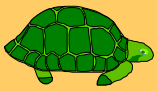
Lecture 12
November 5, 2001

- Key Distribution
- Certification
- Authentication & Identification

The "rabbit-in-the-middle-attack"

- Eve is an active adversary!
- Alice thinks she is talking to Bob

Choose random a



Compute $K_{AB} = (B)^a \bmod p$

$A = g^a \bmod p$

$B = g^e \bmod p$

Choose random e, Compute $K_{EA} = (A)^e \bmod p$

Secure communication. with K_{AE}

Authenticated Key Exchange (STS)

Choose random a

Compute

$A = g^a \bmod p$

$A = g^a \bmod p$

Choose random b, compute

$K_{ba} = (A)^b \bmod p$

$B = g^b \bmod p$

$SIG_{bob} = \{B, A\}^{Bob}$

$CERT_{bob}, B, SIG_{bob}$

Compute

$K_{ab} = (B)^a \bmod p$

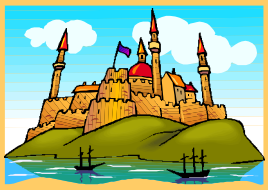
$SIG_{alice} = \{A, B\}^{alice}$

$CERT_{alice}, SIG_{alice}$

Eve is not happy!

Who issues certificates?

- CA: Certification Authority
- Trustworthy
- Off-line operation
- Has a well-known certificate
- May store client certificates
- Revocation
- Very secure: physically and otherwise



Public Key Distribution

- Finding out correct public key of an entity
  - Binding between IDENTITY and KEY
- Possible attacks
  - name spoofing: a person can identify himself using a bogus name
  - denial of service: the legitimate user cannot decrypt messages

Public Key Distribution

- Diffie - Hellman (1976) proposed the "public file" concept
  - commonly accessible
  - no unauthorized modification
  - poor idea

Public Key Distribution

- Popek - Kline (1979) proposed "trusted third parties" (TTPs)
  - TTPs know public keys of the entities and distribute them on-demand basis
  - on-line protocol (disadvantage)

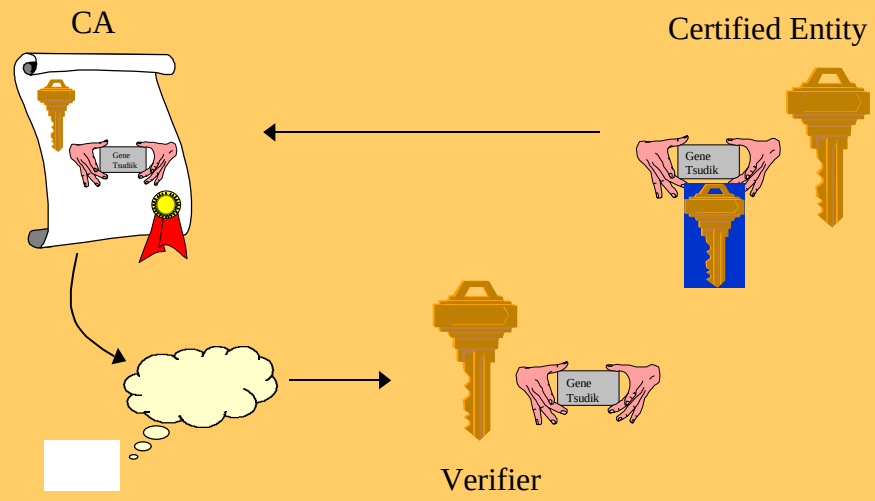
Certificates

- Kohnfelder (1978) proposed "certificates" as yet another public-key distribution method
- Binding between the public-key and its owner
- Issued (digitally signed) by the Certificate Authority (CA)
- Off-line process

Certificates

- Certificates checked by verifiers to find out correct public key of the target entity
- To verify a certificate, the verifier must:
  - know the public key of the CA
  - trust the CA
- Certificate checking is verification of the signature on certificate

