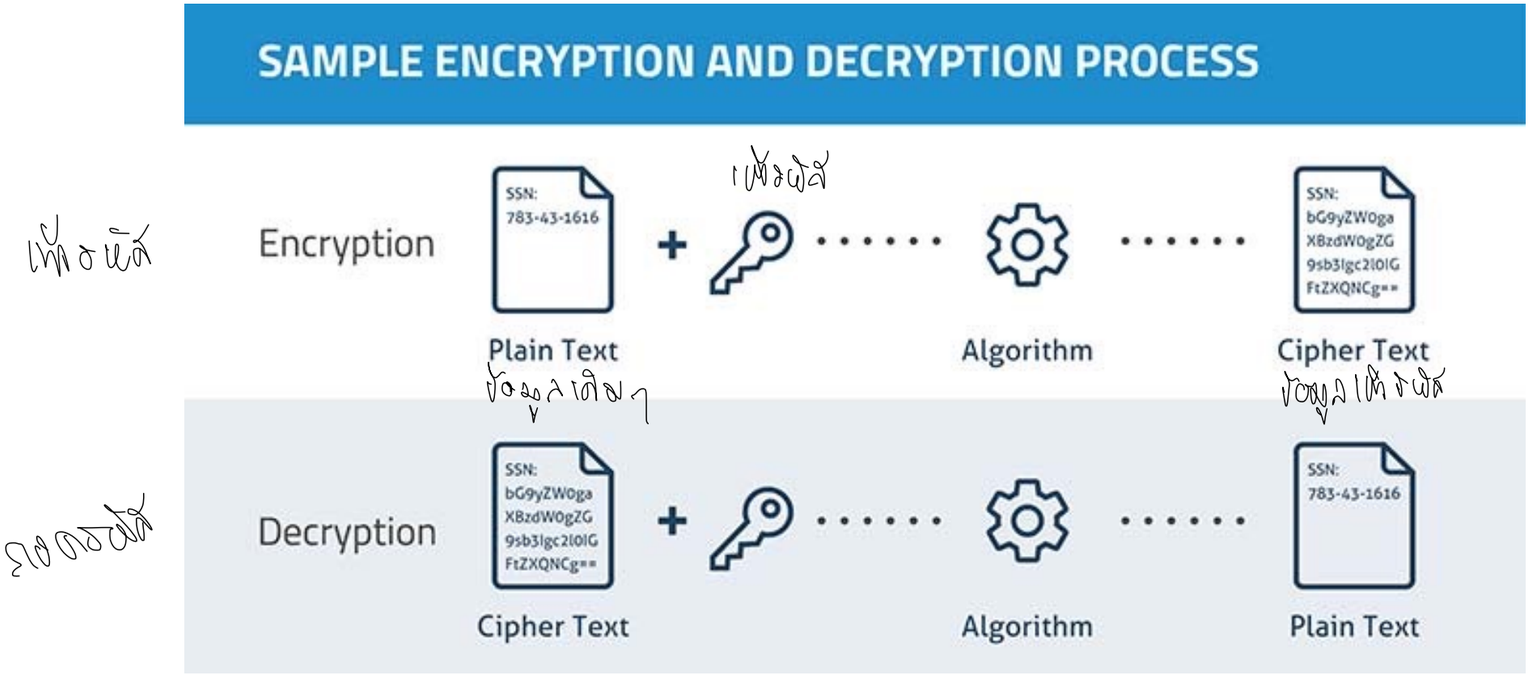
Understanding Core Security Goals

Confidentiality

- Encryption
- Access controls
- Steganography

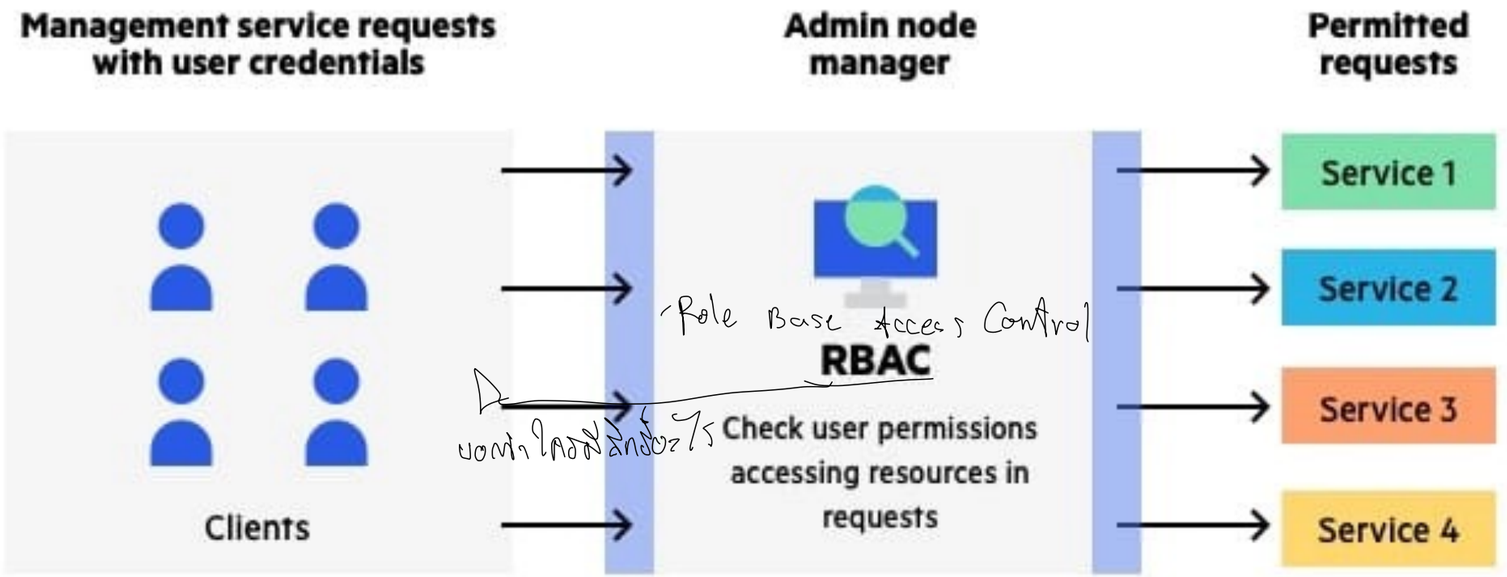
Confidentiality

Encryption



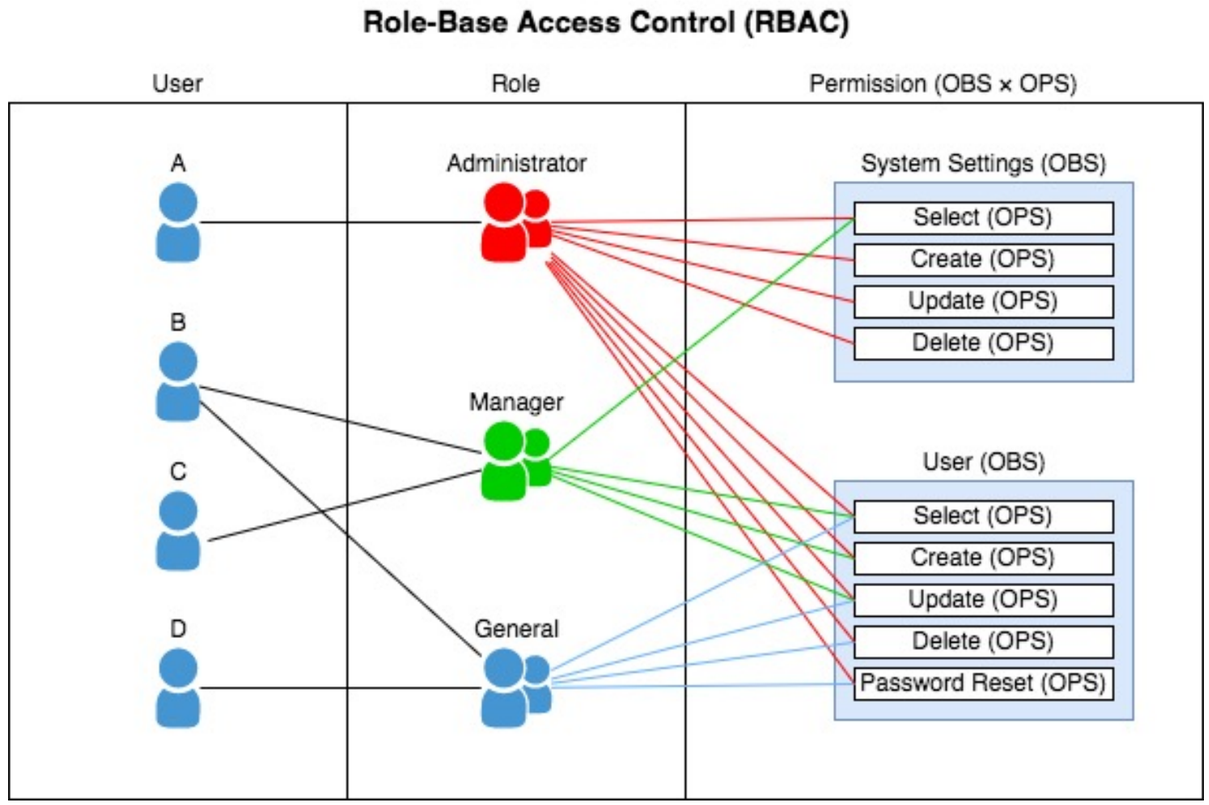
Confidentiality

Access control



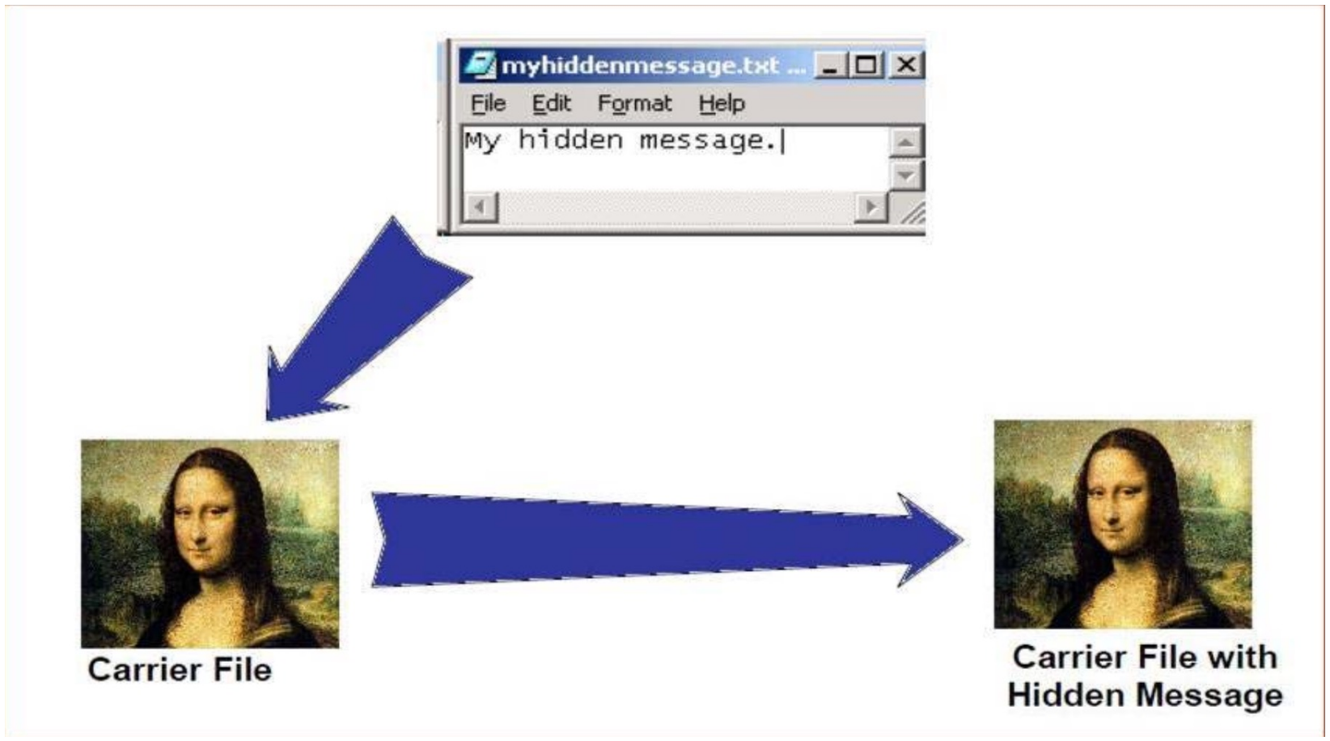
Confidentiality

Access control



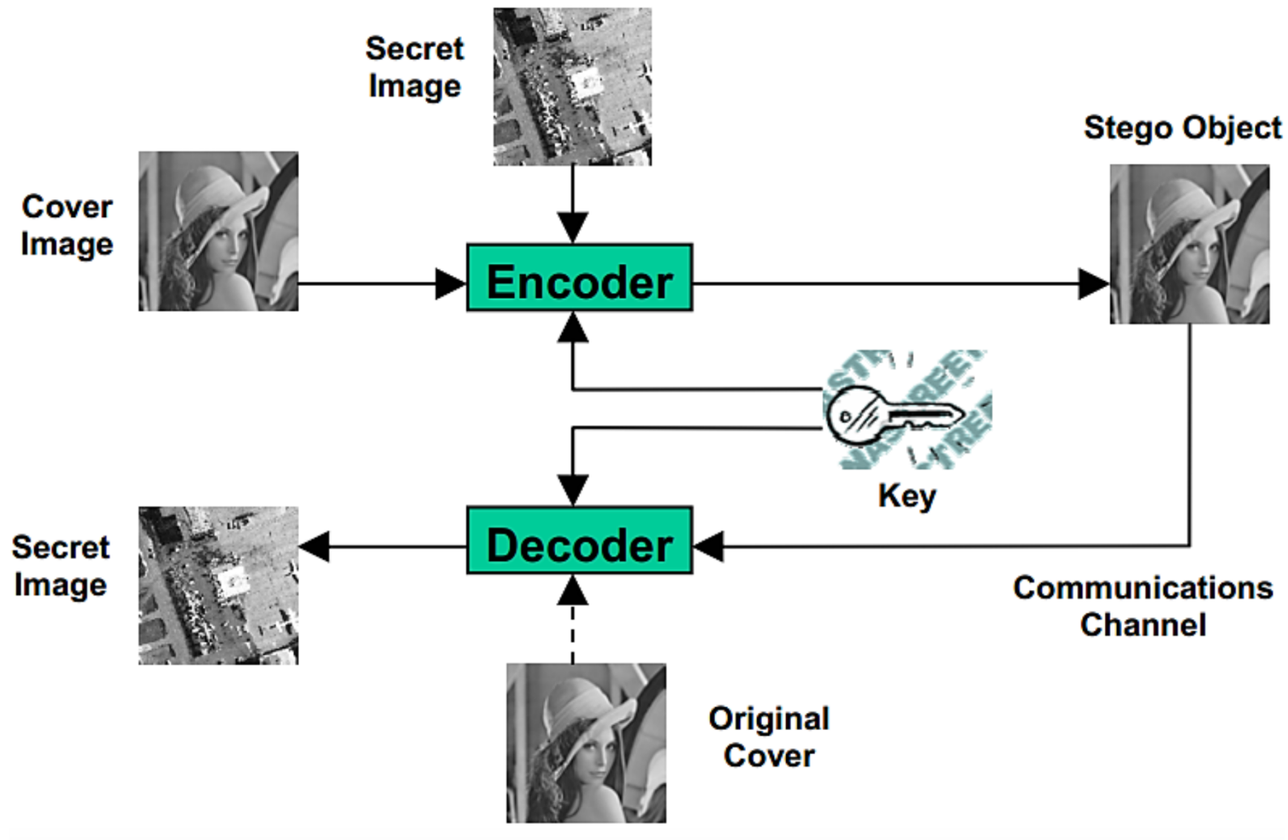
Confidentiality

Steganography



Confidentiality

Steganography

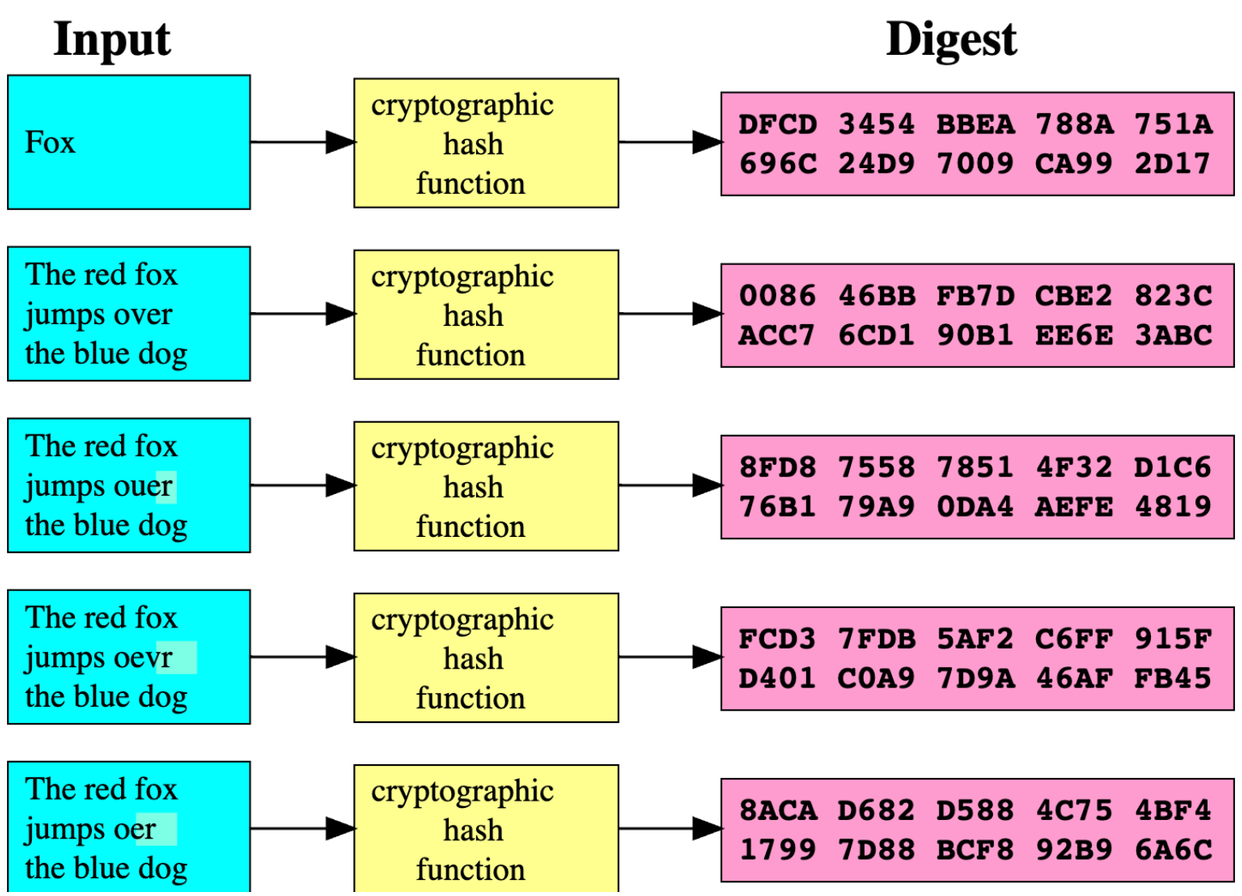


Integrity

- Hashing
- Digital signatures
- Certificates
- Non-repudiation

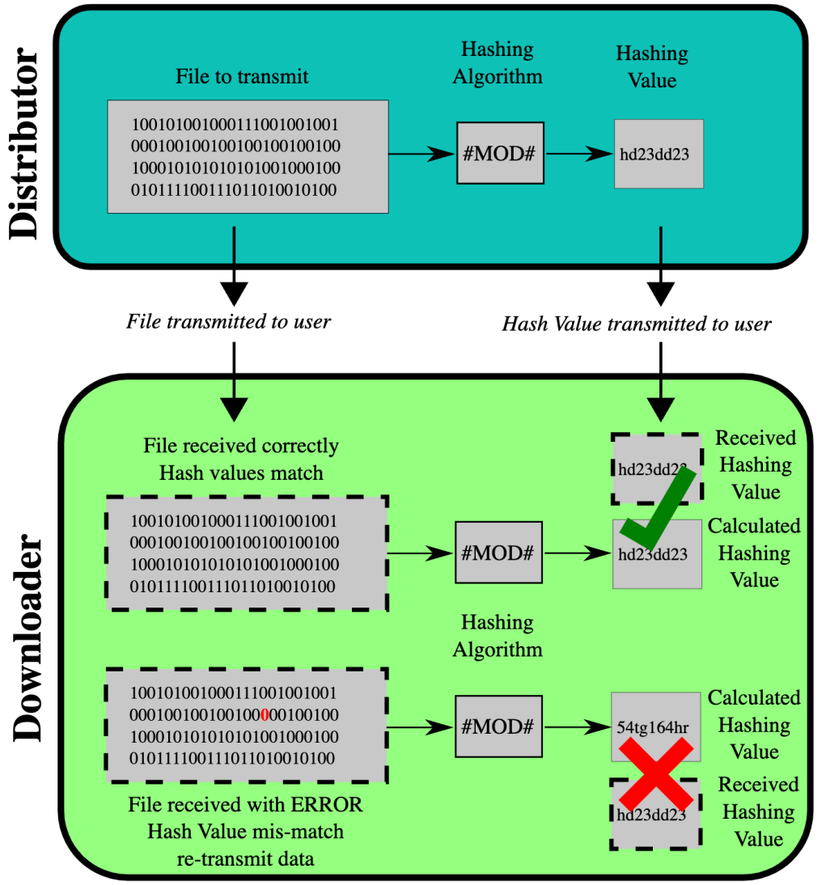
Integrity

Hashing



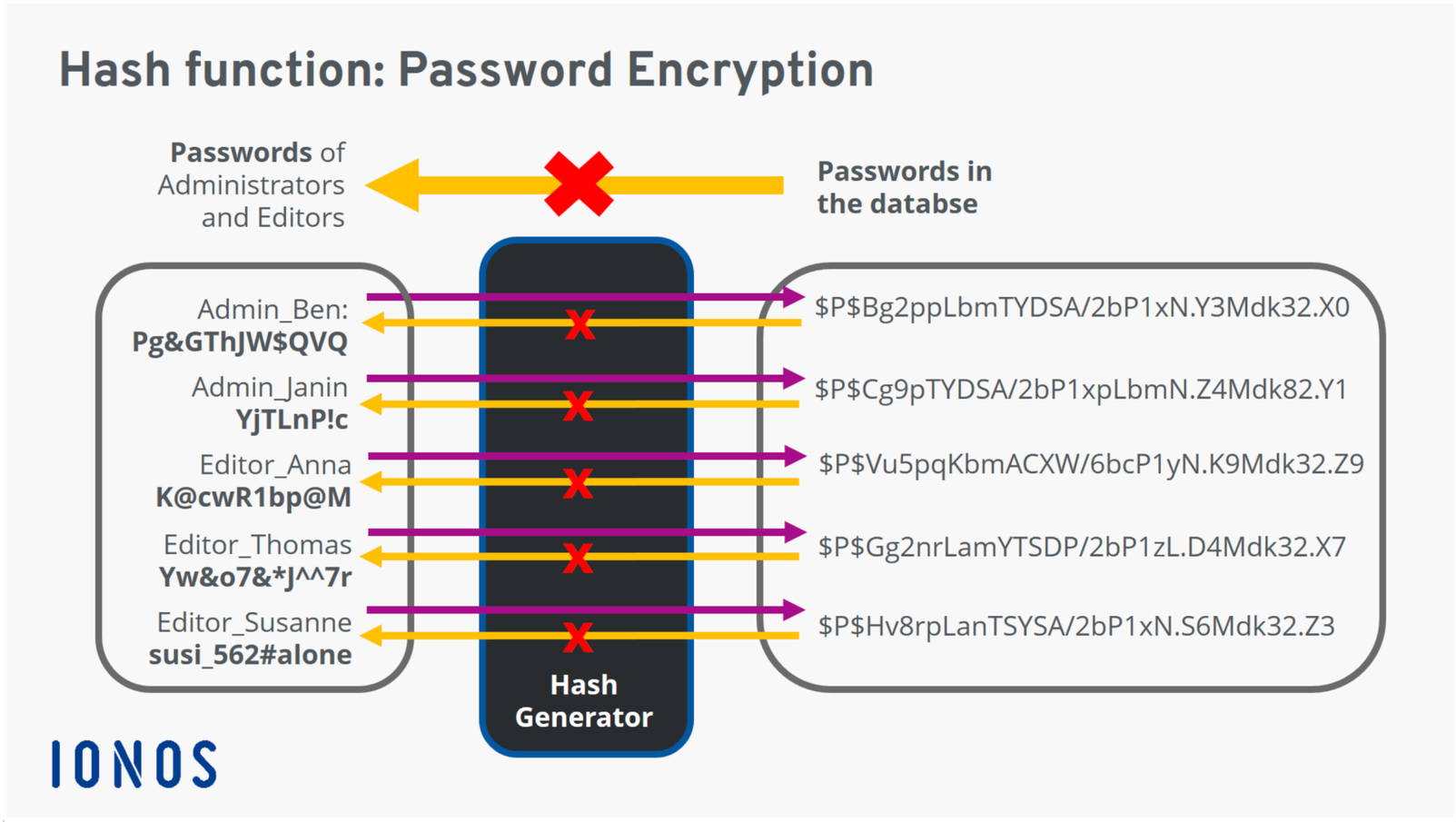
Integrity

Hashing



https://en.wikipedia.org/wiki/MD5

Integrity


Hash function: Password Encryption
Passwords of Administrators and Editors
