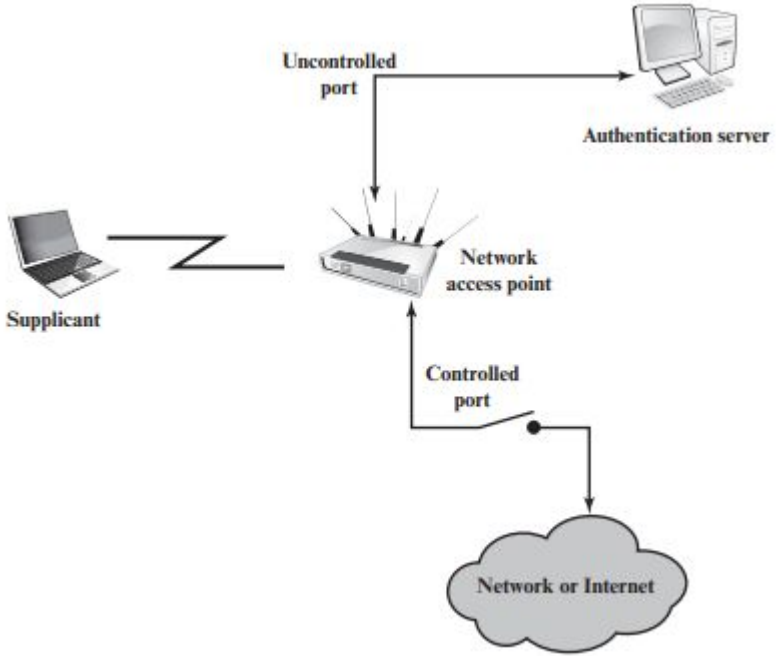
Unit 4 Network Security Applications



Network Security Applications

- Key Distribution
  - Kerberos
  - Public Key Infrastructure(PKI)
- Network Access Control
- Network Access Enforcement Methods
- Cloud Computing
  - Risks
  - Countermeasures
  - Data protection in cloud
  - Cloud Security As A Service
- AAA Concepts

Key Distribution

What is Key Distribution?

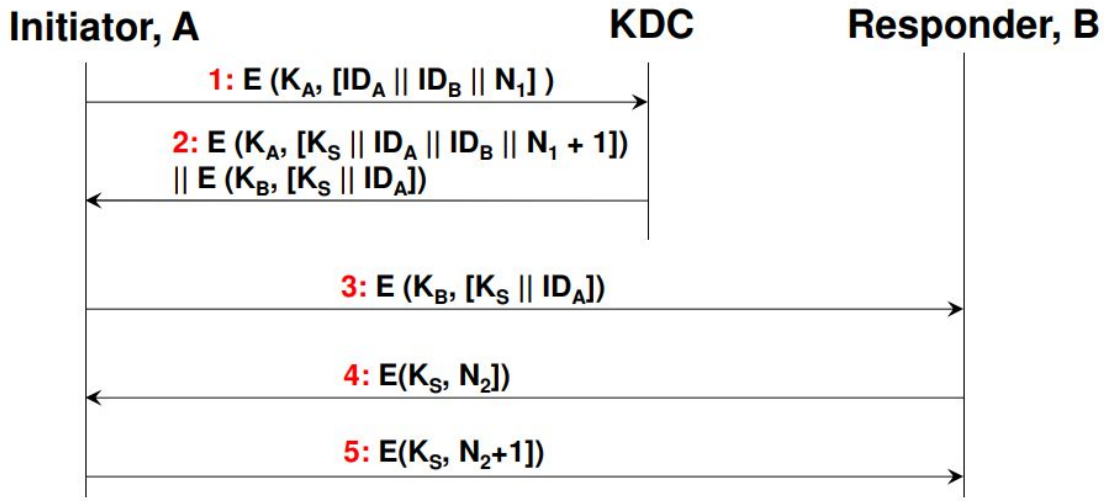
- Key Distribution is the process of securely delivering cryptographic keys to authorized parties. It is a fundamental aspect of cryptography, ensuring that only intended recipients can decrypt encrypted data.
- Both symmetric key schemes and public key schemes require both parties to acquire **valid keys**.
- In symmetric key schemes, the shared key should be securely distributed between the source and destination, while protecting it from others.
- Frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key.
- A new **session key** should be used for each new connection-oriented session.
- For a connectionless protocol, a new session key is used for a certain fixed period only or for a certain number of transactions.
- On many occasions systems have been broken, not because of a poor encryption algorithm, but because of poor key selection or management.
- Preferred Approach, especially for scalability - A third party, whom all parties trust, can be used as a trusted intermediary to mediate the establishment of secure communications between users.

