

Overview of Authentication Systems



- ☐ Passwords
- ☐ Address based authentication
- ☐ Key Distribution Center (KDC)
- ☐ Certification Authorities (CAs)
- ☐ Multiple Trust Domains
- ☐ Session Keys
- ☐ Delegation

Passwords

- ❑ Do not store passwords in clear. Store hashes.
 - ⇒ Subject to offline attack <https://crackstation.net>
<https://emn178.github.io/online-tools/sha256.html>
- ❑ Encrypt the hash storage.
 - ⇒ Where do you keep the master key?
- ❑ Do not transmit passwords in clear.
- ❑ Use password as a key to encrypt a challenge.
 - ⇒ Cryptographic Authentication

Address based authentication

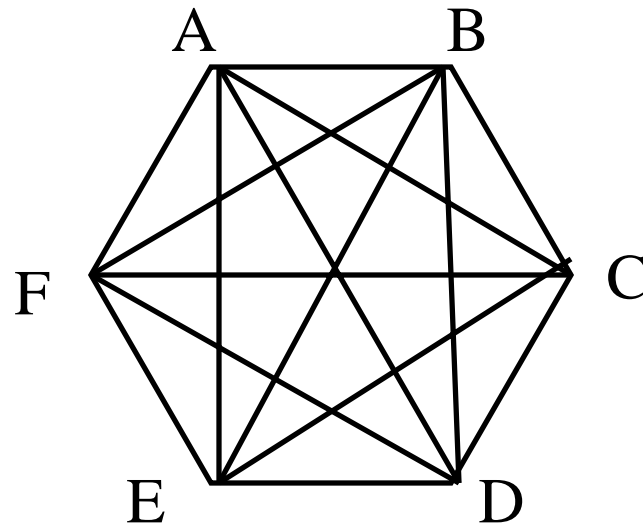
- ❑ /etc/hosts.equiv file in UNIX.
- ❑ John Smith can do on B whatever he is allowed to do on A.
⇒ Users need to have the same name on all machines.
- ❑ Per user .rhosts files.
Lists <address, remote account name>
that can access this account.
- ❑ Issue: Attacker can gain access to all machines
- ❑ Attacker can change IP addresses of machines and can access remote resources of all users on that machine.
- ❑ Attacker can use source route <A, X, D> to send messages to D (from A).

The /etc/hosts.equiv file contains a list of trusted hosts for a remote system, one per line. If a user attempts to log in remotely (using rlogin) from one of the hosts listed in this file, and if the remote system can access the user's password entry, the remote system allows the user to log in without a password.

Machine vs. Person Authentication

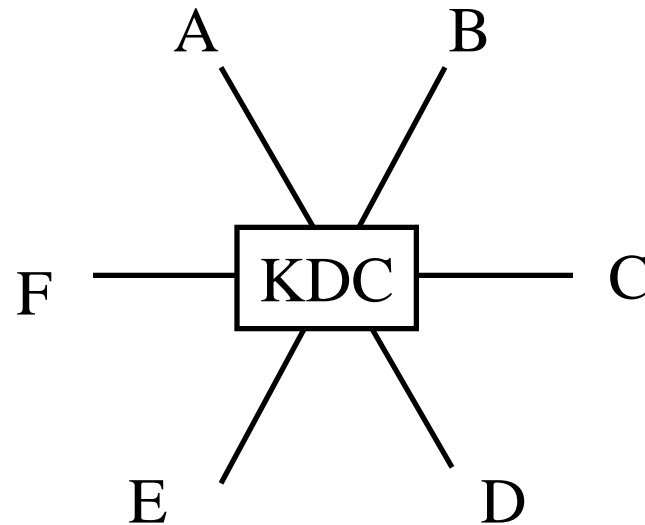
- ❑ Machines can store long secret keys.
- ❑ Person's password can be used to decrypt a long secret key or private key.

Secret Keys for an N-System Network



- ❑ n system need $n(n-1)/2$ pairs of secret keys
- ❑ Each system remembers $n-1$ keys.
- ❑ If a new system comes in n new key are generated.
- ❑ If a system leaves, $n-1$ keys are removed.

Key Distribution Center (KDC)



- ❑ Each node is configured with KDC's key
- ❑ KDC has all the keys.
- ❑ KDC sends a key encrypted with A's key and B's key to A.
- ❑ Issues:
 - If KDC is compromised, all systems are compromised.
 - KDC is single point of failure or performance bottleneck.
 - KDC has to be on-line all the time.