Certificates



Certificate Example

Field	Value
Encryption cipher used	RC4-40, 40 bit
SSL Version	300
Client Certificate	
Serial number	f1f382f3f884f184 f9f48382f28182f8 858182f082f9f6f8 82f582f1f681f3f5
E-mail address	mike_lude@beyond-software.com
Common name	Michael Lude
Organizational unit	VeriSign Class 1 CA - Individual Subscriber
Organization	VeriSign, Inc.
Locality	Internet
Client's state or province	
Client's country	
Issuer's organizational unit	VeriSign Class 1 CA - Individual Subscriber
Issuer's organization	VeriSign, Inc.
Issuer's locality	Internet
Issuer's state or province	
Issuer's country	
Certificate valid from	Wednesday, February 18, 1998 at 12:00:00 AM
Certificate valid until	Monday, April 20, 1998 at 12:59:59 AM
Status	REVOCATION UNKNOWN

Related Issues

- CA certification policies (Certificate Practice Statement)
  - how reliable is the CA?
  - certification policies describe the methodology of certificate issuance
  - ID-control practices
    - loose control: only email address
    - tight control: apply in person and submit picture IDs and/or hard documentation

Related Issues

- TRUST
  - verifiers must trust CAs
  - CAs need not trust certified entities
- What is “trust” in certification systems?
  - How correct is the certificate information?
  - related to certification policies

Issues

- Certificate types
  - ID certificates (for authentication)
  - authorization certificates
    - no identity
    - binding between public key and authorization info
- Certificate storage and distribution
  - along with a signed message
  - distributed directories
  - centralized databases

Issues

- Certificate Revocation
  - certificates have lifetimes, but they may be revoked before the expiration time
  - Reasons:
    - certificate holder key compromise/lost
    - CA key compromise
    - end of contract (e.g. certificates for employees)
  - Certificate Revocation Lists (CRLs) hold the list of certificates that are not expired but revoked

Real World Analogies

- Is a certificate an “electronic identity”?
- Concerns
  - a certificate is a binding between an identity and a key, not a binding between an identity and a real person
  - one must submit its certificate to identify itself, but submission is not sufficient, the key must be used in a protocol
  - anyone can submit someone else’s certificate

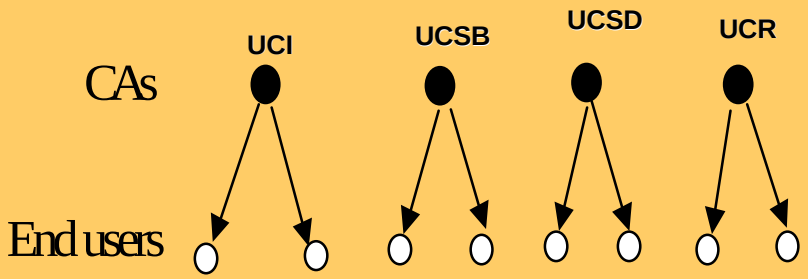
Real World Analogies

- Result: Certificates are not picture IDs
- So, what is the real world analogy for certificates?
  - Endorsed document/card that serves as a binding between the identity and signature, e.g., credit cards

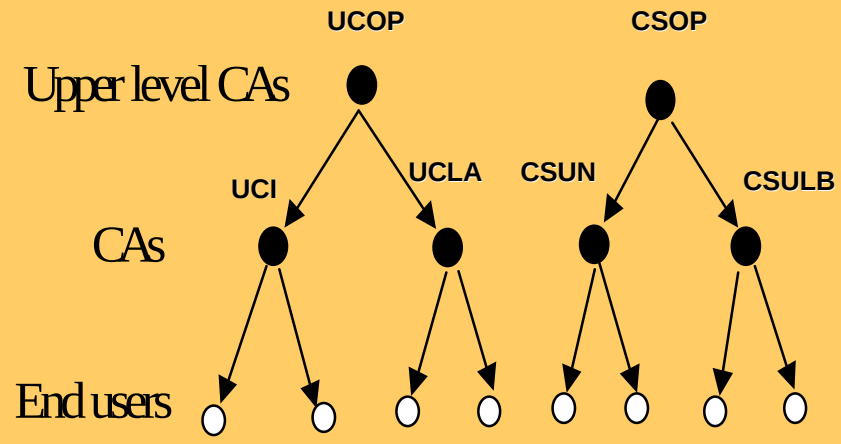
Business Practices

- Issue certificates and make money
  - several CAs
- Several CAs are also necessary due to political, geographical and trust reasons
- 2 interconnection models
  - hierarchical
  - cross certificates
- Result is a certificate network ==> PKI (Public Key Infrastructure)

