

Public Key Infrastructure

Dr. Arjan Durresi
Louisiana State University
Baton Rouge, LA 70810
Durresi@csc.lsu.edu

These slides are available at:

<http://www.csc.lsu.edu/~durresi/csc4601-07/>



- Public Key Infrastructure - PKI
- X.509 authentication and certificates

Public Key Infrastructure

- ❑ PKI – securely distribute public keys
 - Certificates
 - Repository of certificates
 - Method for revoking certificates
 - Chain certificates
- ❑ Certificate – a signed message vouching that a particular name goes with a particular public key
 - [Alice's public key is 775899]_{Carol}
 - [Carol's public key is 823756]_{Ted} ⇒ [Alice's public key is 775899]_{Carol}

Certification Authority

- ❑ CA – a trusted third part that authenticates entities taking part in an electronic transaction
- ❑ Certificate – a digital document that establishes the credentials of the entities participating in a transaction
 - Name of the subscriber
 - Public key of the subscriber
 - Issuing CA's public key

Registration Authority

- ❑ RA – responsible for the interaction between clients and CAs
- ❑ Intermediary between CA and clients
- ❑ RA's tasks:
 - Receive entity request and validate them
 - Send the request to CA
 - Receive the processed certificate from CA
 - Send the certificate to the correct entity
- ❑ RA – scale PKI applications across different geographic locations

PKI Clients

- ❑ Send a request to generate a public-private key pair. A CA or the client can do this.
- ❑ After the key is generated, a request is sent to the CA for a certificate. This request can be routed through an RA
- ❑ After the client receives the certificate from CA, it can use the certificate to identify itself
- ❑ All communication between CA and clients are secure
- ❑ A Client is responsible to ensure the safety of its private keys

Digital Certificates

- ❑ Digital certificates enables to:
 - Establish the integrity of the public key
 - Bind the public key and its associated information to the owner in a trusted manner
- ❑ Digital certificates includes the following elements:
 - Serial number of the certificate
 - Digital signature of CA
 - Public key of the user
 - Date of expiration
 - Name of the CA that has issued the certificate

Digital Certificates

- ❑ After a digital certificate is obtained, the entity can use it in the following manner
 - The subscriber digitally signs the message with his private key
 - The recipient after receiving the message, verifies the digital signature with the subscriber's public key and queries the global directory database to check the validity of the subscriber's digital signature
 - The global directory database returns the status of the subscriber's digital signature
- ❑ To verify a CA's signature, its public key is needed. Typically pre-installed in web browsers
- ❑ Certificates are distributed by users themselves or using a directory server

Terminology

- ❑ Anything that has a public key – *principal*
- ❑ Who signs a certificate – *issuer*
- ❑ *Subject* – whose name and key are being vouched
- ❑ *Target* – whose path key is being verified
- ❑ *Verifier* – who evaluates a chain of certificates
- ❑ *A trusted anchor* – an entity that is trusted

PKI Trust Models

- ❑ Monopoly Model
- ❑ Monopoly & Registration Authorities (RAs)
- ❑ Delegated CAs
- ❑ Oligarchy
- ❑ Anarchy

Monopoly Model

- ❑ One single that signs all certificates – Single CA. This solution is simple but:
 - There is no one universally trusted organization
 - Difficult to change keys
 - Difficult to certify keys – How would they know you? How to securely transmit your key?
 - Monopoly control ...

Monopoly & Registration Authorities (RAs)

- ❑ Similar to Monopoly model – CA chooses other organizations RAs to securely check identities and obtain voucher for public keys
- ❑ RAs securely communicate to CA
- ❑ More convenient and secure than the Monopoly model
- ❑ Other disadvantages remain
- ❑ RA has to do the security-sensitive operation of mapping name to key
- ❑ CA might provide a tamper-proof audit trail of certificates it has signed.

