Lecture 7 - 09/27/2019

Key Management

Symmetric : kerberos
Asymmetric : Public key infrastructure (PKI)

Certification Authority (CA)

A Certificate has 3 things.

- A name for a person
- A public key the that person
- A signature for those two items.

Assumptions

- Alice and Bob knows public key of CA
    - The public key of a CA is the trust anchor
- Certificates must be stored somewhere that is publicly accessible.
- Names in certs correspond to actual entities that wish to communicate
- Names must be unique and valid
- Certs have not been revoked.
- Private keys have not been compromised

Online KDC

- Holds all keys in system
- If compromised, the attacker can read all traffic on a network

Offline CA

- Holds its own private key
- Requires a physically secured room

Access Control

Policy

- We need a policy that is written by humans and is readable by software
- **Entrust** attempted to solve the issues of standardizing access control policies

XACML

- XML for access control
- W3 standardized
- Oasis