Passwords in the databse
Admin_Ben:
Pg&GThJW$QVQ
PBg2ppLbmTYDSA/2bP1xN.Y3Mdk32.X0
Admin_Janin
YjTLnP!c
PCg9pTYDSA/2bP1xpLbmN.Z4Mdk82.Y1
Editor_Anna
K@cwR1bp@M
PVu5pqKbmACXW/6bcP1yN.K9Mdk32.Z9
Editor_Thomas
Yw&o7&*J^^7r
PGg2nrLamYTSDP/2bP1zL.D4Mdk32.X7
Editor_Susanne
susi_562#alone
PHv8rpLanTSYSA/2bP1xN.S6Mdk32.Z3
Hash Generator
IONOS

Integrity

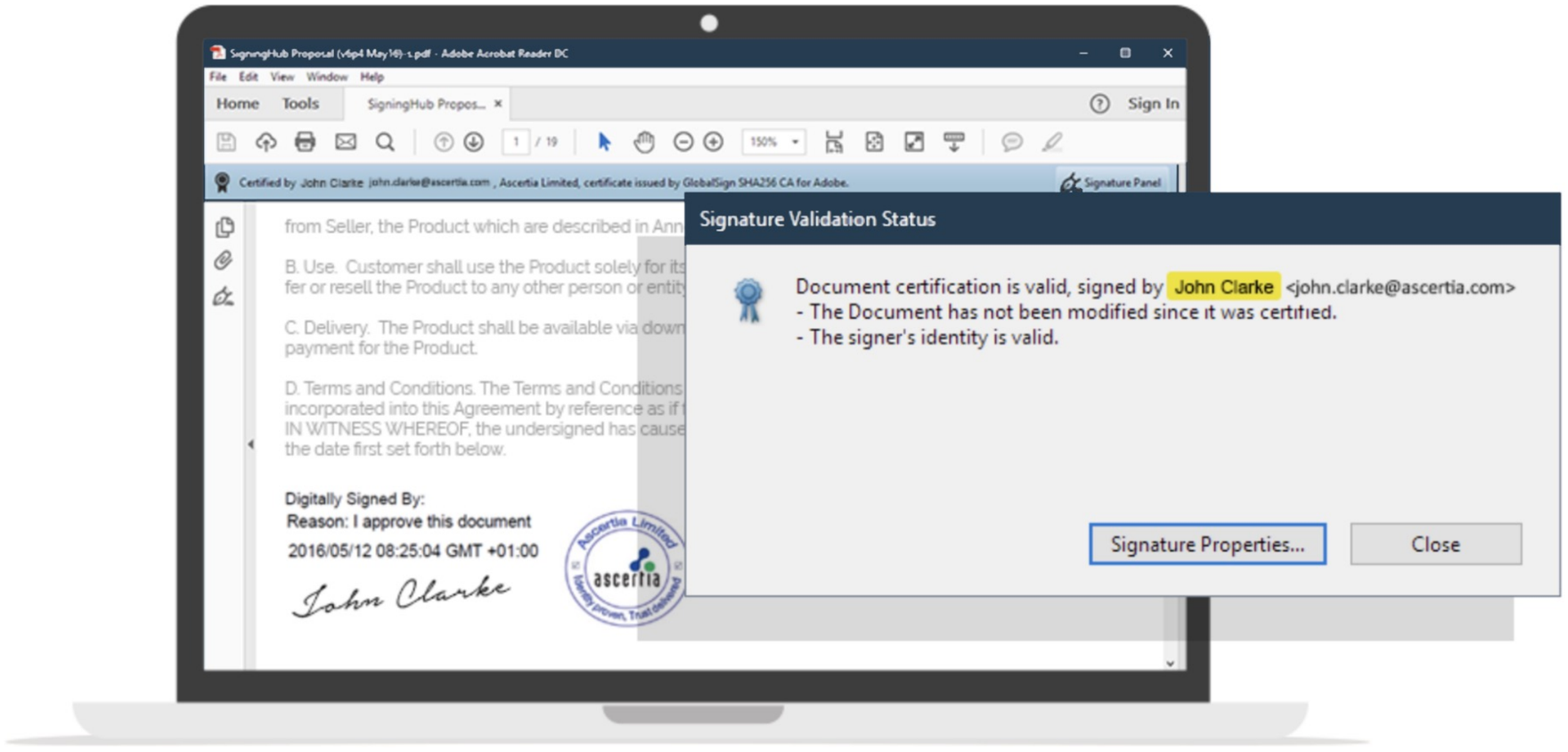
Digital signatures

https://www.linkedin.com/pulse/digital-signature-electronic-ihits-technologies-technologies-/

Integrity

Digital signatures

https://www.codium.co/blogs/30-What-the-difference-between-e-signature-and-digital-signature



CODIUM

https://www.codium.co/blogs/30-What-the-difference-between-e-signature-and-digital-signature

Integrity

Digital signatures

https://www.codium.co/blogs/30-What-the-difference-between-e-signature-and-digital-signature