Key Distribution Issues

- **Kerberos Protocol**
  - The Kerberos protocol is a network authentication system that offers safe communication over insecure networks by using symmetric key cryptography. It distributes session keys and performs user authentication using a reliable third party called the Key Distribution Centre (KDC).
- **Public key infrastructure**
  - The issue of identity authentication has been addressed with the proposal of public key infrastructures (PKIs). In their most common application, each user requests for a digital certificate from a "certificate authority" (CA) that is universally trusted. This certificate acts as an immutable means of identity verification for other users. Even in the event that the CA is hacked, the infrastructure is secure. However, a lot of PKIs offer a mechanism to revoke certificates in case such happens, making other users suspicious of them. Certificate revocation lists, against which any certificate can be compared, are often where revoked certificates are stored.
- **Hybrid Key Distribution Scheme**
  - This scheme retains the use of a key distribution center (KDC) that shares a secret master key with each user and distributes secret session keys encrypted with the master key. A public key scheme is used to distribute the master keys. The addition of a public-key layer provides a secure, efficient means of distributing master keys.
- **Distribution of Public Keys**
  - Using Public-Key Authority (centralized approach, needs real-time access to the authority) and Public-Key Certificates (no need for real-time access to the certificate authority)

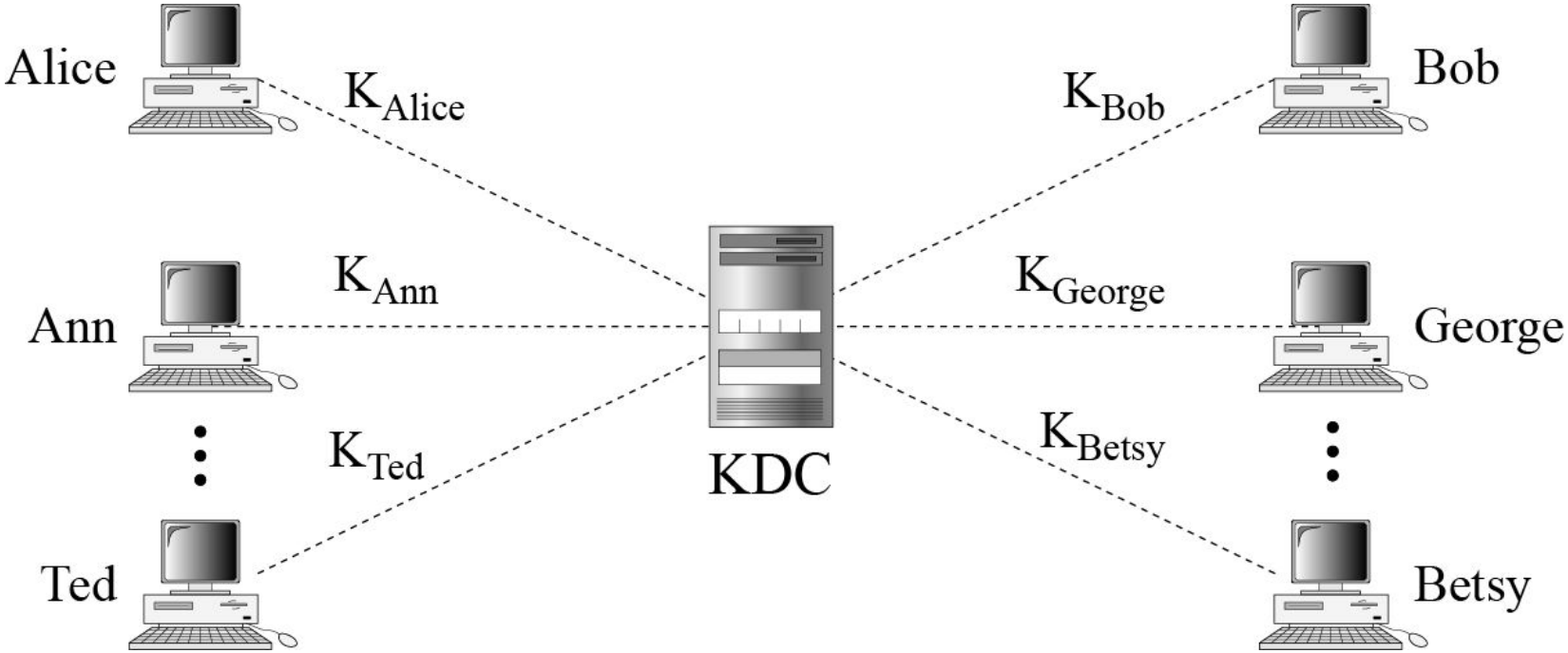
Key Distribution Center

- Key Distribution Center (KDC) shares a unique key with each party/ user.
- For very large networks, a hierarchy of KDCs can be established.
- For communication among entities within the same local domain, the local KDC is responsible for key distribution. If two entities in different domains desire a shared key, then the corresponding local KDCs can communicate through a (hierarchy of) global KDC(s)
- The use of a key distribution center imposes the requirement that the KDC be trusted and be protected from subversion. This requirement can be avoided if key distribution is fully decentralized (not easy though).



