PKI (continued) Kerberos

Tom Longstaff

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 1521

The CERT Coordination Center is sponsored by the Advanced Research Projects Agency (ARPA). The Software Engineering Institute is sponsored by the U.S. Department of Defense.

PKI

Mechanism to distribute and trust public keys

Two types in common use: Hierarchical and the Web of Trust

Modified Hierarchical combines distinct Hierarchical PKIs with cross-realm authentication

Common use of PKI refers to Hierarchical, but also covers Web of Trust and Modified Hierarchical

Carnegie Mellon University
CERT Coordination Center

Key and signature revocation

What if a private key is compromised in the web of trust?

First of all, need a mechanism to distribute this information

Secondly, need to invalidate all signatures under this key

May be able to limit the extent of revocation based on date of the revocation certificate

3

Carnegie Mellon University
CERT Coordination Center

Building up a hierarchy of keys

In a hierarchical PKI, you need a root certificate who's security is above reproach

- **Why?**

ROOTPublicKey,(ROOTPublicKey[MD5])ROOTPrivateKey

CAPublicKey,(CAPublicKey[MD5])CAPrivateKey,(CAPublicKey[MD5])ROOTPrivateKey

UserPublicKey,(UserPublicKey[MD5])UserPrivateKey,(UserPublicKey[MD5])CAPrivateKey

4

Carnegie Mellon University
CERT Coordination Center

Distribution of Hierarchical Public Keys

The root public key must be widely distributed in a variety of paths to everyone in the hierarchy

- **Why multiple paths?**
- **What is the primary vulnerability here?**

If the root key is secure, the system can be consistent

Root key is used to sign all revocation certificates for Cas

Root servers *do not need to sign keys lower in the hierarchy*

- **Why not?**

5

Carnegie Mellon University
CERT Coordination Center

One versus Multiple Hierarchies

What are the problems with a single root server for all PKI systems?

If you want to trust users across hierarchies, you need *cross-realm certification*

Combines Web-of-Trust with Hierarchical PKI

Means that some root or CA public key is signed by one in the other hierarchy

6

Carnegie Mellon University
CERT Coordination Center

Problems in cross-realm certification

- Naming
- Different policies for inclusion in the hierarchy
- Different uses of keys
- Compatibly of algorithms and key records

7

Carnegie Mellon University
CERT Coordination Center

What does this have to do with operating system security architectures?

- Application-level architecture
- Trust of users within the operating system
- Basic tool for linking users with processes
- Kerberos and related systems make use of these concepts to implement OS trust

8

Kerberos

Based on symmetric key encryption

Solves the problems:

- **Untrusted client machines need to authenticate users**
- **Need data protection for applications**
- **Provides authentication and authorization for services**

Once the infrastructure is in place, applications must be instrumented to use kerberos

Examples of Kerberoized applications:

- **Telnet**
- **BSD Rtools**
- **Email**
- **NFS, AFS, etc.**

The Key Distribution Center (KDC)

Must be a physically secure host in the system

Stores a shared key with each principal (each user and service that uses kerberos)

The main job of the KDC is to create session keys and distribute them based on the shared secret key of the user

Also known as an authentication server in the Kerberos documentation

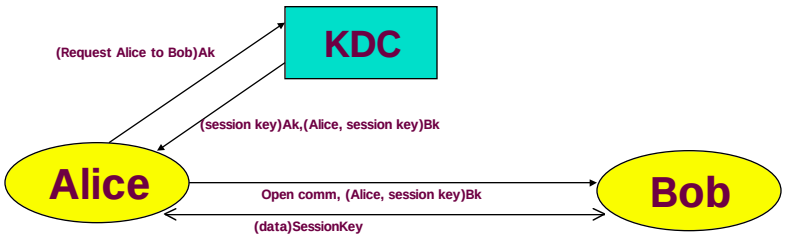
KDC Example

Alice requests a session with Bob

KDC encrypts a session key with Alice's key and sends to Alice

Also sends the session key and some info on Alice encrypted with Bob's key

Now Alice can talk to Bob, Bob can decrypt the session key and open a comm with Alice



TicketGrantingServer (TGS)

Really does the same job as the KDC, but in theory provides another layer of security

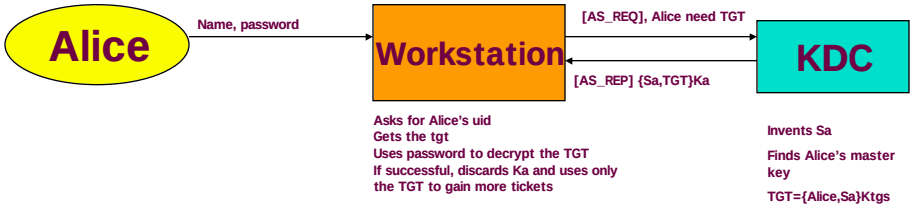
Alice gets a ticket (session key) to talk to a TGS from the KDC

Uses this ticket to request tickets to talk to Bob

In practice, the KDC and TGS are the same system as the TGS has to have the same database of shared keys to create tickets for Bob

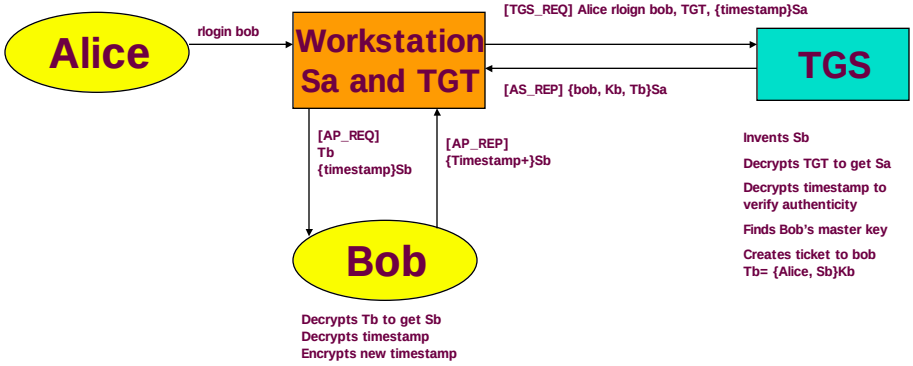
Logging in to a Network

You need to get a session key and a ticket-granting-ticket



Using the TGT and Sa

After logging into the network, Alice asks to talk to Bob (e.g., rlogin to Bob the workstation)



Kerberos V5

In principle, the same as V4 but with a major overhaul of the implementation and addition of features.

Allows for delegation of rights,

renewable and postdated tickets,

other cryptographic algorithms (V4 used only DES and Jueneman),

allowed for a hierarchy of realms