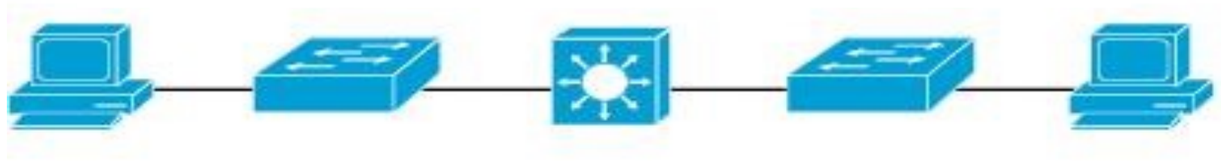
Availability

- Redundancy
- Fault tolerance
- Patching

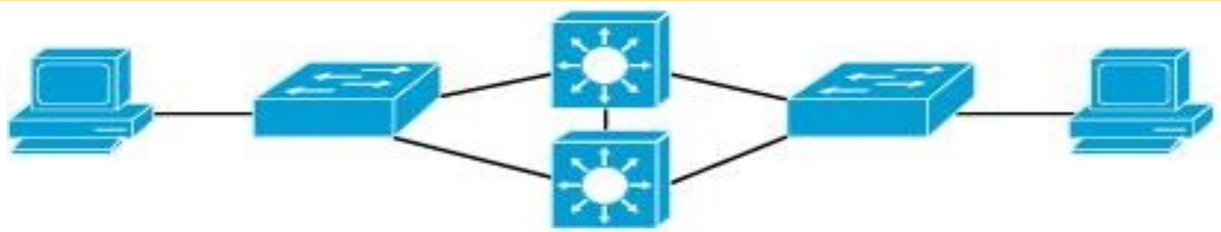
Availability

Redundancy & Fault tolerance

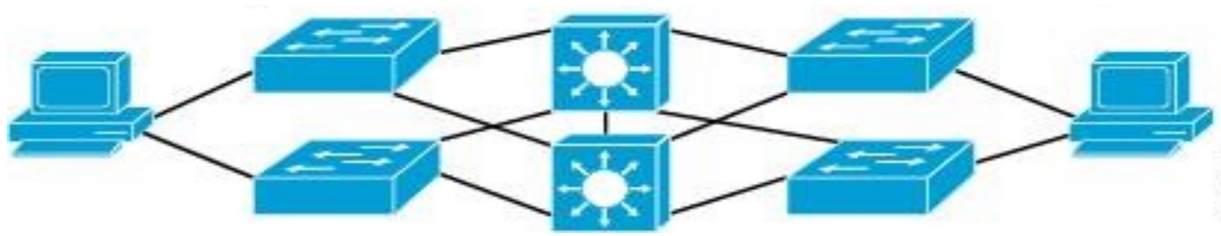
1



2



3

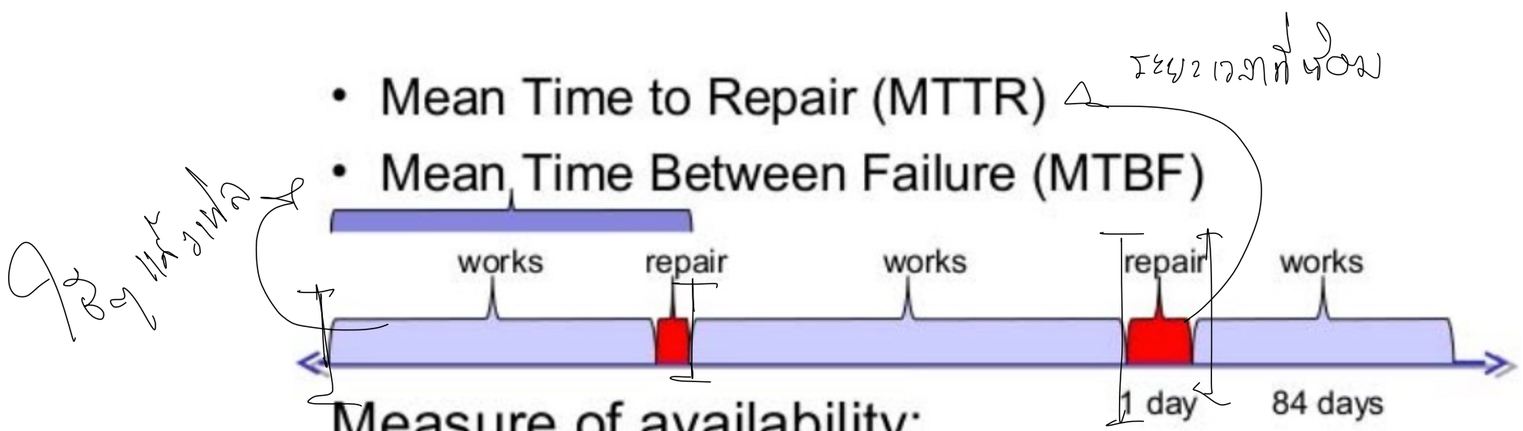


Availability

Mean Time Between Failures

MTBF = MTTF + MTTR

- Mean Time to Repair (MTTR)
- Mean Time Between Failure (MTBF)



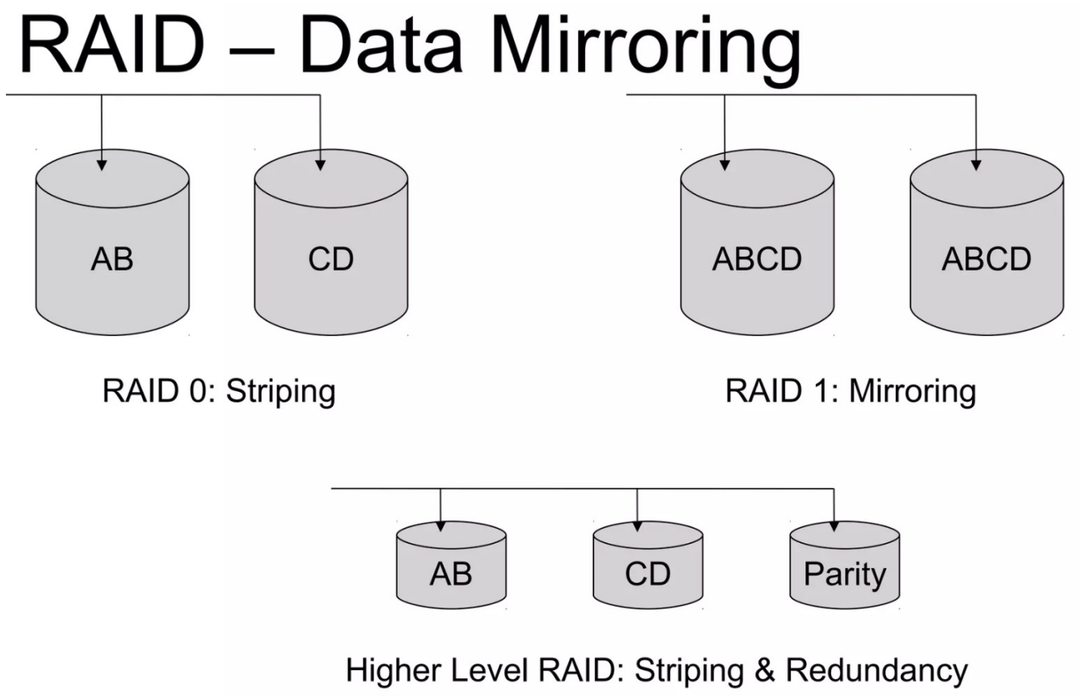
Measure of availability:

- 5 9s = 99.999% of time working = 5 ½ minutes of failure per year.

https://www.slideshare.net/MuhammadAdeelJavaid1/business-continuity-and-disaster-recovery-24531073

Availability

Redundancy & Fault tolerance



Redundant Array of Independent Disks

https://www.slideshare.net/MuhammadAdeelJavaid1/business-continuity-and-disaster-recovery-24531073

Availability

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

https://serverfault.com/questions/316637/100-uptime-for-a-web-application

Understanding Core Security Goals

Safety

Safety of people and safety of assets

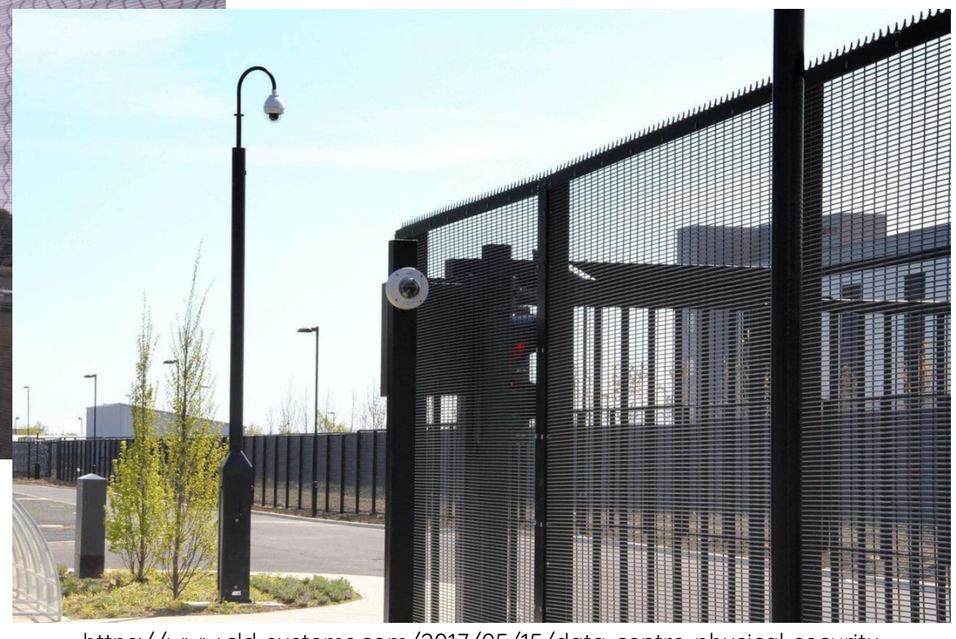
- Fencing รั้วกั้น
- Lighting แสงสว่าง
- Locks
- CCTV

- Escape plans
- Drills
- Escape routes

Safety

Fencing

https://securityvaultsystems.com/security-fences



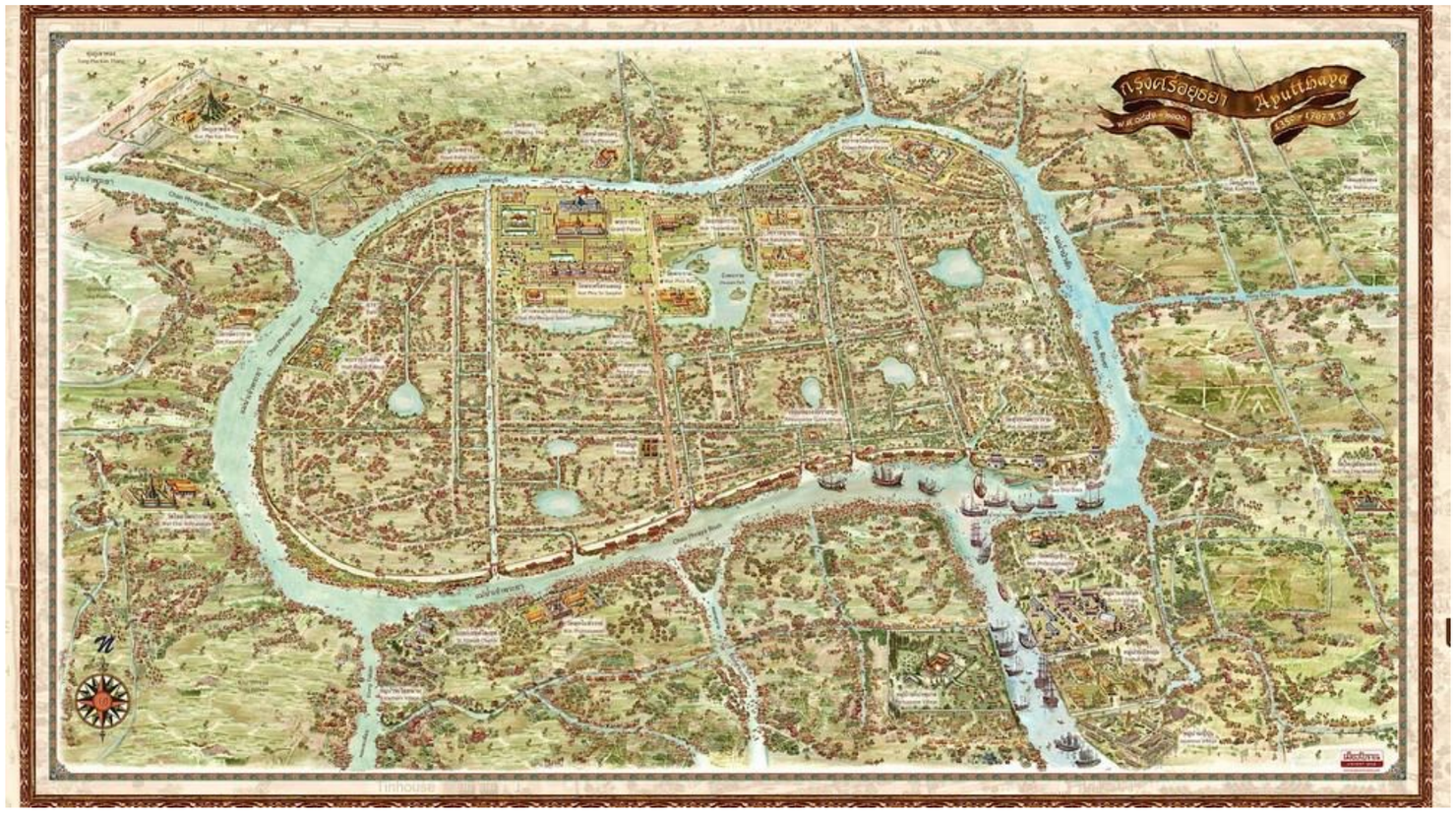
https://www.cld-systems.com/2017/05/15/data-centre-physical-security

Safety

Tourism people architecture house Netherlands water trees garden grass village boat flowers canal summer wallpaper