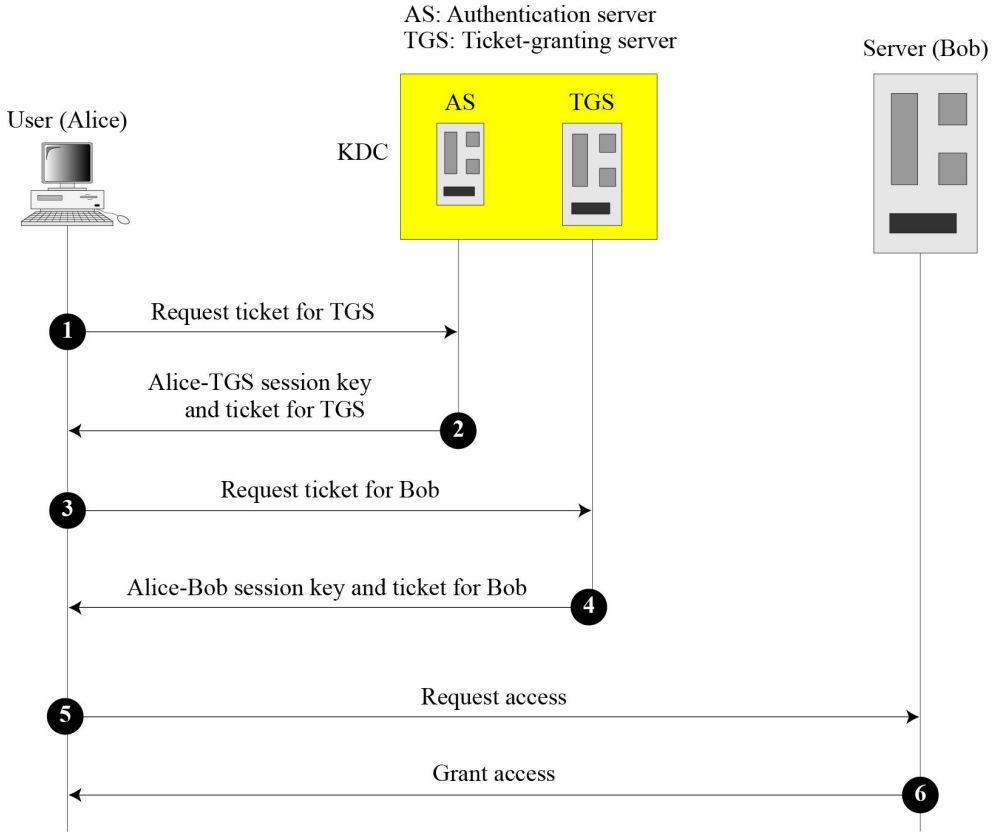
Note: Steps 1, 2 and 3 are related to "Key Distribution," while steps 3, 4 and 5 are related to providing "Authentication" for the initiator A at the responder B

Key Distribution Center



Kerberos

- Kerberos is an authentication protocol, and at the same time a KDC, that has become very popular. Several systems, including Windows 2000, use Kerberos. Originally designed at MIT, it has gone through several versions.



How Does Kerberos Work

Four Parties involved in the Kerberos Protocol :

1) Client

2) Authentication Server (AS)

The authentication server (AS) is the KDC in the Kerberos protocol.

3) Ticket-Granting Server (TGS)

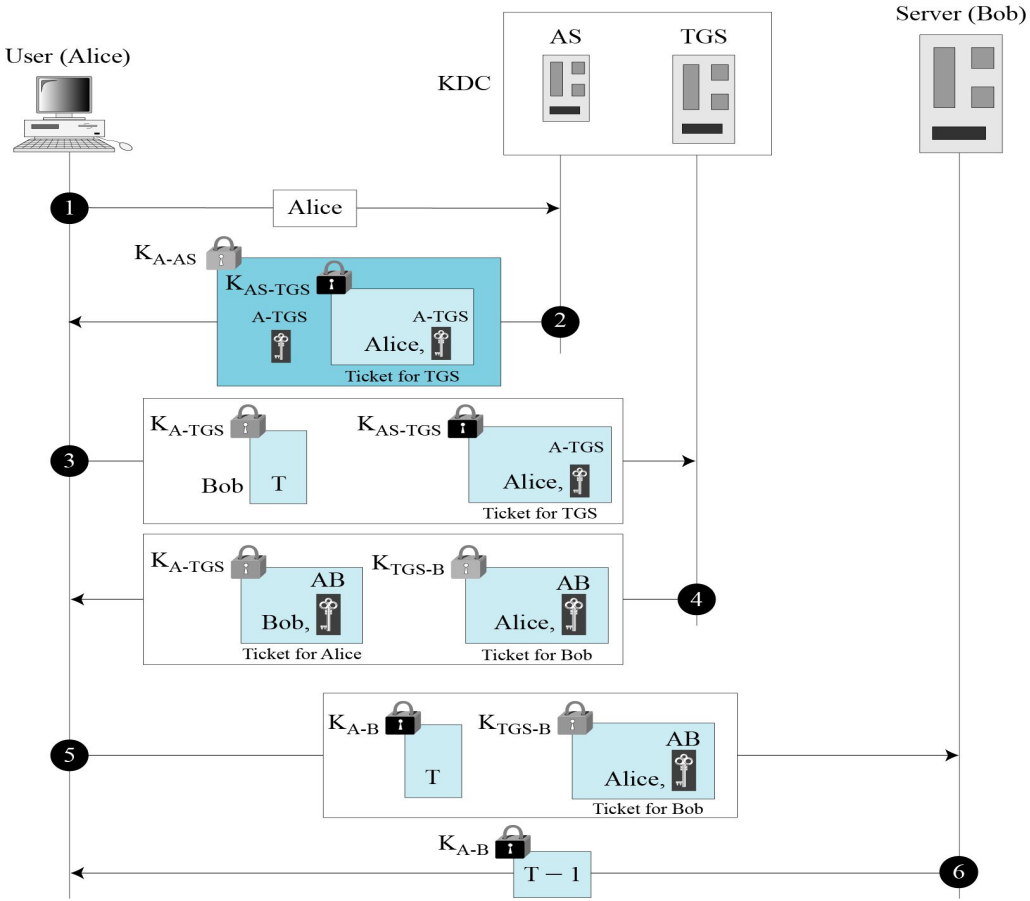
The ticket-granting server (TGS) issues a ticket for the real server (Bob).