Hierarchical PKI Example

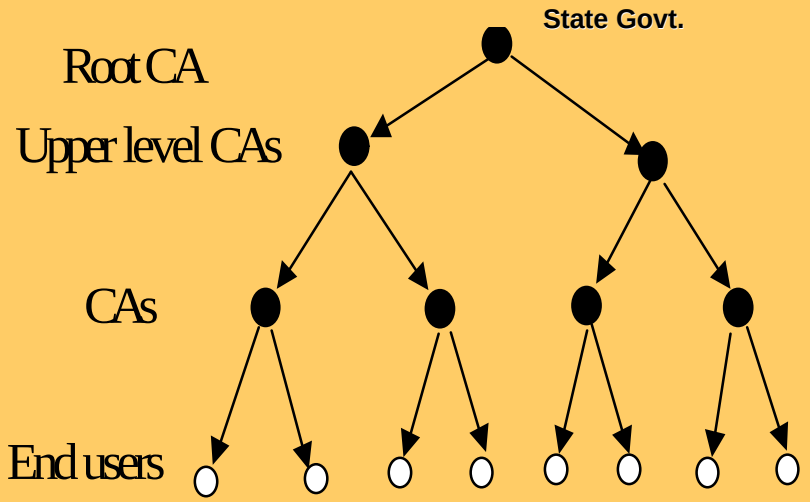


Hierarchical PKI Example

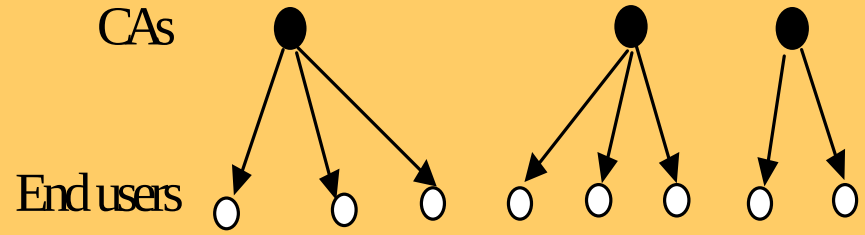


gtsudik@uci.edu

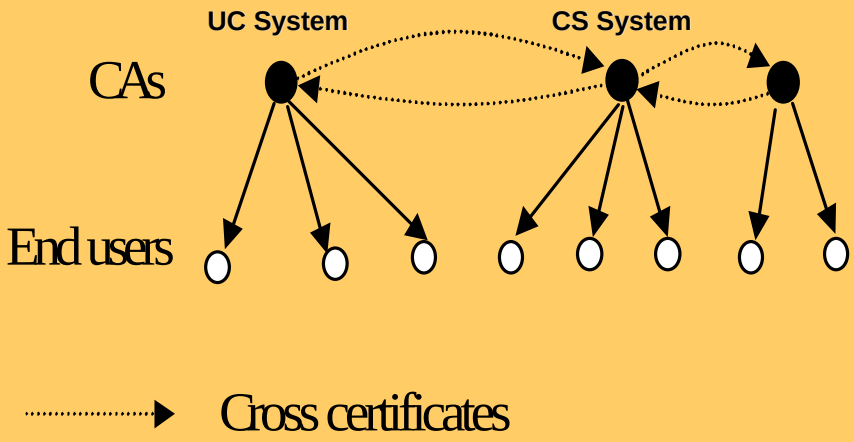
Hierarchical PKI Example



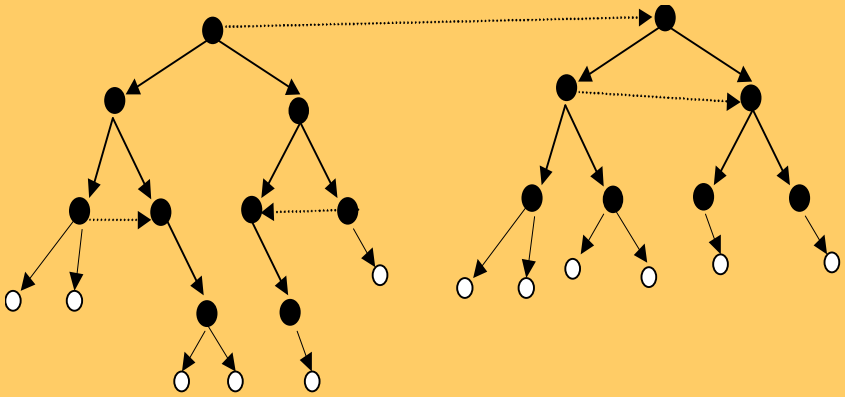
Cross Certificate Based PKI Example



Cross Certificate Based PKI Example

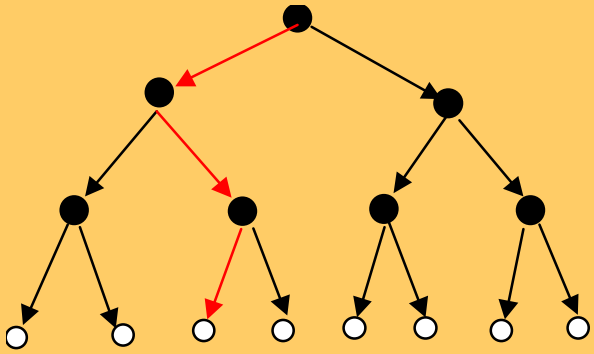


Hybrid PKI example

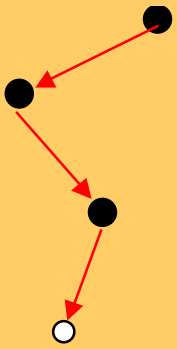


Certificate Paths

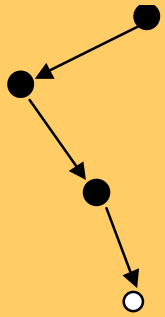
- Derived from PKI



Certificate Paths



Certificate Paths



- Verifier must know public key of the first CA
- Other public keys are found out one by one
- All CAs on the path must be trusted by the verifier

X.509

- X.509v3 current version
- ITU standard
- ISO 9495-2 is the equivalent ISO standard
- Defines certificate structure, not PKI
- Identity and attribute certificates
- Supports both hierarchical model and cross certificates
- End users cannot be CAs

Some X.509 based PKIs

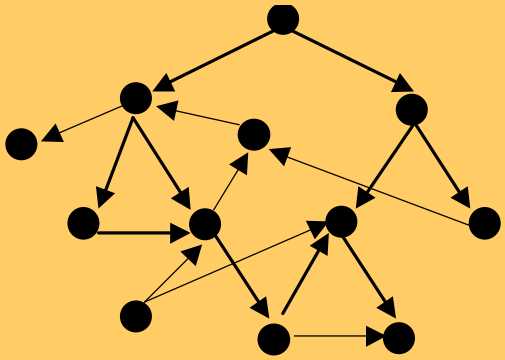
- Privacy Enhanced Mail (PEM)
  - hierarchical, no cross certificates
  - first but discontinued
- Secure Electronic Transaction
  - PKI for electronic payment
  - secure but not widely deployed
- PKIX
  - general purpose X.509 based PKI
  - S/MIME is based on PKIX

PGP (Pretty Good Privacy)

- E-mail security system with unique certificate and PKI structure
- Remarkable
  - PKI from scratch
  - thousands of users
  - no boss, no governing body
  - everybody is end user, everybody is CA
  - user-centered trust structure

PGP (Pretty Good Privacy)

- PKI of PGP
  - chaotic



DNSSEC

- Security extension to DNS
- Not X.509 based, but hierarchical (uses existing DNS topology)
- Distributed
- Provides
  - authentication of domain information, i.e., who is authorized for what addresses
  - storage and distribution of certificates
- Good and practical system

SSL and S-HTTP

- SSL (Secure Socket Layer), S-HTTP (Secure HTTP)
- Certificate based systems, but do not have a particular PKI
- CA certificates are embedded in browsers
- You trust them (by default), because browser company says so !
- The worst, but the most practical !!!