Safety

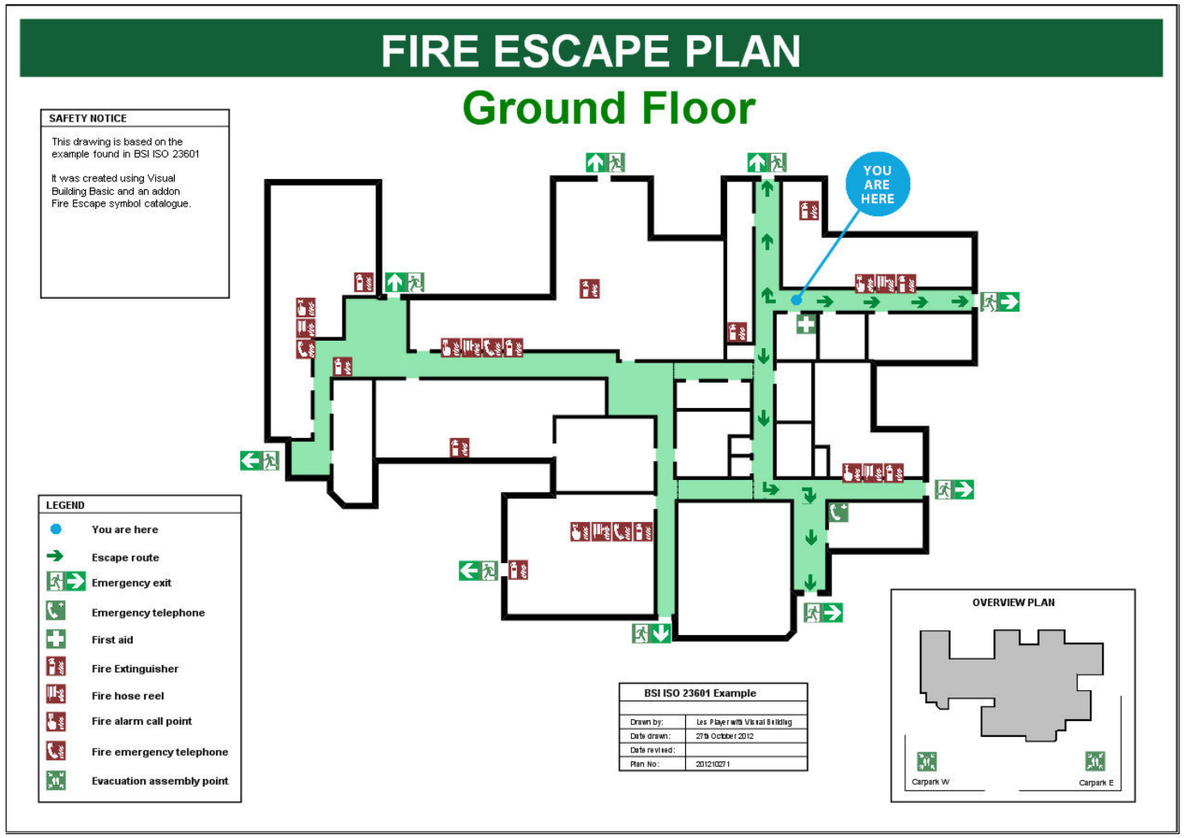
AYUTHAYA CAPITAL Map



https://www.facebook.com/HistoryKrungsriAyutthaya/photos/a.848161005257838/1302843383122929/

Safety

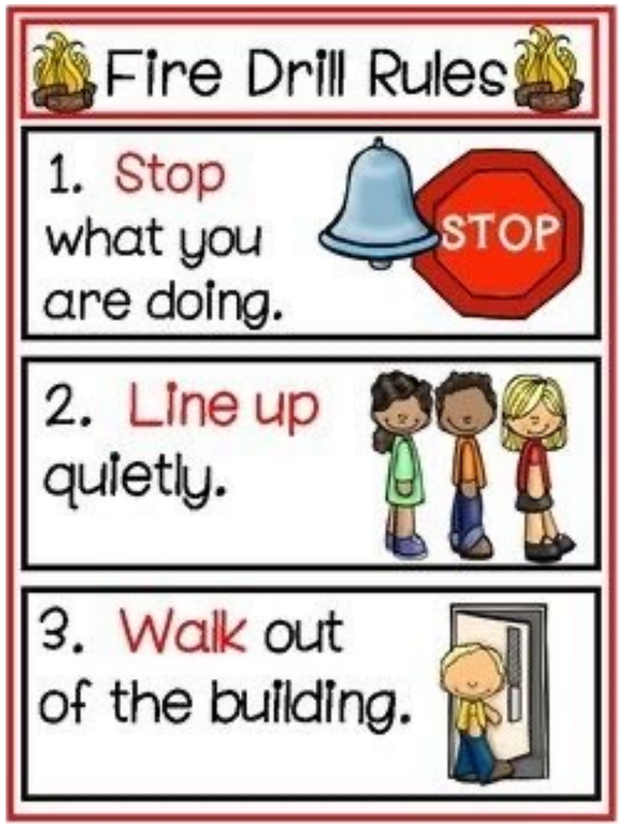
Fire Evacuation Plans / Fire Escape Plans



https://www.visualbuilding.co.uk/guides/specials/fire-escape-plans

Safety

Fire Evacuation Plans / Fire Escape Plans



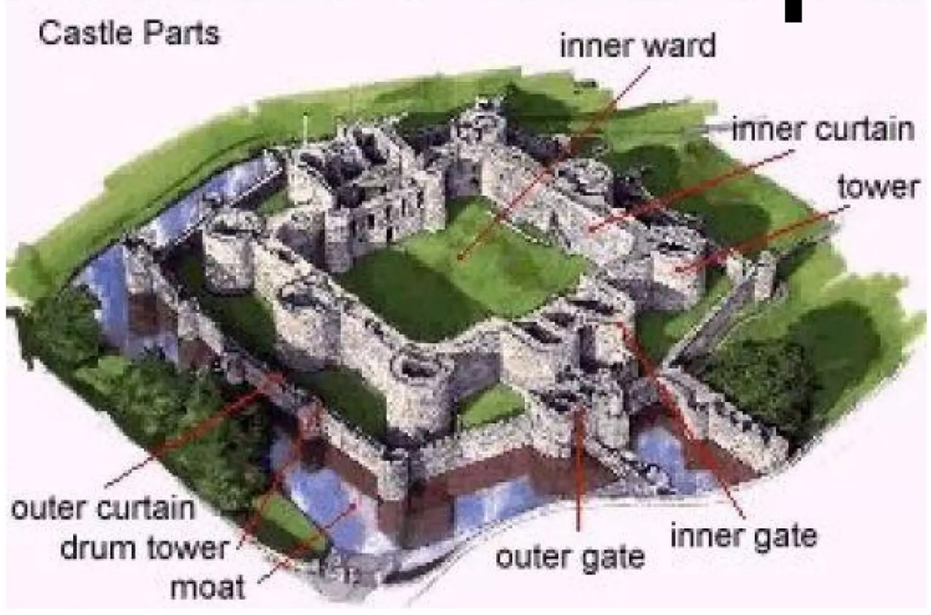
https://www.pinterest.com/pin/406449935119224265

Layered Security / Defense in Depth

Security is never done

- Defense in depth
- Employs multiple layers of security

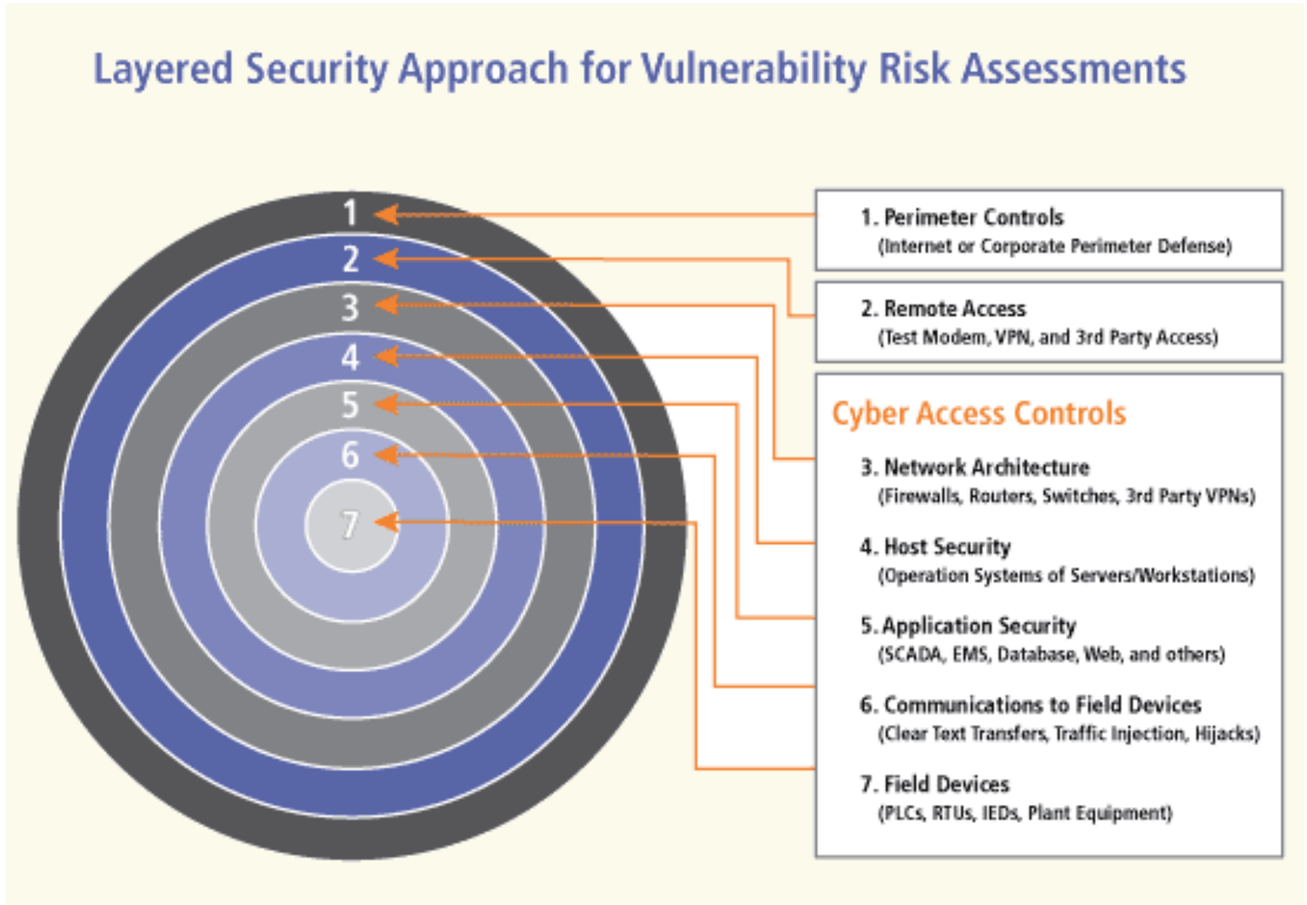
Safety
Defence in Depth



Shepherding Solution Architecture Security Decisions

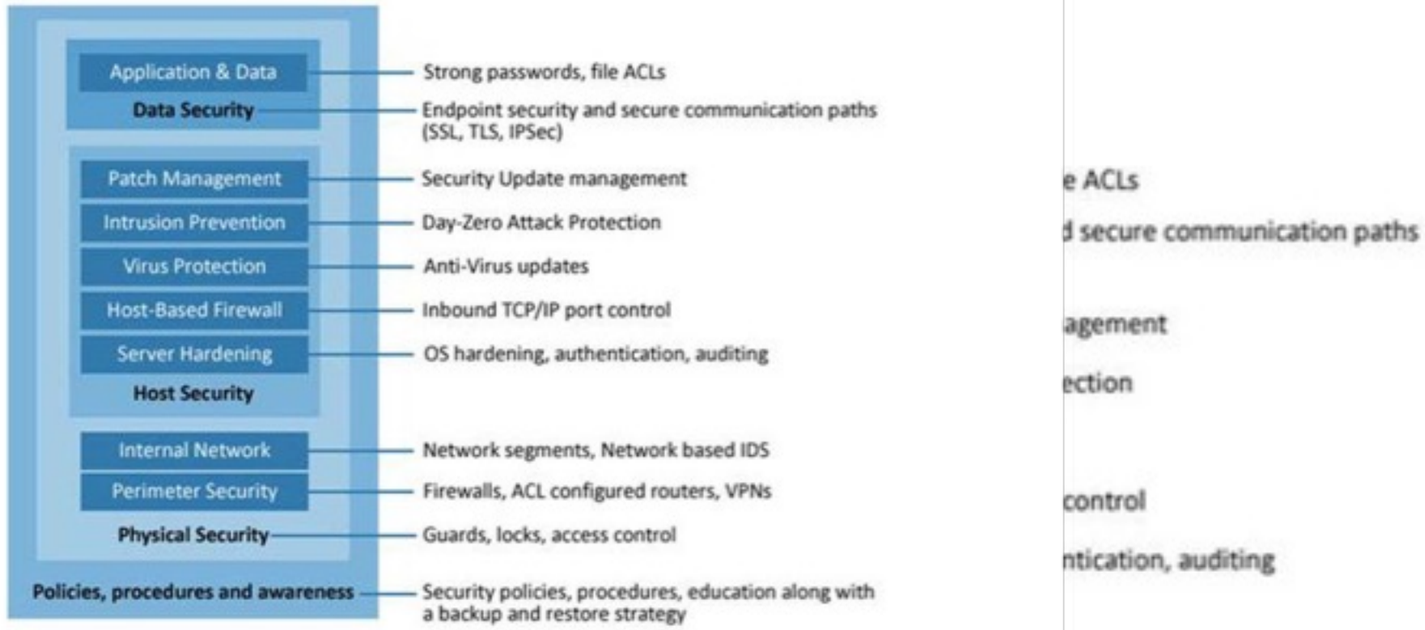
https://www.slideshare.net/prawsthorne/defen

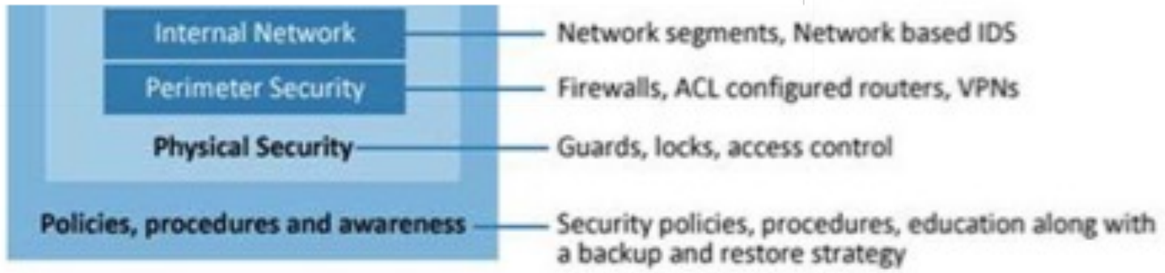
Safety



https://www.remote-instruments.com/secure.html

Safety

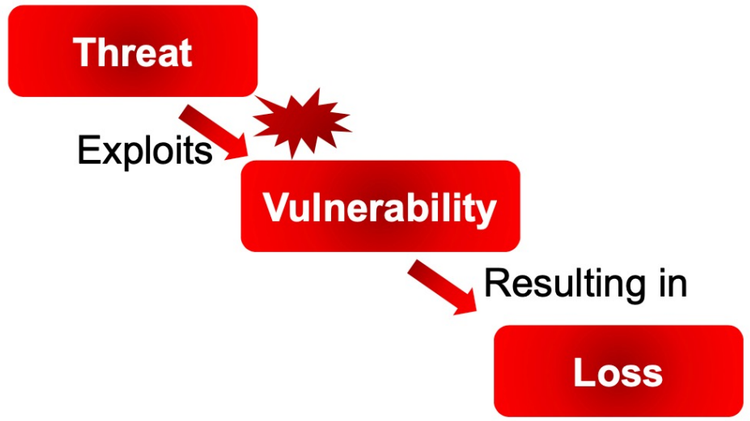




https://www.cyberoam.com/blog/defense-in-depth/

Introduce Basic Risk Concept

- Threats
- Vulnerabilities
  - Any weakness
- Risk is
  - The likelihood that a threat will exploit a vulnerability.
- Risk mitigation
  - Reduces the chances that a threat will exploit a vulnerability by implementing controls.