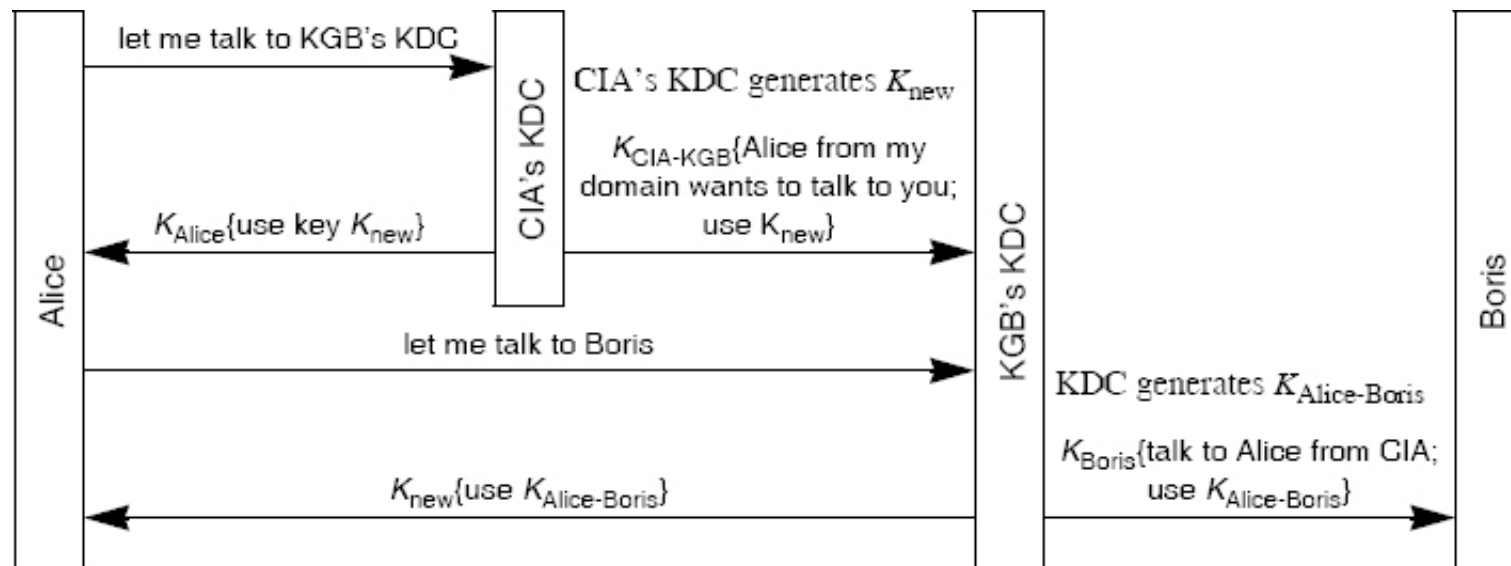
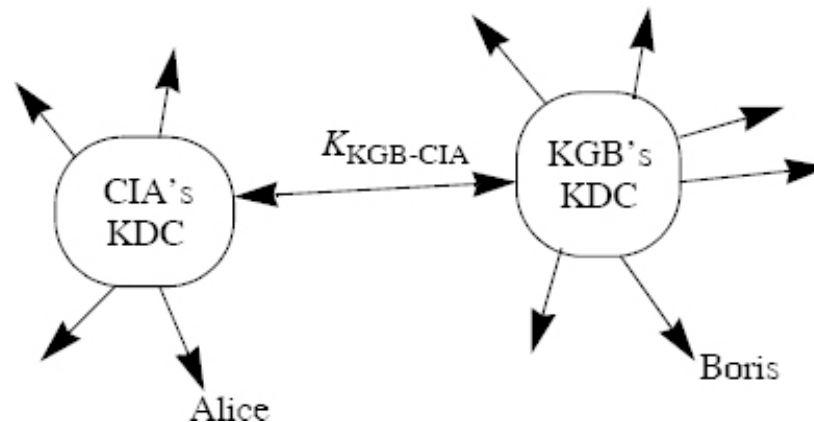
Certification Authorities (CAs)

- ❑ Unsigned public keys can be tampered.
- ❑ Public Keys are signed by CAs \Rightarrow Certificates.
- ❑ Each system is configured with CA's public key.
- ❑ CA's don't have to be on-line.
- ❑ A compromised CA cannot decrypt conversations.

Certificate Revocations Lists (CRL)

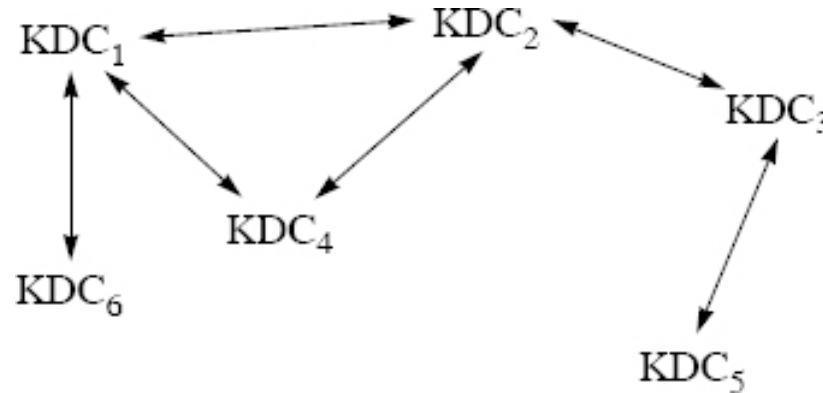
- ❑ The lists are published regularly.
- ❑ Certificates are checked in a recent CRL.
- ❑ Certificate contains user's name, public key, expiration time, a serial number, and CA's signature on the content.