4) Real Server

The real server (Bob) provides services for the user (Alice).

Kerberos

Note that if Alice needs to receive services from different servers, she need repeat only the last four steps.



K_{A-AS} Encrypted with Alice-AS key

K_{TGS-B} Encrypted with TGS-Bob key

K_{A-TGS} Encrypted with AS-TGS key

K_{AS-TGS} Encrypted with Alice-TGS session key

K_{A-B} Encrypted with Alice-Bob session key

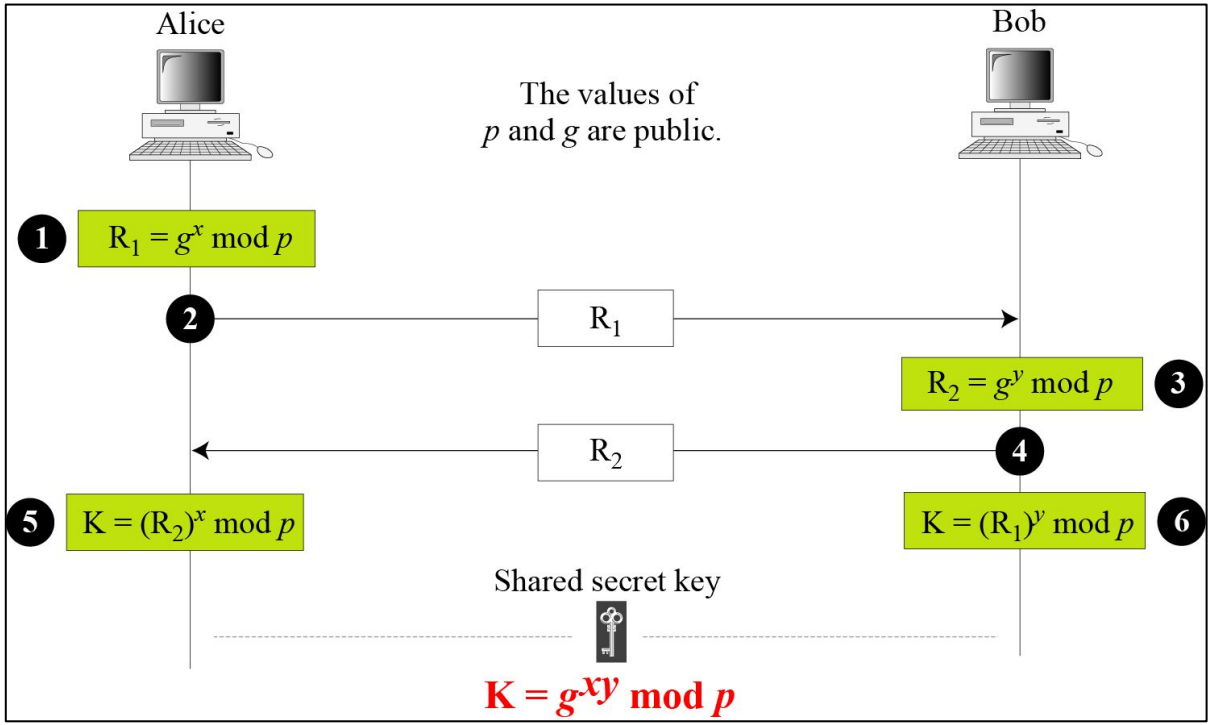
A-TGS
Alice-TGS session key

AB
Alice-Bob session key

KDC: Key-distribution center
AS: Authentication server
TGS: Ticket-granting server
T: Timestamp (nonce)

SYMMETRIC-KEY AGREEMENT

- Alice and Bob can create a session key between themselves without using a KDC. This method of session-key creation is referred to as the symmetric-key agreement.
-



Diffie-Hellman method

SYMMETRIC-KEY AGREEMENT

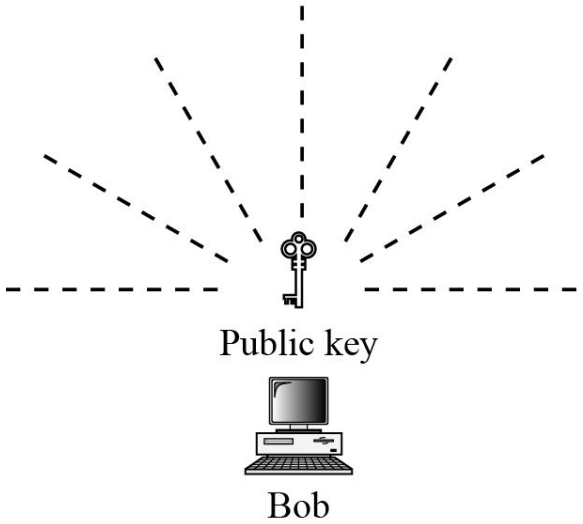
- Assume that g = 7 and p = 23. Solve using Diffie-Hellman method the steps are as follows:

- Alice chooses x = 3 and calculates R1 = 73 mod 23 = 21.
- Bob chooses y = 6 and calculates R2 = 76 mod 23 = 4.
- Alice sends the number 21 to Bob.
- Bob sends the number 4 to Alice.
- Alice calculates the symmetric key K = 43 mod 23 = 18.
- Bob calculates the symmetric key K = 216 mod 23 = 18.
- The value of K is the same for both Alice and Bob;
- g^{xy} mod p = 718 mod 35 = 18.