Exploring Authentication Concepts

- Identification
  - User professes an identity
- Authentication
  - User proves identity
- Authorization
  - Access to resources granted based on proven identity

Verifying Identities

- Verifying people are who they claim to be
- Identity proofing for verification
- Self-service Password Reset Systems

Factors of Authentication

- Something you know
  - Such as username and password
- Something you have
  - Such as a smart card
- Something you are
  - Such as a fingerprint or other biometric identification
- Somewhere you are
  - Such as your location obtained using geolocation
- Something you do
  - Such as gestures on a touch screen

Factors of Authentication

Something you know

Password

- Should be strong
- Should be changed regularly
- Validate identities before resetting
- Prevent password reuse with password history
- Protect with account lockout policies
- Default passwords should be changed
- Previous logon notification
- Passwords should not be written down
- Passwords should not be shared
- Provide training to users

Factors of Authentication

Something you have

- Smart cards
  - CACs (Common Access Cards)
    and PIVs (Personal Identity Verifications) (US government)

- Proximity card

http://www.tdsi.co.uk/proximity_cards.html

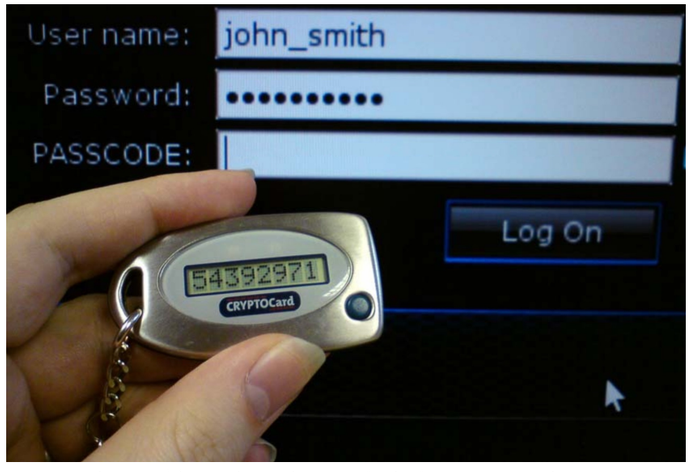
Factors of Authentication

Something you have

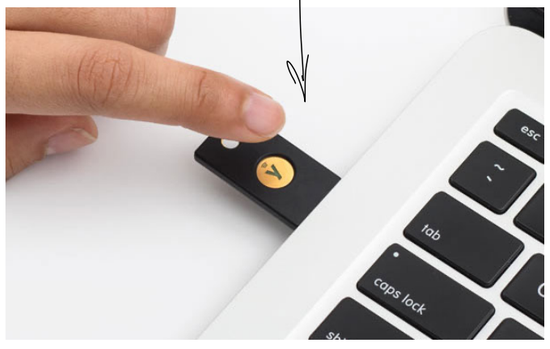
- Tokens or Key fobs

multi factor

Commonly combined with something you know (MFA)



https://en.wikipedia.org/wiki/Security_token



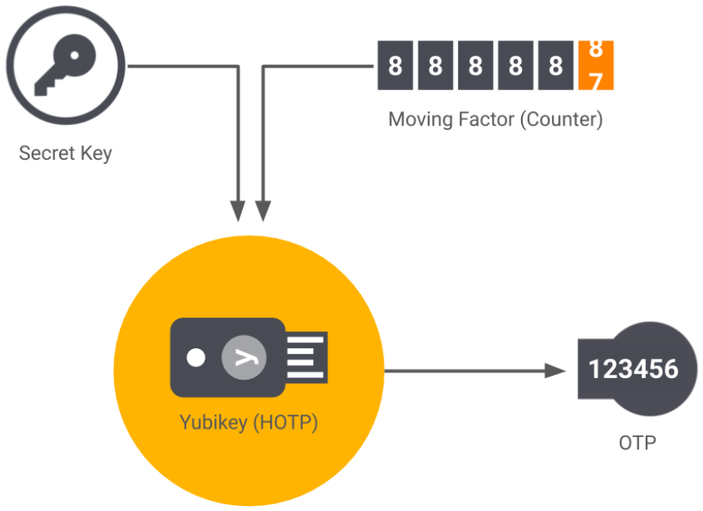
https://www.ldlc.com/en/product/PB00405118.html

https://www.cnet.com/news/privacy/usb-c-hardware-security-keys-get-cheaper-with-29-yubikey/

Factors of Authentication

Something you have

- HOTP
  - HMAC-based One-time Password
  - Event-based



Limitations and Advantages
HOTP doesn't have the time-based limitation, it's a little more user-friendly, but may be more susceptible to brute force attack. That's because of a potentially longer window in which the HOTP is valid. Some forms of HOTP have accounted for this vulnerability by adding a time-based component to their code.

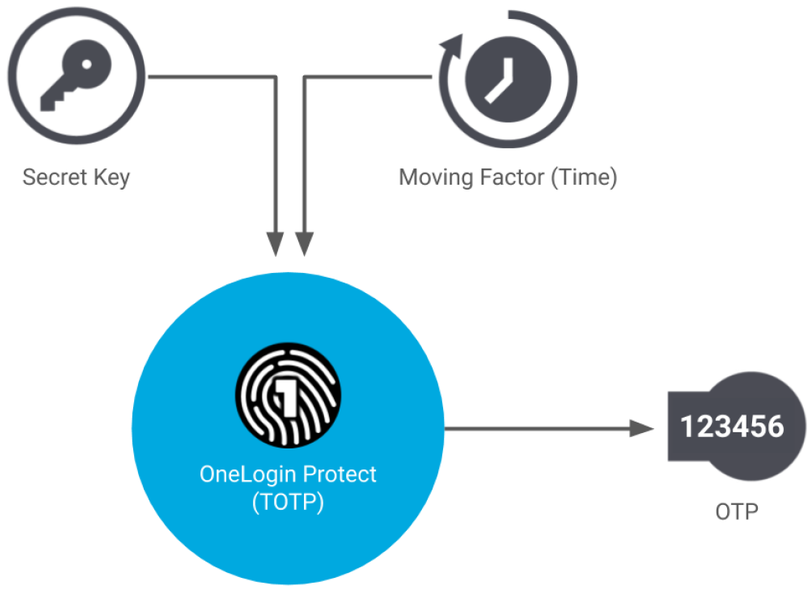
https://www.ldlc.com/en/product/PB00405118.html

https://www.cnet.com/news/privacy/usb-c-hardware-security-keys-get-cheaper-with-29-yubikey/

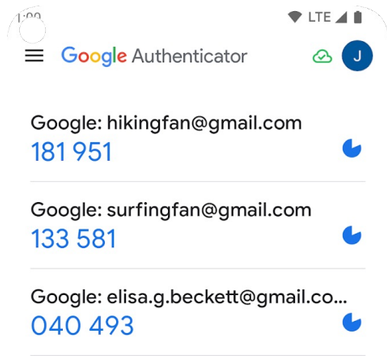
Factors of Authentication

Something you have

- TOPT
  - Time-based One-Time Password
  - Expire after 30 seconds



Limitations and Advantages
The time-based element does have a potential for time-drift (the lag between the password creation and use). If the user doesn't enter the TOTP right away, there's a chance it will expire before they do. So, the server has to account for that and make it easy for the user to try again without automatically locking them out.



Factors of Authentication

Something you are

Biometrics Methods

- Fingerprint, Thumbprint, or Handprints
- Retinal scanners (scans the retina of one or both eyes)
- Iris scanners(scans the iris of one or both eyes)

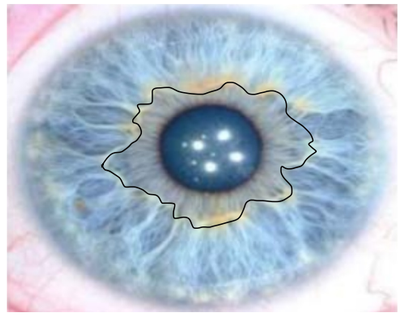
Factors of Authentication

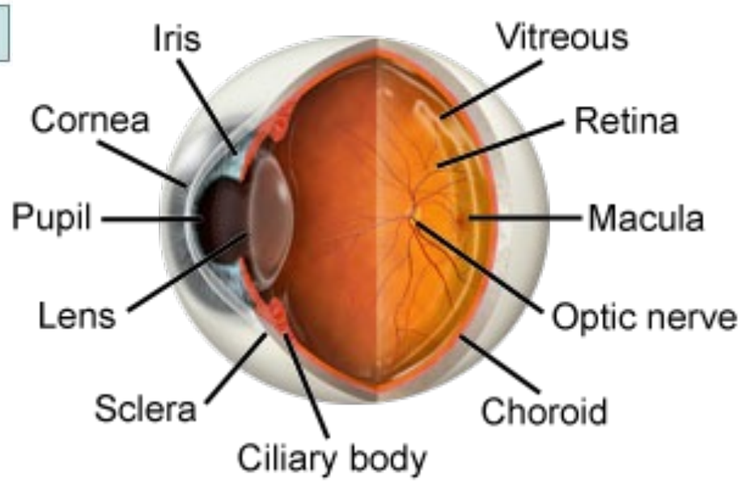
Something you are

- Retinal scanners (scans the retina of one or both eyes)
- Iris scanners(scans the iris of one or both eyes)

Focusing on the colored area around the pupil

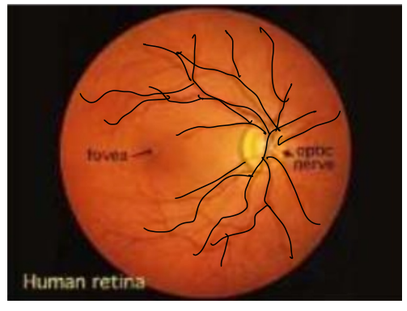
Iris scanning





Retina scans focus on the pattern of blood vessels at the back of the eye.

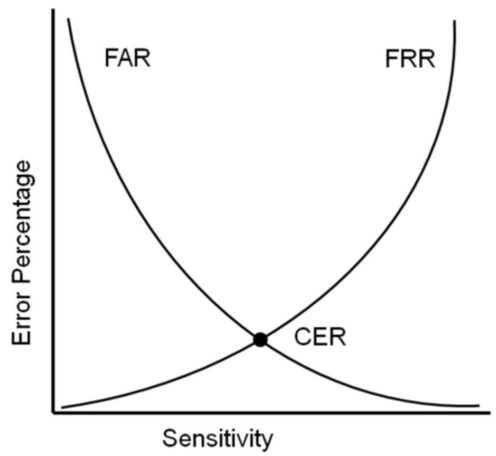
Retina scanning



Factors of Authentication

Something you are

- Fingerprint, Thumbprint, or Handprints
    - False rejection rate (FRR) (Type I Error): rejects an authorized user
    - False acceptance rate (FAR) (Type II Error): identifies an unauthorized user as an authorized user
    - Crossover error rate
        - The lower the number or percentage, the more accurate the biometrics system is. For example, a CER of 2 (or 2 percent) is much better than a CER of 10 (or 10 percent).



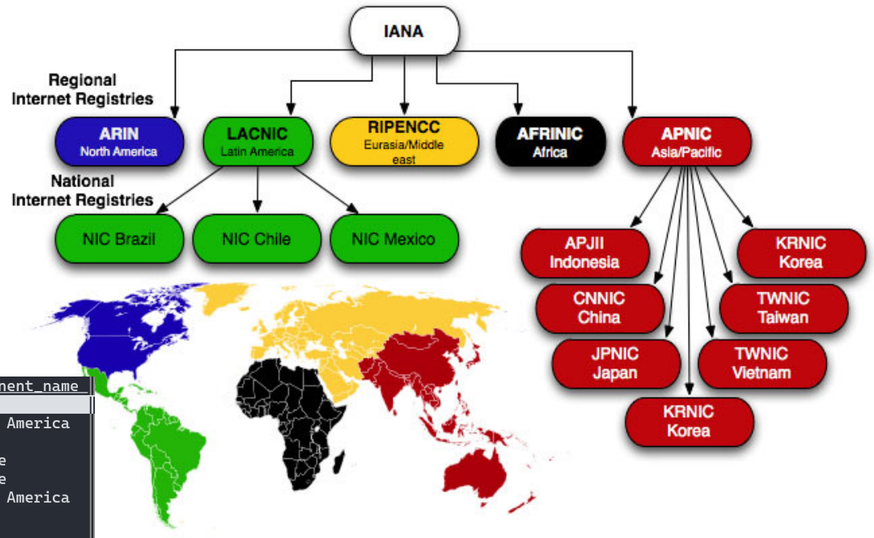
Ref: CISSP Study Guide, Third Edition, Eric Conrad and Seth Misenar, Dec 3, 2015

Factors of Authentication

Somewhere you are

Biometrics Methods

- Often uses geolocation
  - IP address
  - MAC address

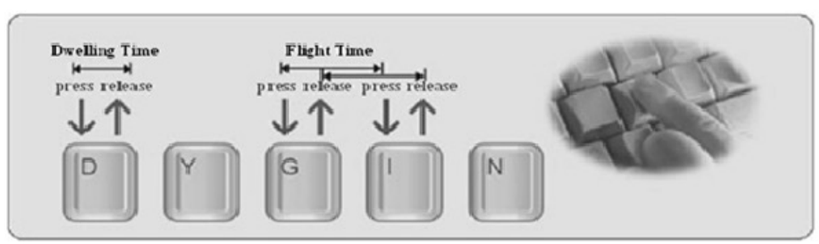


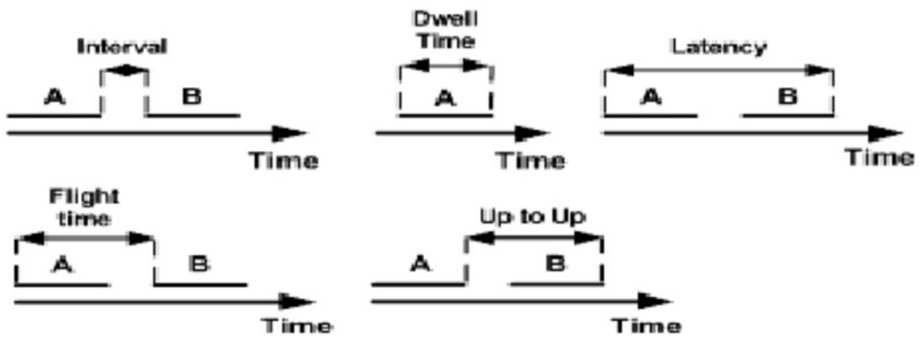
start_ip	end_ip	country	country_name	continent	continent_name
223.119.47.207	223.119.47.208	HK	Hong Kong	AS	Asia
2801:80:721::	2801:80:72f:ffff:f…	UY	Uruguay	SA	South America
26.59.248.128	26.59.248.255	IR	Iran	AS	Asia
25.165.117.128	25.165.123.127	GB	United Kingdom	EU	Europe
2a01:4101::	2a01:411f:ffff:fff…	NL	Netherlands	EU	Europe
209.85.241.78	209.85.241.79	CL	Chile	SA	South America
2409:4061:2db7:d30…	2409:4061:2db7:d3f…	BD	Bangladesh	AS	Asia
13.105.106.224	13.105.106.255	JP	Japan	AS	Asia
185.137.120.0	185.137.123.255	DE	Germany	EU	Europe
36.94.168.138	36.94.168.147	ID	Indonesia	AS	Asia
164.52.36.0	164.52.37.255	JP	Japan	AS	Asia
130.176.164.0	130.176.164.255	BR	Brazil	SA	South America
2606:54c0:28e0:f8::	2606:54c0:28e0:f8:…	GB	United Kingdom	EU	Europe
2804:7fc1::	2804:7fc3:ffff:fff…	UY	Uruguay	SA	South America
2401:4900:713f:800…	2401:4900:713f:8ff…	BD	Bangladesh	AS	Asia
217.146.5.0	217.146.5.255	BR	Brazil	SA	South America
2001:67c:22c0::	2001:67c:22c0:ffff…	SE	Sweden	EU	Europe
2001:4c08:2e10:180…	2001:4c08:2e10:1fe…	GB	United Kingdom	EU	Europe
25.74.229.0	25.74.237.255	GB	United Kingdom	EU	Europe
2a02:5747:198::	2a02:5747:198:ffff…	UA	Ukraine	EU	Europe
154.195.84.0	154.195.85.255	MU	Mauritius	AF	Africa
2606:54c0:27c0:1a1…	2606:54c0:27c0:1a1…	FR	France	EU	Europe
94.142.101.65	94.142.101.68	GB	United Kingdom	EU	Europe
81.201.80.241	81.201.80.242	US	United States	NA	North America
202.165.251.0	202.165.255.255	CN	China	AS	Asia