KDCs in Multiple Trust Domains

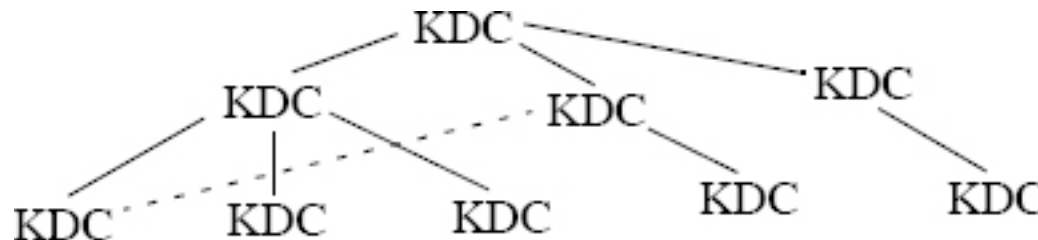


KDCs in Multiple Trust Domains (Cont)

- Some pairs of KDCs have a secret key



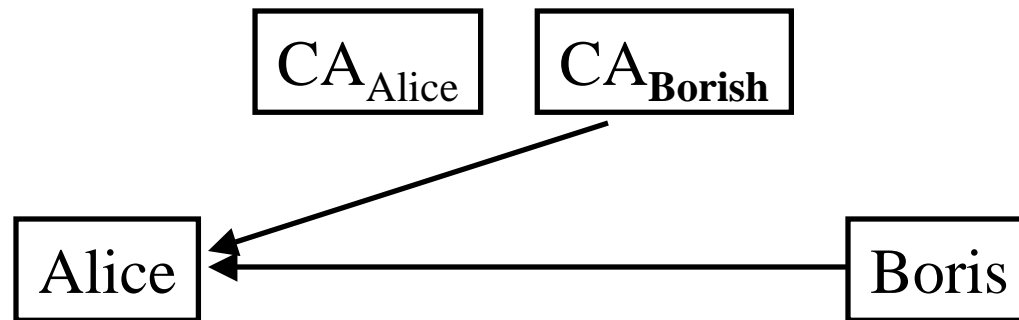
- Issue: Every pair of KDC needs a shared key
⇒ KDC hierarchy



- Issue: Every pair of KDC needs a shared key
⇒ KDC hierarchy

CA's in Multiple Domains

- ❑ Each CA has a certificate from the other.
- ❑ Alice with Boris's certificate and Boris's CA's certificate issued by Alice's CA can authenticate Boris



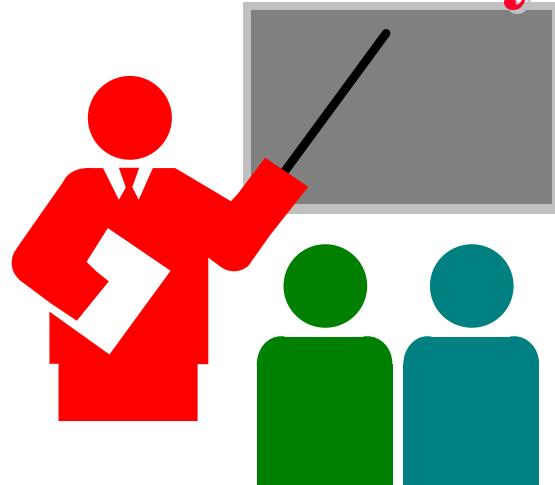
Session Keys

- ❑ Public key is used to exchange a secret key.
- ❑ Each session should start with a new secret key.

Delegation

- ❑ Authentication forwarding
- ❑ A signed message with time limit and details of privileges

Summary



- ❑ Passwords should not be stored or transmitted in clear
⇒ Use to generate keys
- ❑ Address based authentication is not safe.
- ❑ Key Distribution Center (KDC): Single point of failure
- ❑ Certification Authorities (CAs) sign public keys.
- ❑ Multiple Trust Domains: Hierarchy of KDCs or CAs

Homework 9

- ❑ Read Chapter 9 of the textbook
- ❑ Submit answers to Exercise 9.3
- ❑ Extend the scenario in Section 9.7.4.1 Multiple KDC Domains to a chain of three KDCs. In other words assume that Alice wants to talk to Boris through a chain of three KDCs (Alice's KDC, A KDC that has shared keys with both Alice's KDC and Boris's KDC and finally, Boris's KDC). Give the sequence of events necessary to establish communication.