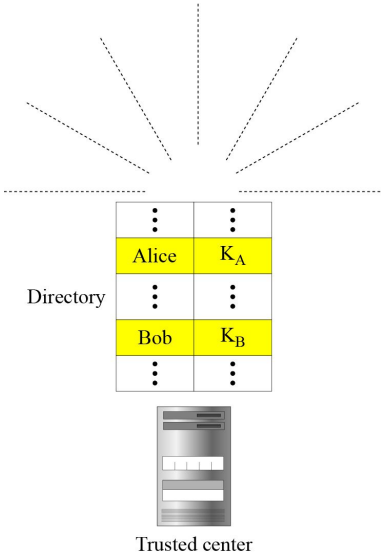
Public-Key Infrastructures (PKI)

- In asymmetric-key cryptography, people do not need to know a symmetric shared key; everyone shields a private key and advertises a public key.

1. Announcing a public key



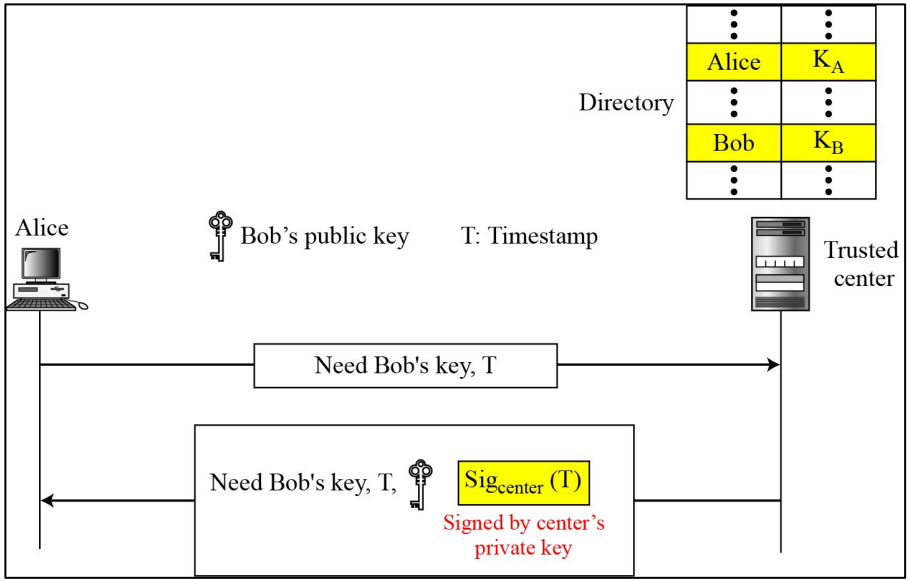
2. Trusted center



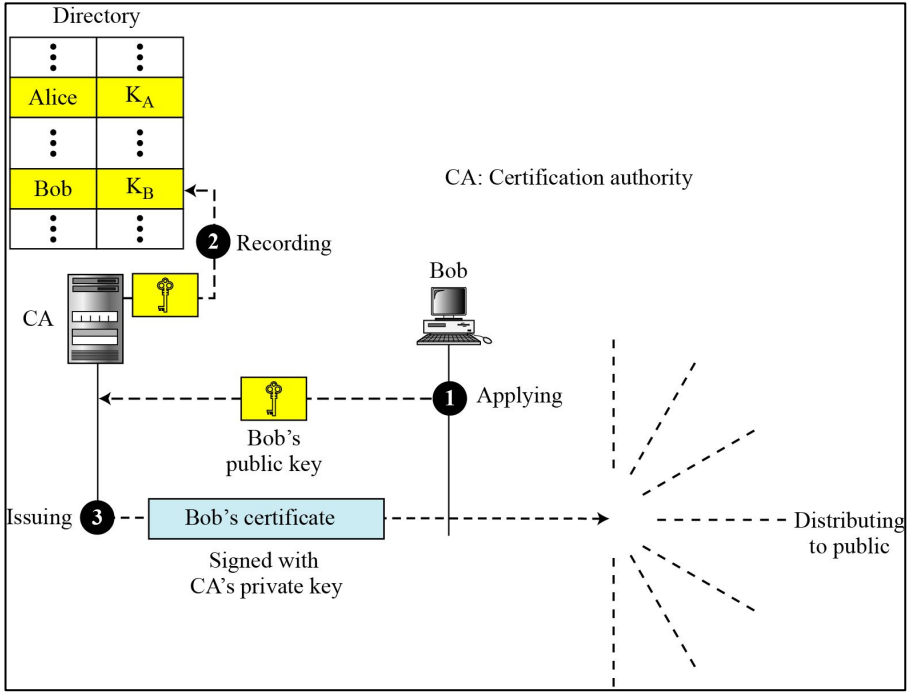
Public-Key Infrastructures (PKI)

- In asymmetric-key cryptography, people do not need to know a symmetric shared key; everyone shields a private key and advertises a public key.