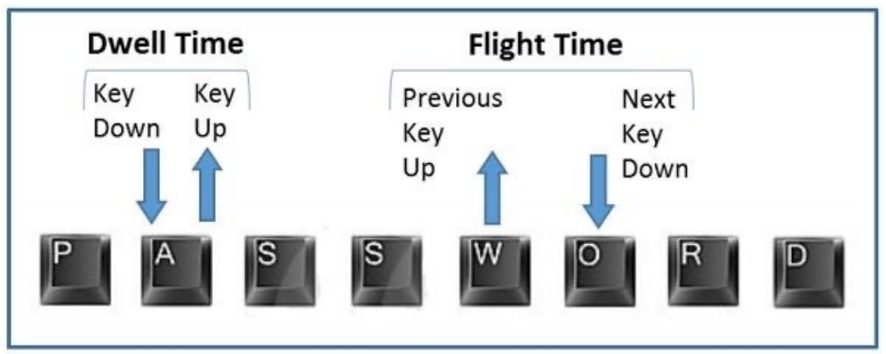
Factors of Authentication

Something you Do

- Gestures
- Keystrokes on keyboard
  - Dwell time
  - Flight time







Factors of Authentication

Multifactor Authentication

Combines authentication from two or more factors

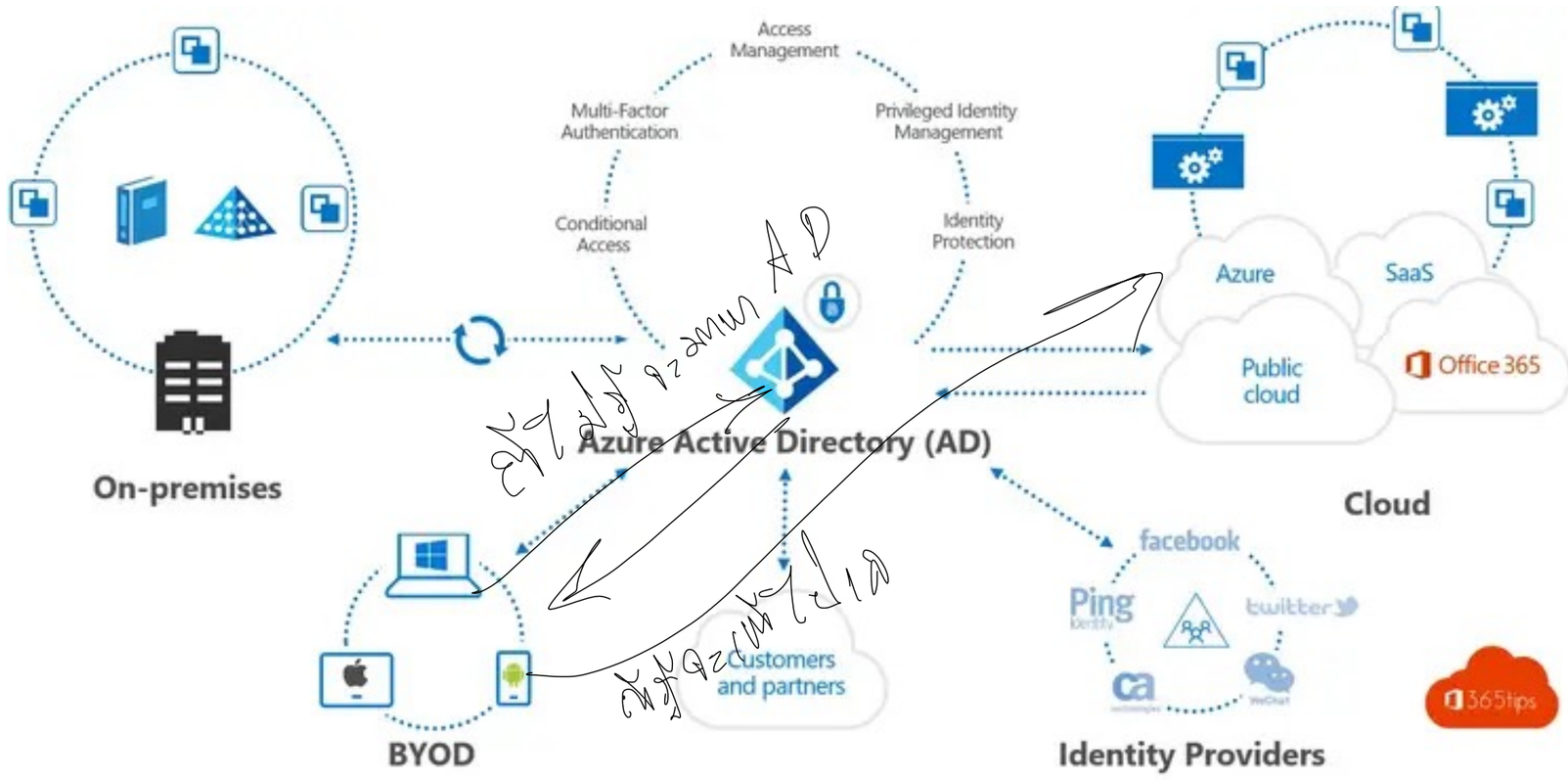
Examples:

- PIN and CAC
- PIV and password
- Fingerprint and smart card
- Password and Token key

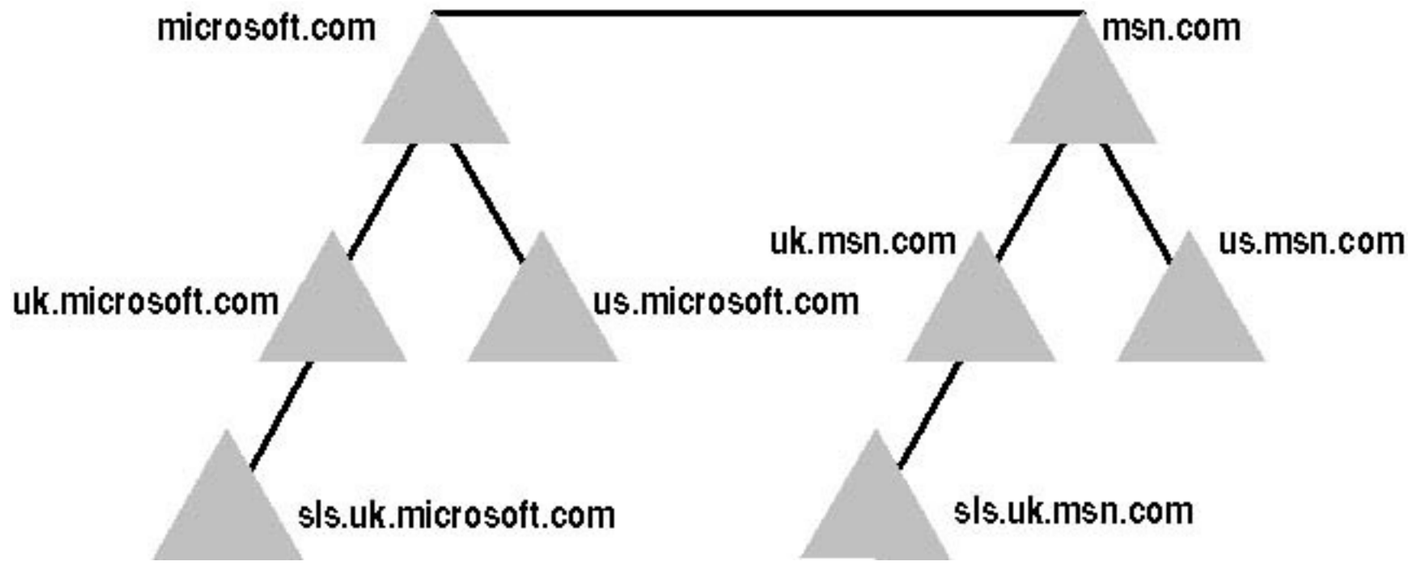
AD vs Kerberos vs LDAP

- Active Directory
  - Windows database
    - Query for access control to object.
- Kerberos
  - Authentication and Access granting Service
- Light weight access protocol (LDAP)
  - Protocol for clients to query and manage information in Directory service (like AD)
    - TCP port 389

Active Directory (AD)

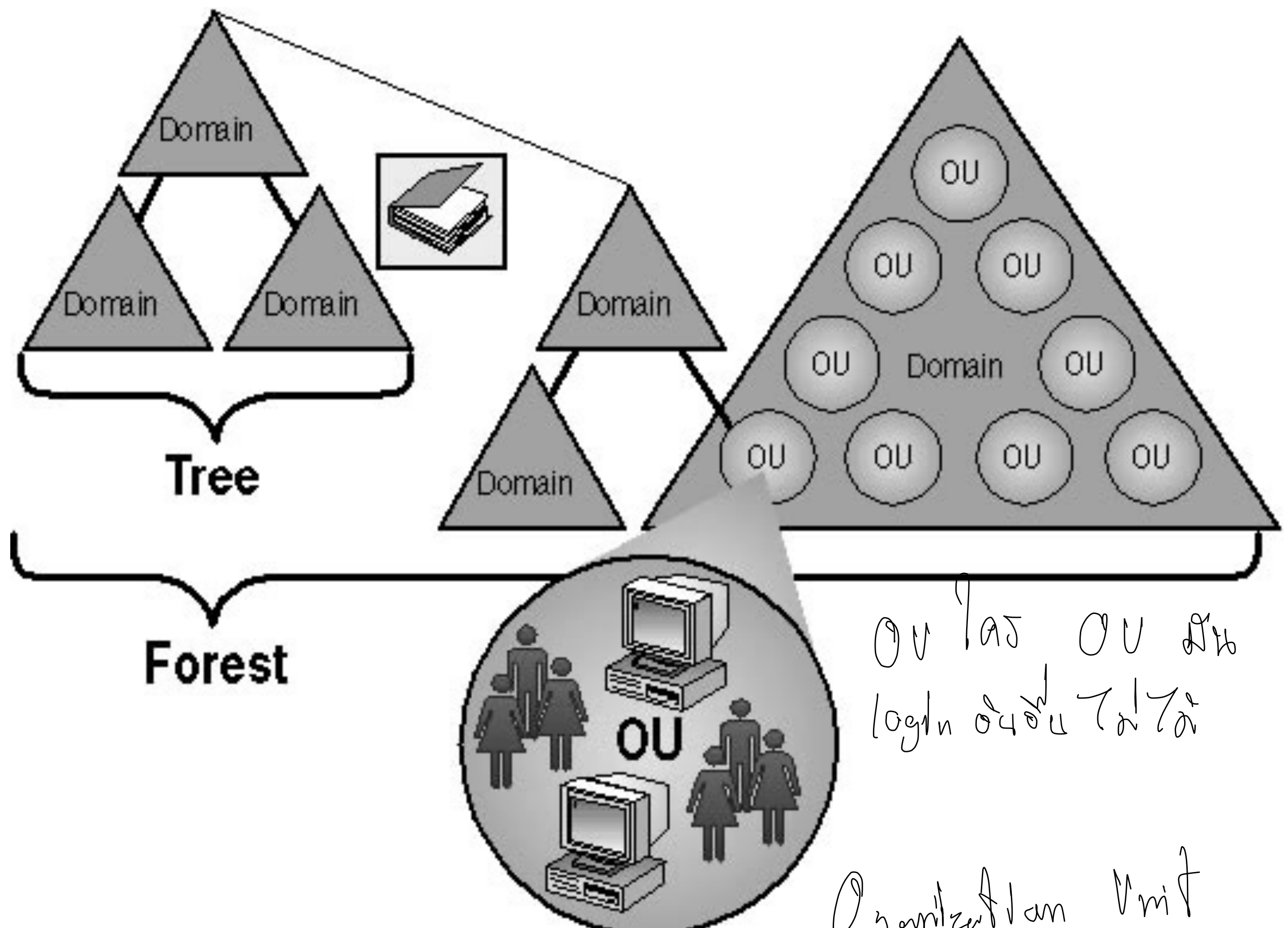


Active Directory (AD)



https://etutorials.org/Microsoft+Products/microsoft+windows+xp+professional+training+kit/Chapter+5+-+Using+the+DNS+Service+and+Active+Directory+Service/Lesson+5nbspUnderstanding+Active+Directory+Structure+and+Replication/

Active Directory (AD)

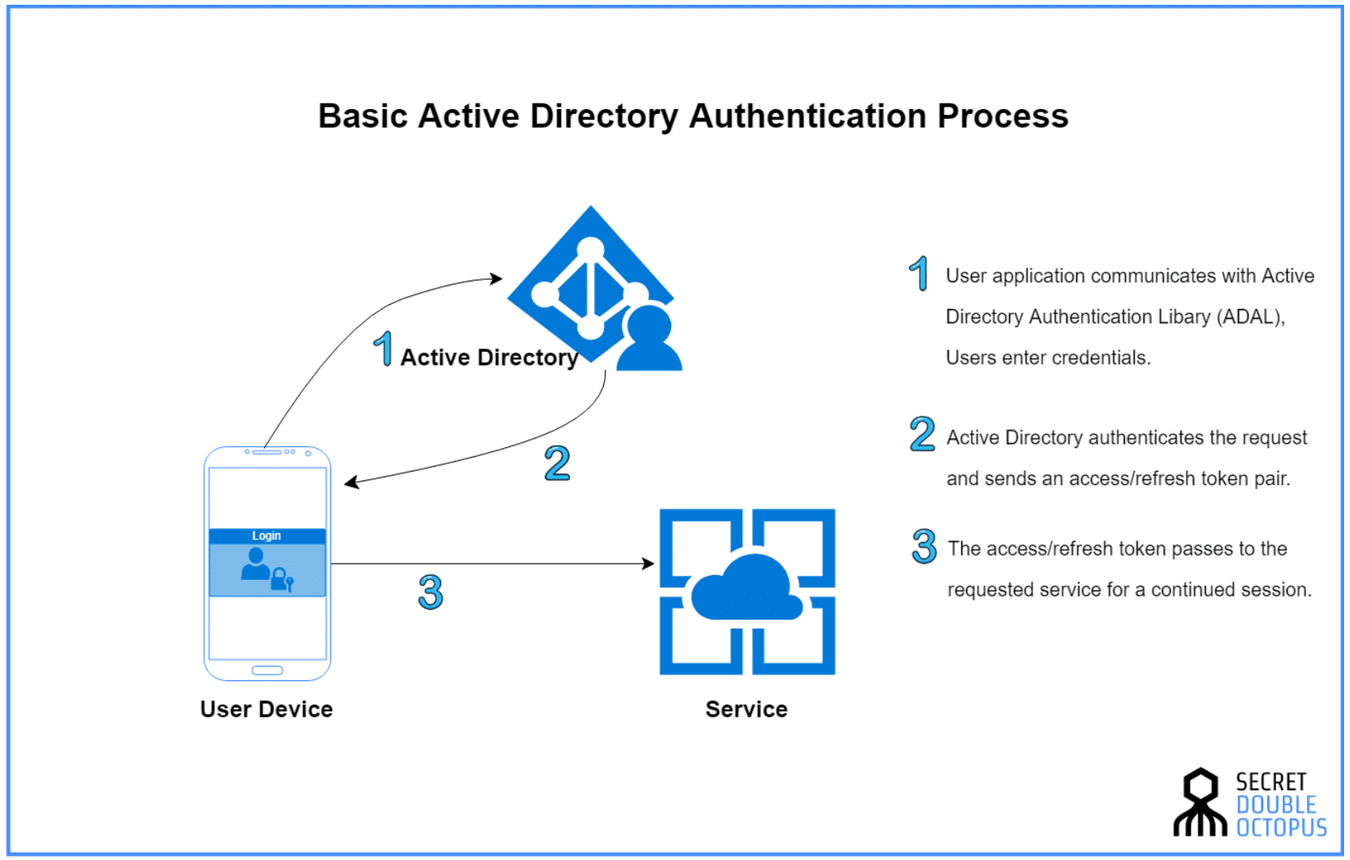


OU ไหน OU มัน
login อันอื่นไม่ได้

Organization Unit

https://etutorials.org/Microsoft+Products/microsoft+windows+xp+professional+training+kit/Chapter+5+-+Using+the+DNS+Service+and+Active+Directory+Service/Lesson+5nbspUnderstanding+Active+Directory+Structure+and+Replication/