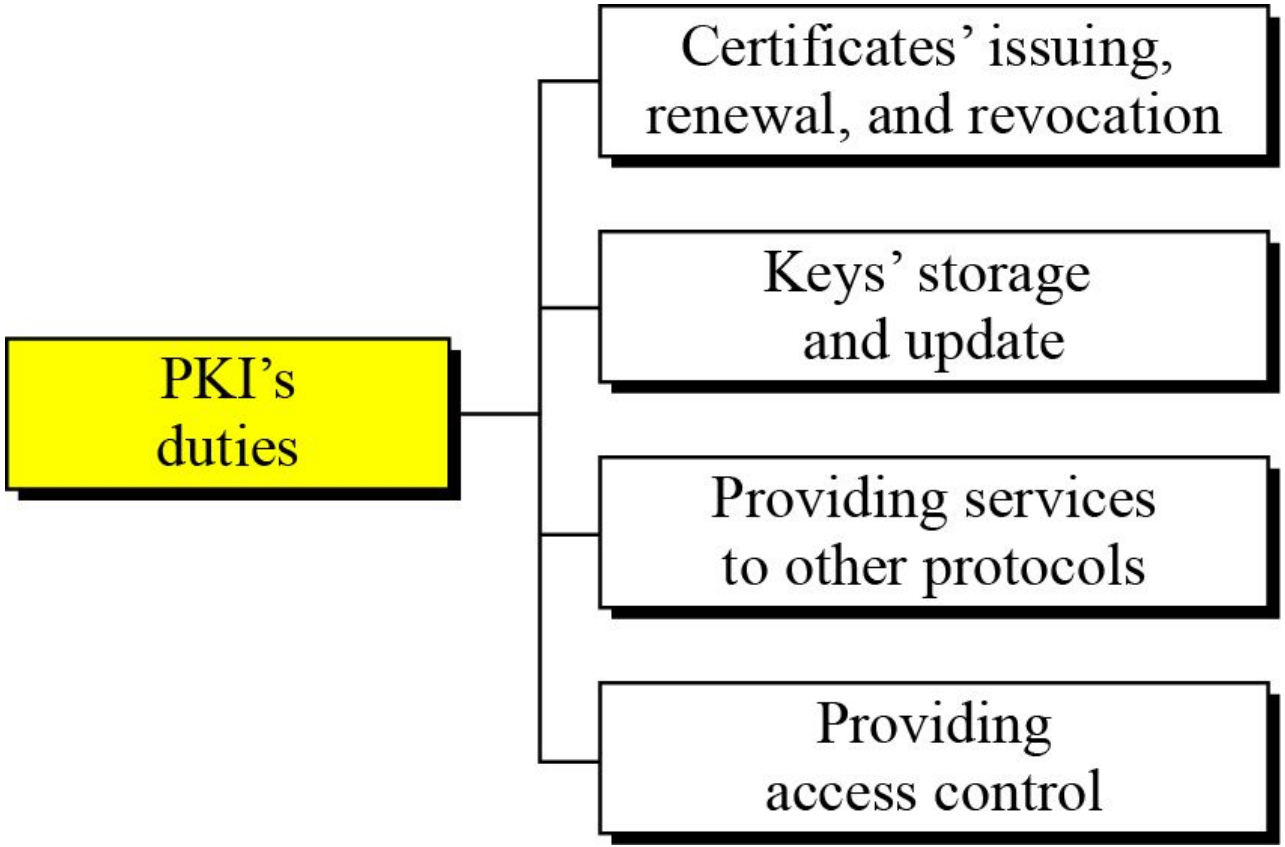
3. Controlled trusted center



4. Certification authority

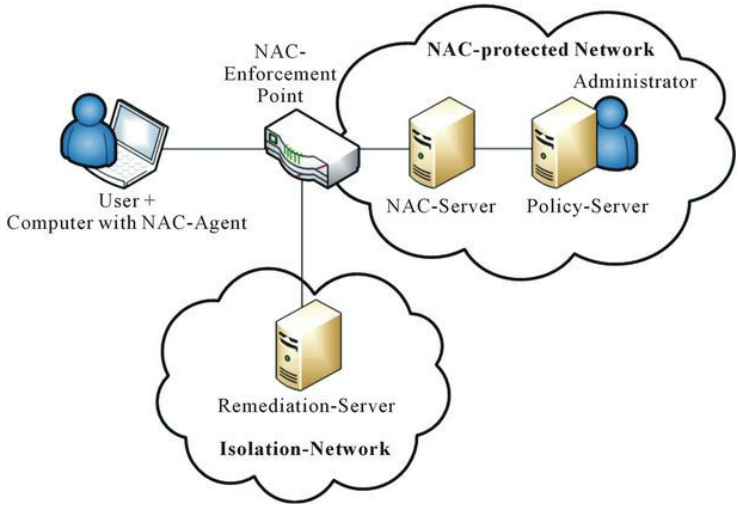


Some duties of a PKI



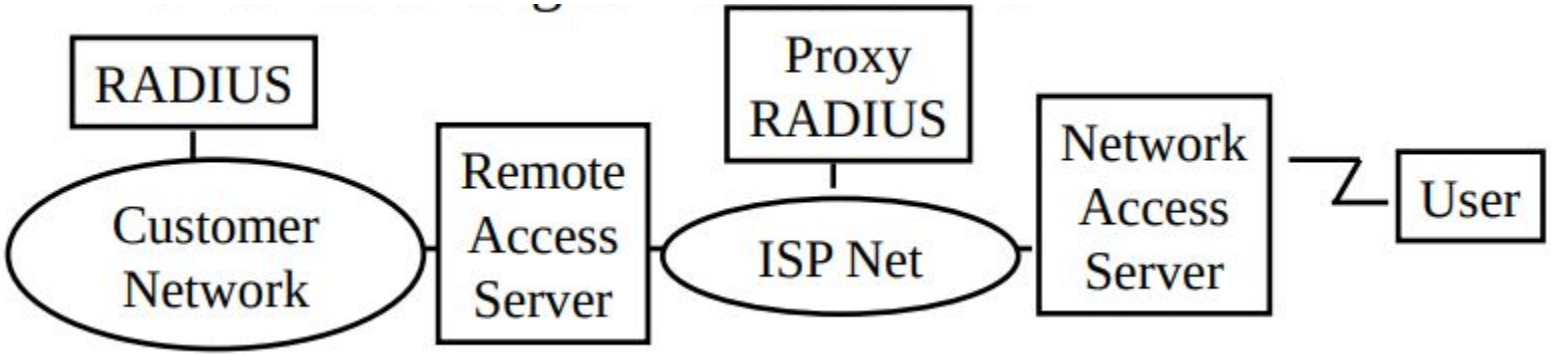
What is Network Access Control?

- Network Access Control is a security solution that uses a set of protocols to keep unauthorized users and devices out of a private network or give restricted access to the devices which are compliant with network security policies. It is also known as **Network Admission Control**.
- It handles network management and security that implements security policy, compliance, and management of access control to a network.
- NAC works on wired and wireless networks by identifying different devices that are connected to the network. For setting up an NAC network security solution, administrators will determine the protocols that will decide how devices and users are authorized for the right level of authorization.
- Access rules are generally based on the criterion such as device used, the location accessed from, the access rights of various individuals, as well as the specific data and resources being accessed.



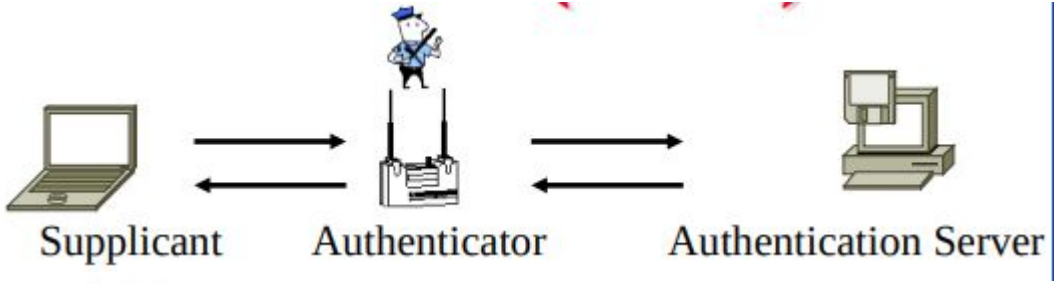
RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ AAA server
- Network Access servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application level retransmission required
- **TCP** takes to long to indicate failure

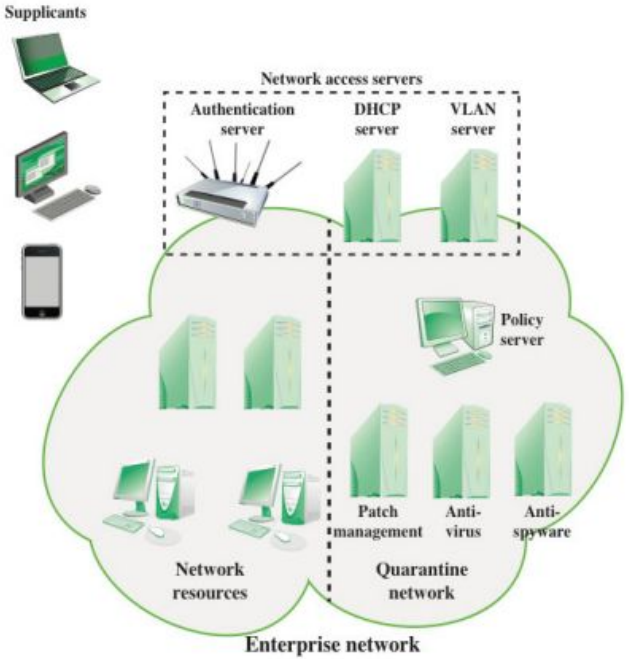


AAA Concepts of NAC

- Authentication- Is user legit?
- Authorization-What is he allowed to do?
- Accounting-Keep track of usage



- **Components:**
- Supplicant:User
- Authenticator:Network edge device
- Authentication Server: Remote Access Server (RAS) or Policy Server Backend policy and access control



Components of Network Access Control Scheme:

- Restricted Access
  - It restricts access to the network by user authentication and authorization control.
  - For example, the user can't access a protected network resource without permission to access it.
- Network Boundary Protection
  - It monitors and controls the connectivity of networks with external networks. It includes tools such as controlled interfaces, intrusion detection, and anti-virus tools. It is also called perimeter defense.
  - For example, the firewall can be used to prevent unauthorized access to network resources from outside of the network.