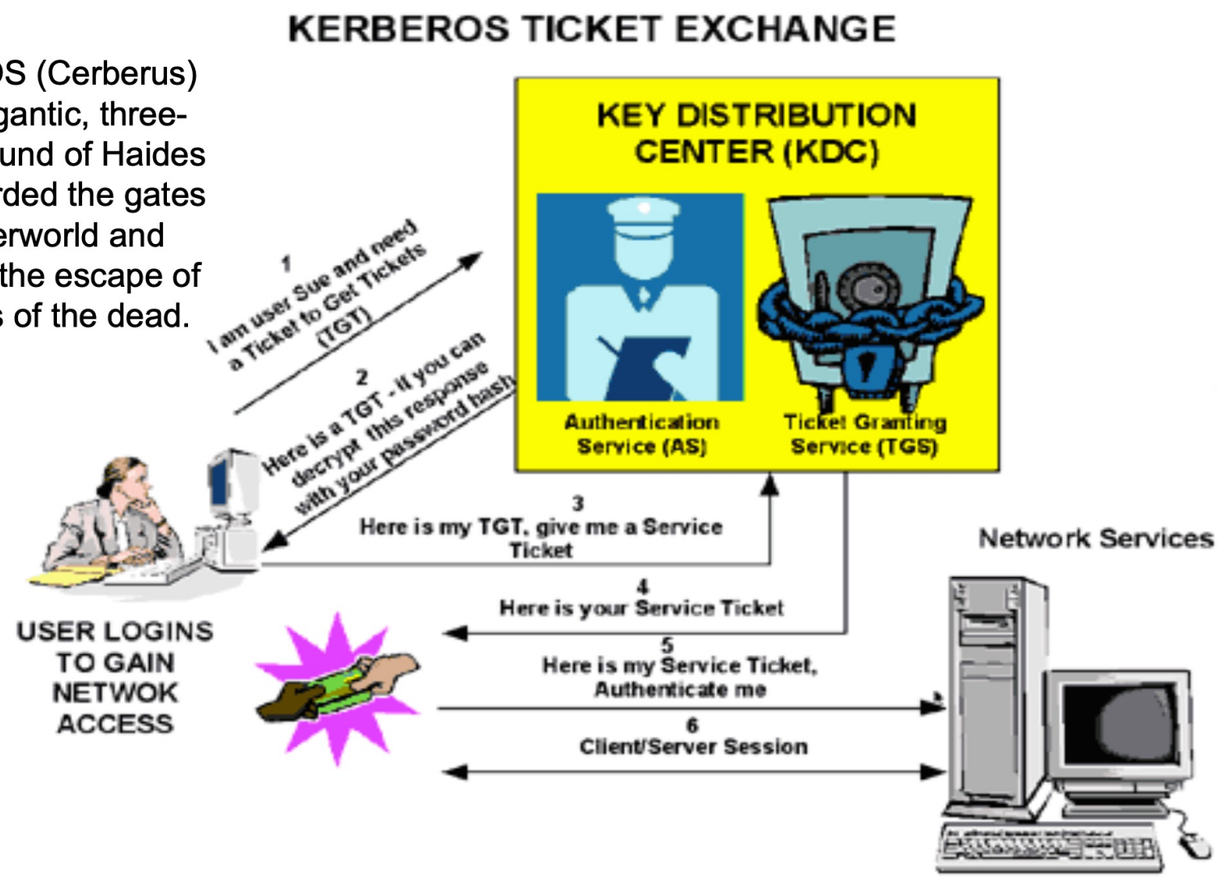
Active Directory (AD)



https://doubleoctopus.com/blog/passwordless-mfa/ldap-active-directory-and-federated-identities/

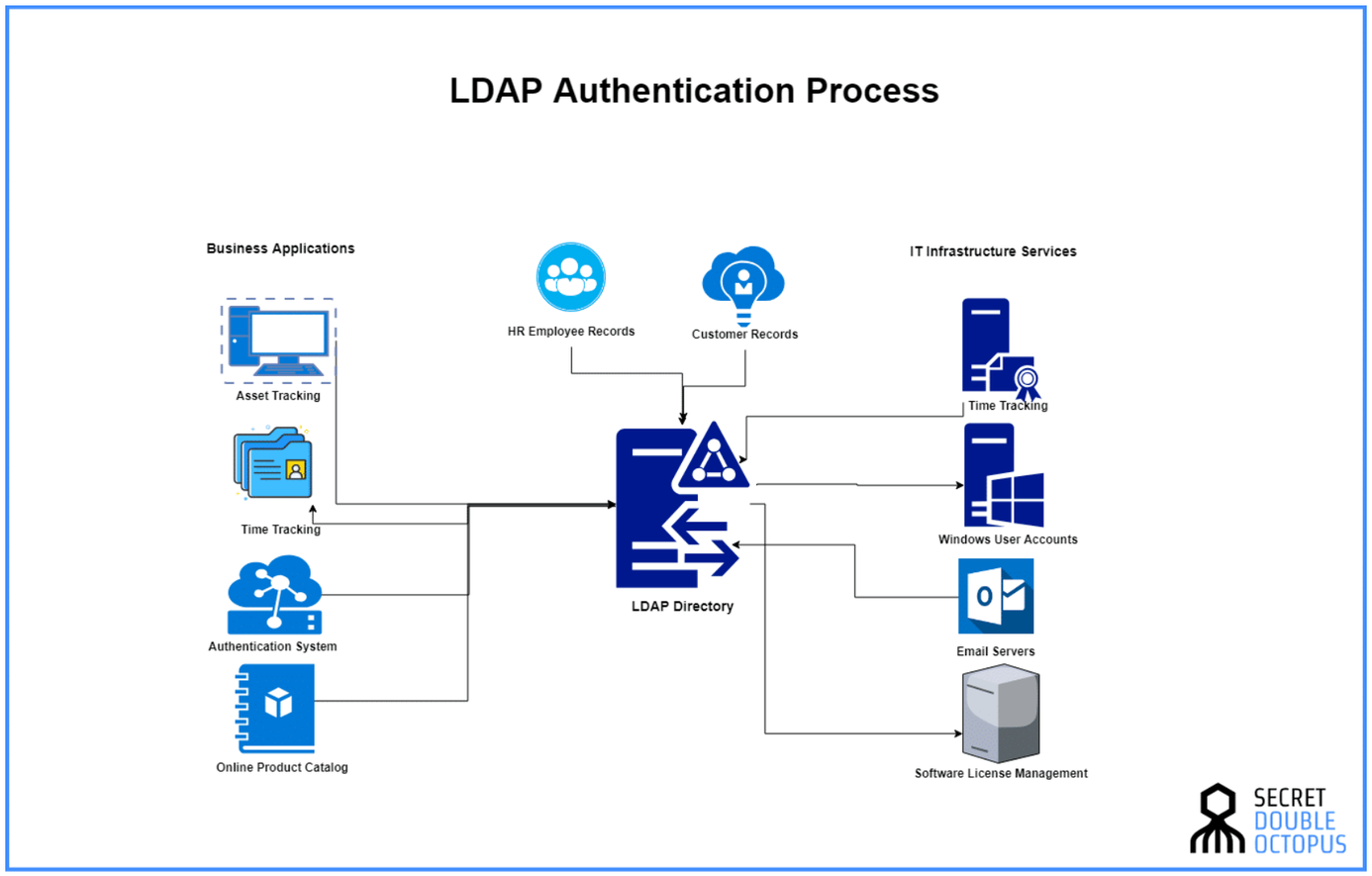
Kerberos

KERBEROS (Cerberus) was the gigantic, three-headed hound of Haides which guarded the gates of the underworld and prevented the escape of the shades of the dead.



https://msdn.microsoft.com/en-us/library/bb742516.aspx

Light weight access protocol (LDAP)



https://doubleoctopus.com/blog/passwordless-mfa/ldap-active-directory-and-federated-identities/

Light weight access protocol (LDAP)

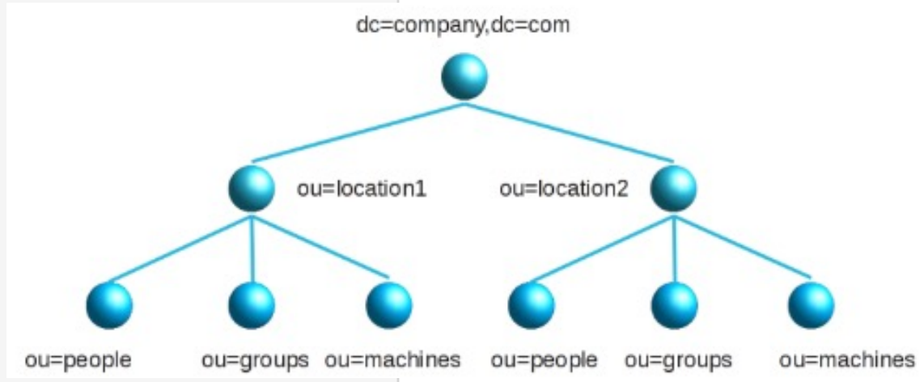
Comparing Authentication Services

- LDAP (Lightweight Directory Access Protocol)
  - X.500 based
  - Uses specifically formatted strings
    LDAP://CN=Homer,CN=Users,DC=GetCertifiedGetAhead,DC=com
  - CN=Homer. CN is short for common name.
  - CN=Users. CN is sometimes referred to as container in this context.
  - DC=GetCertifiedGetAhead. DC is short for domain component.
  - DC=com. This is the second domain component in the domain name.
- Secure LDAP
  - Version 2 uses SSL
  - Version 3 uses TLS

Light weight access protocol (LDAP)

ตัวอย่าง entry ที่แสดงในรูปแบบ LDAP Data Interchange Format (LDIF)

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```



dn คือ Distinguished Name ของ entry นี้ ไม่ใช่ attribute “cn= John Doe” เป็น RDN (Relative Distinguished Name)

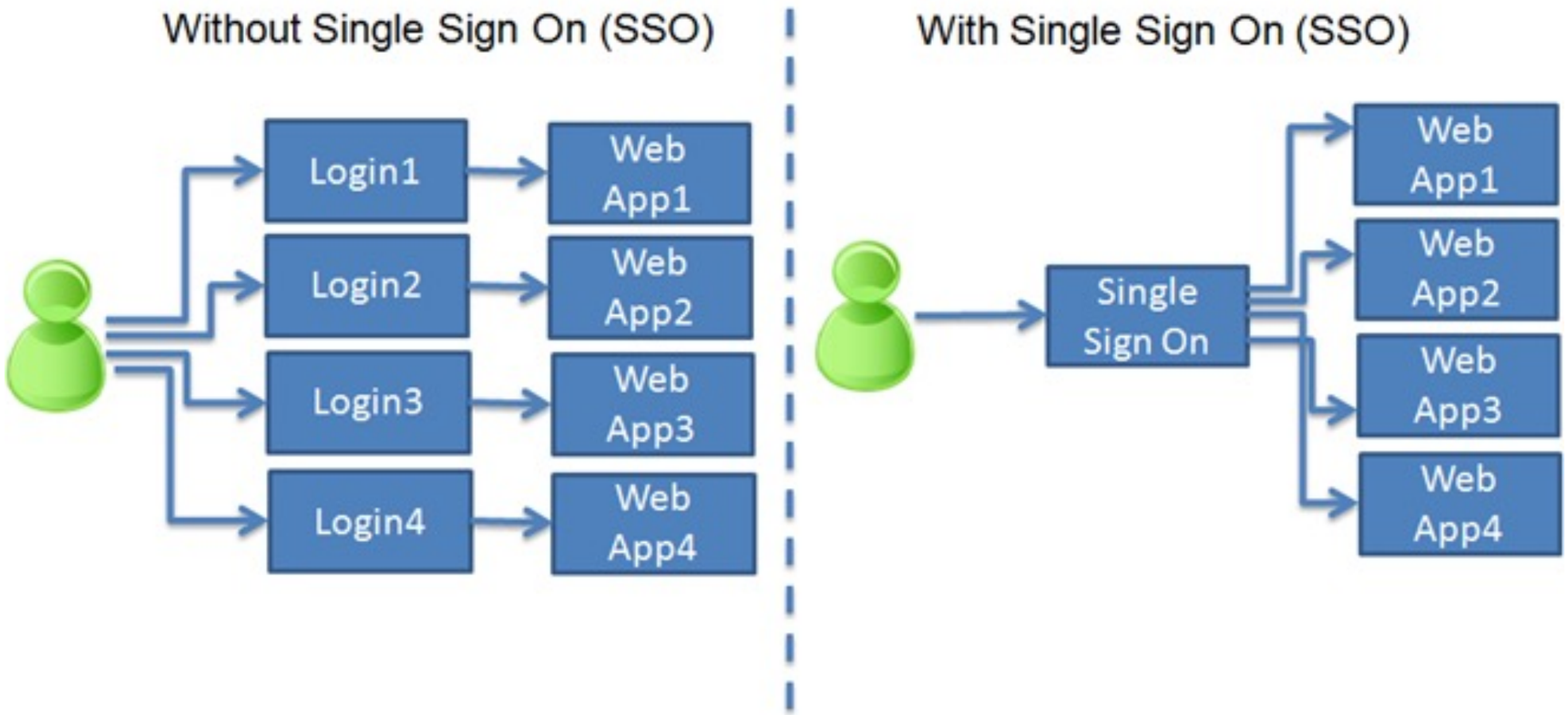
- “cn= John Doe” คือ RDN (Relative Distinguished Name)
- “dc= example, dc=c0m” ทั้งหมดคือ DN ของ parent entry

cn คือ Common Name

dc คือ Domain Component

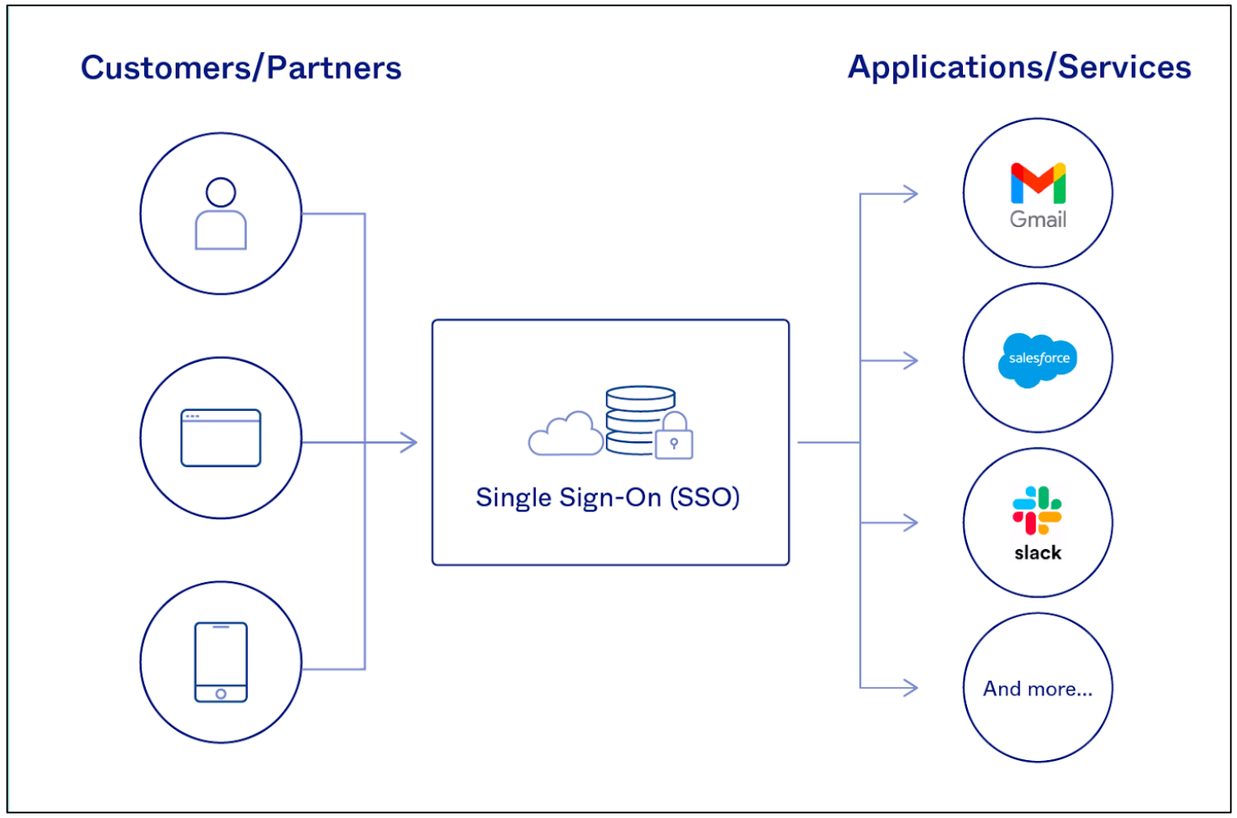
https://saixiii.com/what-is-ldap/

Single Sign-on (SSO)



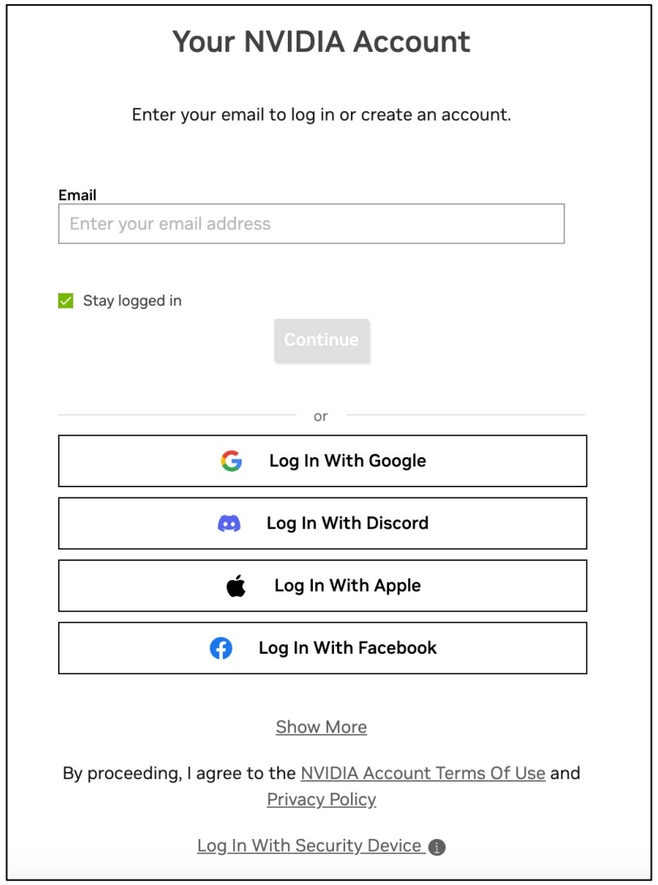
https://arunendapally.com/post/implementation-of-single-sign-on-(sso)-in-asp.net-mvc

Single Sign-on (SSO)

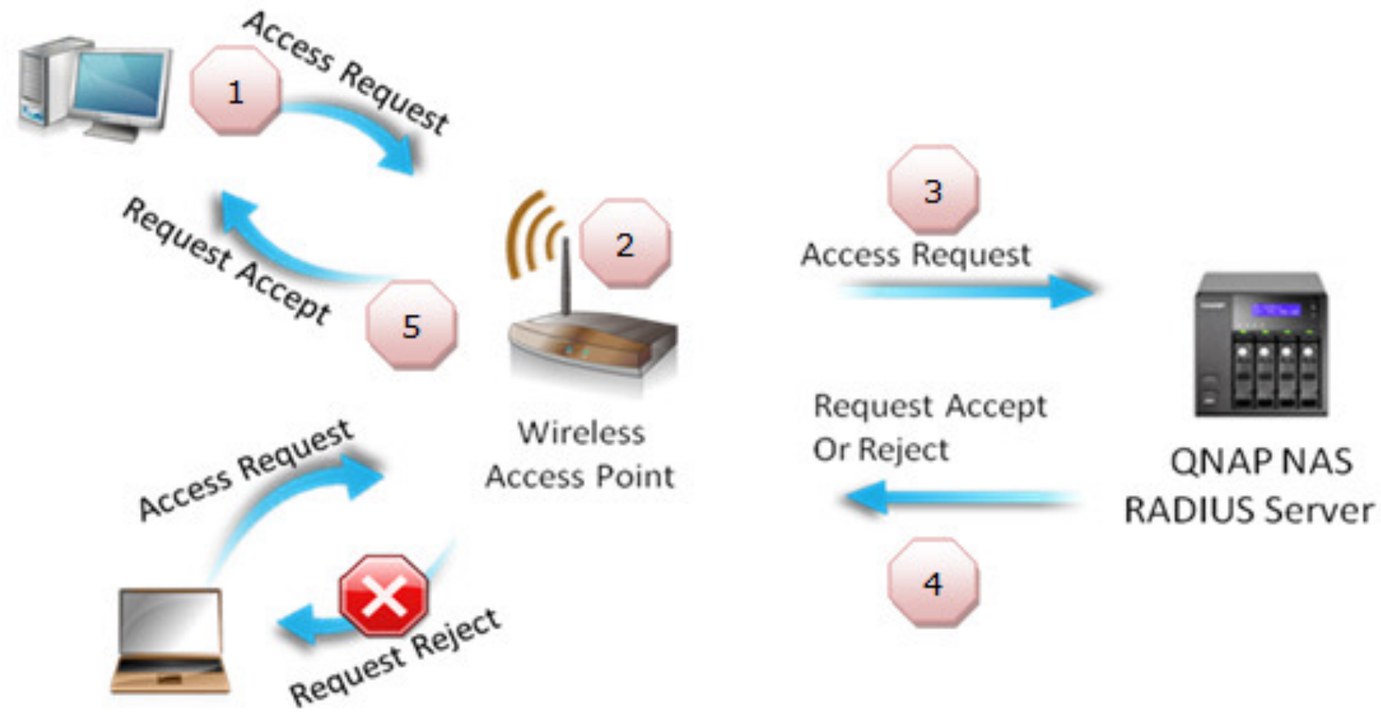


https://www.okta.com/blog/2021/02/single-sign-on-sso/

Single Sign-on (SSO)

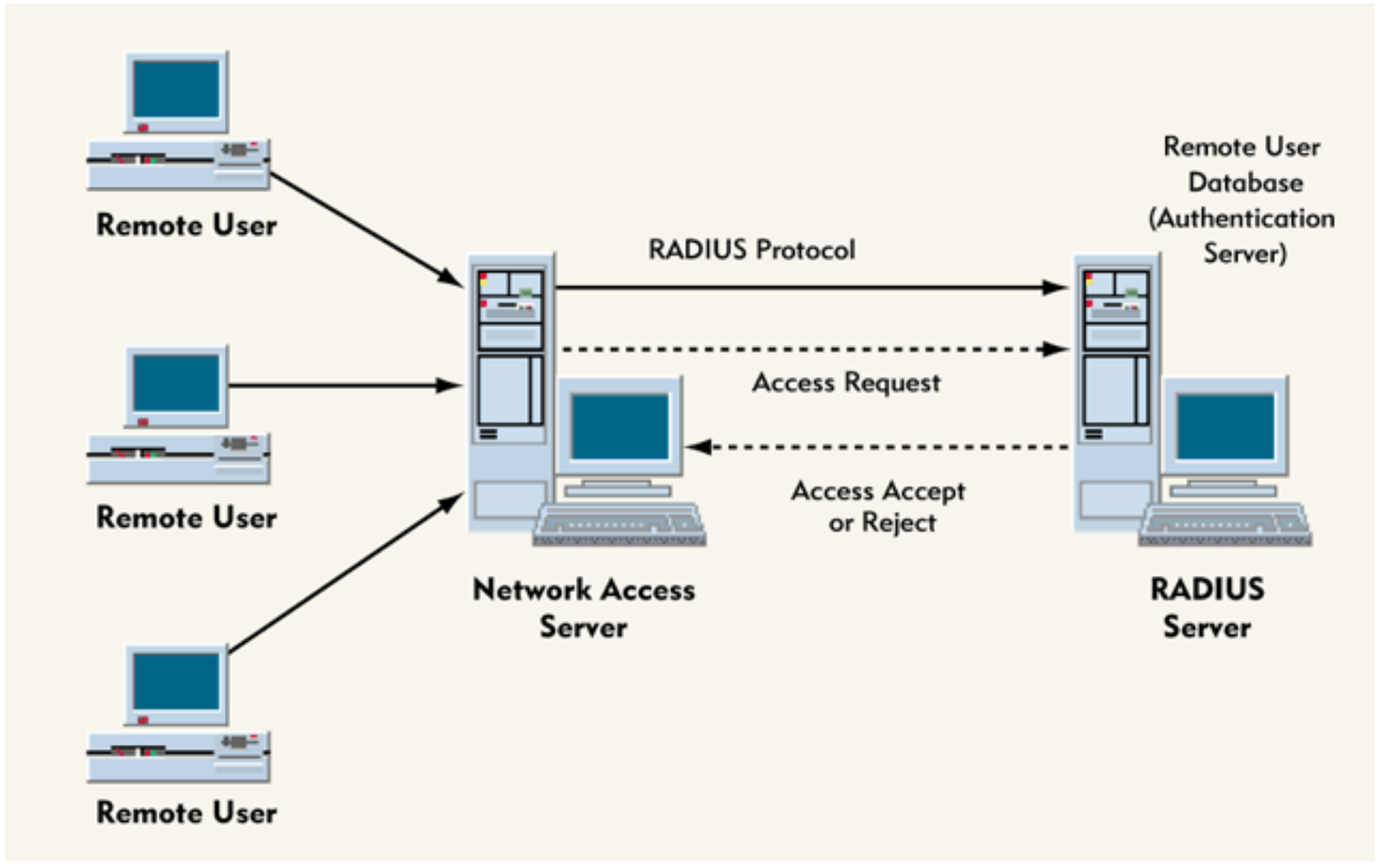


RADIUS (Remote Authentication Dial In User Service)



http://www.thaiall.com/blog/burin/5317

RADIUS (Remote Authentication Dial In User Service)



https://www.tech-faq.com/radius-server.html

RADIUS vs TACACS+

RADIUS was designed for subscriber AAA, and TACACS+ was designed for administrator AAA.

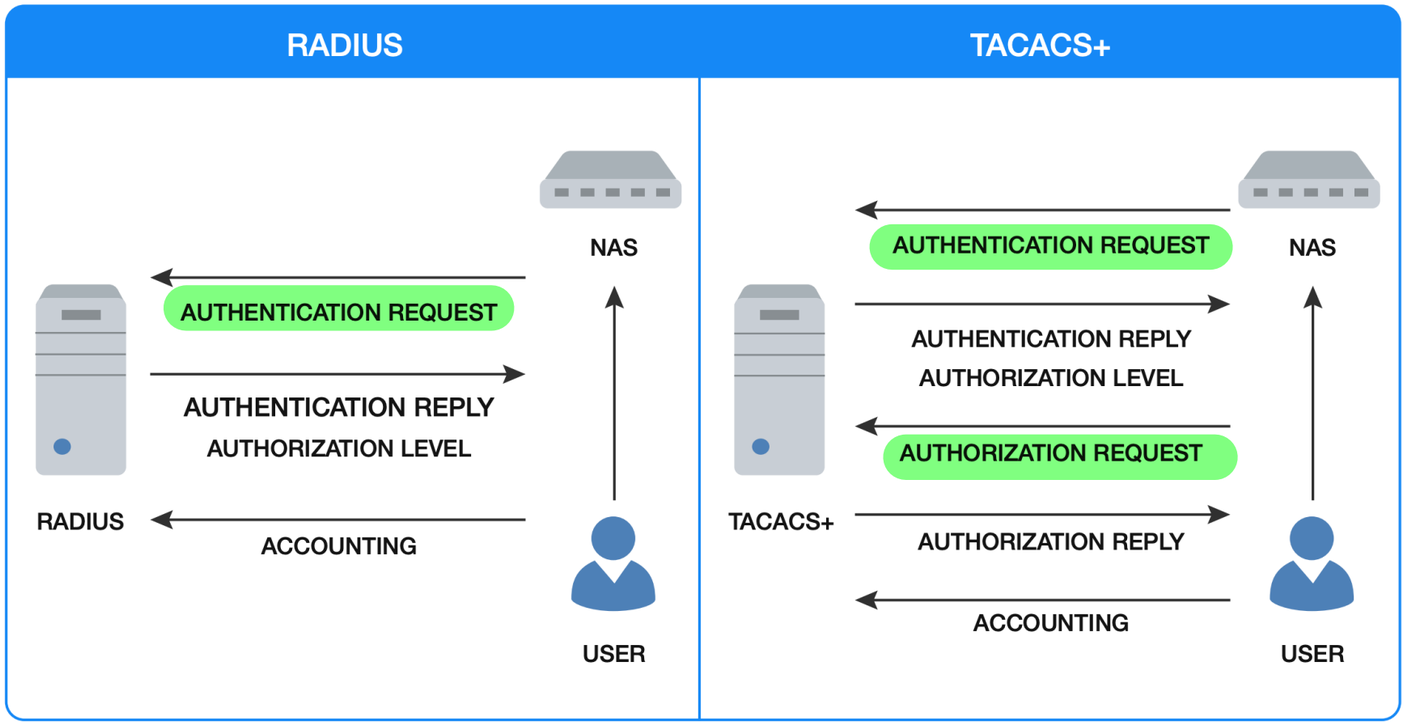


Figure 1: RADIUS vs. TACACS+

http://www.tacacs.net/docs/TACACS_Advantages.pdf

RADIUS vs TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Less secure – only runs a hash on the password.	More secure - Encrypts the whole packet including username, password, and attributes.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

Table 1: RADIUS vs. TACACS+

http://www.tacacs.net/docs/TACACS_Advantages.pdf


Q&A