Types of Network Access Control

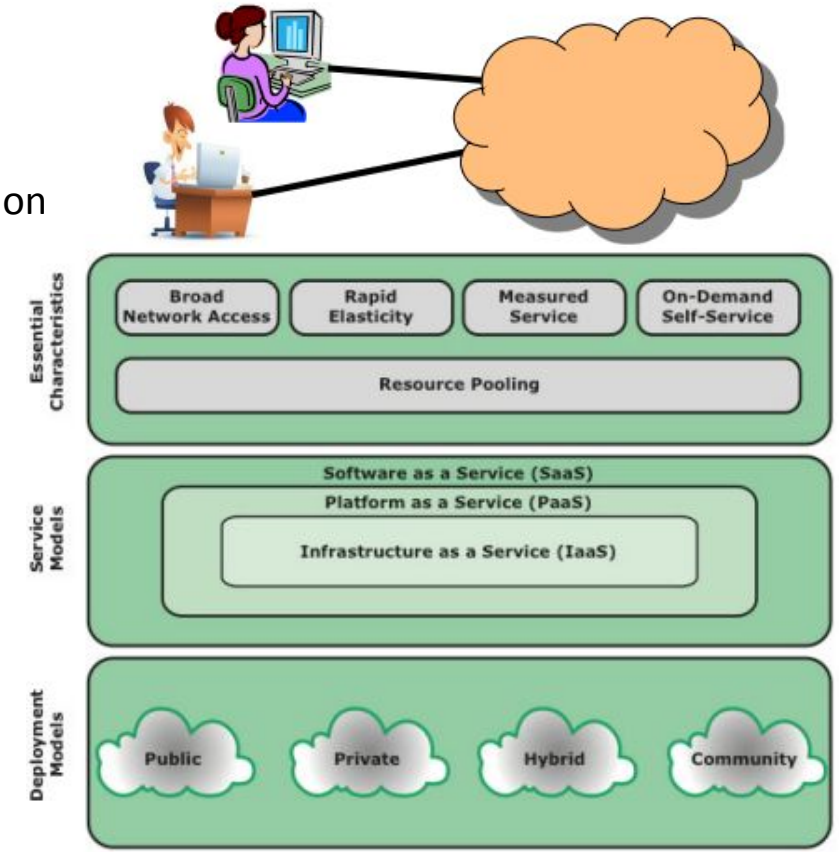
- Pre-admission
  - It happens before access to the network is granted on initialization of request by user or device to access the network.
  - It evaluates the access attempt and only allows the access if the user or device is compliant with organization security policies and authorized to access the network.
- Post-admission
  - It happens within the network when the user or device attempts to access the different parts of the network.
  - It restricts the lateral movement of the device within the network by asking for re-authentication for each request to access a different part of the network.

Network Access Enforcement Methods

- IEEE 802.1X used in Ethernet, WiFi
- Firewall
- DHCP Management
- VPN
- WLANs

Cloud Computing

- Using remote resources (Processor, Storage, Network, software, services)
- **Three Service Models**
  1. Infrastructure as a Service(IaaS):CPU
  2. Platform as a Service (PaaS):CPU+OS
  3. Software as a Service (SaaS): Application
- **Four Deployment models**
  1. Public
  2. Private
  3. Hybrid
  4. Community
- **Five Characteristics**
  1. Shared: Resource Pooling
  2. Ubiquitous: Broad network access
  3. Rapidly Provisioned: Rapid Elasticity
  4. Configurable: Measured Service
  5. On-demand Self-Service



Cloud Security Risks and Countermeasures

- **7 Risks and Countermeasures**
- 1. Abuse and Criminal Use:
  - Strict user authentication
  - Intrusion detection
  - Monitoring public blacklists for own network blocks
- 2. Malicious Insiders:
  - Comprehensive assessment of CSP
  - Human resource requirement as a part of the legal contract
  - Transparency into overall security management
  - Security breach notification process
- 3. Insecure Interfaces and API's:
  - Analyze security models of CSP interface
  - Ensure strong authentication and encryption
- 4. Shared Technology Issues:
  - Monitor environment for unauthorized changes
  - Strong authentication and access control for administrators
  - SLAs for patching vulnerability remediation
  - Conduct vulnerability scanning and configuration audits
- 5. Data Loss or Leakage:
  - Strong API access control Encrypt data in transit Analyze data protection at design and runtime Strong key generation, storage, management, and destruction
- 6. Account or Service Hijacking:
  - No sharing of credentials between users and services Strong two-factor authentication Intrusion detection Understand CSP security policies and SLAs
- 7. Unknown Risk Profile:
  - Disclosure of applicable logs and data
  - Partial/full disclosure of infrastructure details
  - Monitoring and alerting on necessary information

Data Protection Risks

- **Two database service models:**
- 1. Multi-instance model:
  - Each subscriber gets a unique DBMS on a VM Subscriber has complete control over role definition, user authorization, and other administrative tasks related to security
- 2. Multi-tenant model:
  - Subscriber shares a predefined environment with other tenants, typically by tagging data with a subscriber identifier CSP needs to establish and maintain a sound secure database environment

Cloud Security as a Service (SecaaS)

- **SecaaS:** Provisioning of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems
- Every danger is continuously monitored on a regular basis by SECaaS.
- Cybersecurity is handled by security analysts.
- Threat intelligence reacts right away to any malfunctions that compromise security.
- To minimize the impact on the system, sophisticated techniques identify the infection.
- The automations respond to spam and viruses automatically and eliminate them.
- **SecaaS Categories of Service :**

1. Identity and access management
2. Data loss prevention
3. Web security
4. Email security
5. Security assessments
6. Intrusion management
7. Security information and event management
8. Encryption

THANK YOU