Delegated CAs

- ❑ The trust anchor CA issues certificates to other CAs, vouching for their trustworthiness as CAs
- ❑ The difference between delegated CAs and RAs
 - One certificate vs. chain of certificates
- ❑ Similar security and operational properties as RAs model

Oligarchy

- ❑ Used in browsers
- ❑ Many trust anchors – a certificate issued by any of them is accepted
- ❑ If any of CAs is compromised – all security at risk
- ❑ The trust anchors are chosen by the product vendor
 - How? Why? – depends on the vendor
 - Users have no way to check
- ❑ Users can be tricked

Anarchy Model

- ❑ Used by PGP
- ❑ Each user is responsible for configuring some trust anchors
- ❑ Some organization volunteer to keep a certificate database into which any user can deposit certificates
- ❑ Works for small communities where the chain can be trusted
- ❑ How can be trusted a chain of unknown entities?

Name Constrains

- ❑ A CA is trusted to certify a subset of users
- ❑ For example LSU CA can be trusted to certify keys of xxx@lsu.edu but not yyy@osu.edu
- ❑ Users might have multiple names. Each name is a separate PKI entity

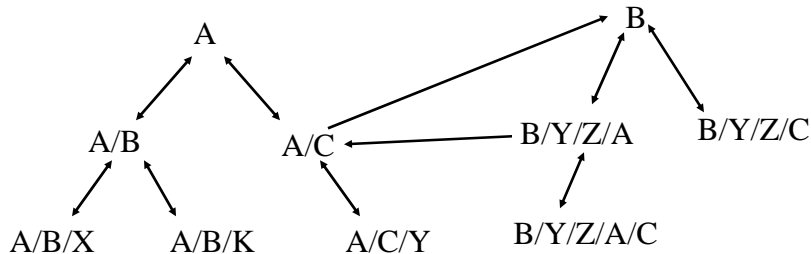
Top-down with name constrain

- ❑ Similar to the monopoly model.
- ❑ Everyone must be configured with a pre-ordered, never changing root key and that root CA delegates to other CAs.
- ❑ The delegated CAs are allowed to issue certificates for their portion of namespace
- ❑ Easy to find the path of a name – follow the namespace from the root down
- ❑ Problems of monopoly model

Bottom-up with name constrain

- ❑ Each organization can create its own PKI and then link to others
- ❑ The parent certifies the child's name and the child certifies the parent's name
- ❑ In addition to up and down links cross links are allowed

Bottom-up with name constrain



Revocation

- ❑ The validity time is in order of months
- ❑ There are cases when certificates need to be revoked, similar to credit cards
- ❑ On line certificate status protocol OCSP
 - For each transaction one has to check the status of the certificate
- ❑ Then why expiration time:
 - There are systems that don't do revocation
 - A way to collect revenue multiple times

Revocation Mechanism

- ❑ Certificate Revocation List: CA periodically issues a signed list of all the revoked certificates
- ❑ Each CRL contains a complete list of all the unexpired revoked certificates
- ❑ Delta CRL: lists changes from the last
 - There are all certificates that have been revoked since November 4, 3:00PM
- ❑ On-line revocation server (OLRS) – a system that can be queried over the net about revocation status

Good list

- ❑ If the CRL contains the list of all valid certificates it is more difficult to insert bogus certificates
- ❑ Good list longer than bad list – low performance
- ❑ An organization might not want to make the list of its valid certificates public. Having published only the hashes of valid certificates
- ❑ Both good and bad list will contain only serial numbers and hashes

Directories

- ❑ PKI can be facilitated by a distributed database indexed by a hierarchical name
- ❑ Each name – repository of information
- ❑ DNS – directory -fast
- ❑ X.500, its querying language – LDAP, less flexible
- ❑ Most deployed PKI do not use directories

Finding Certificates Chains

- ❑ The search can be done from subject and working towards the trust anchors – in *forward direction* or from a trust anchor – *reverse*

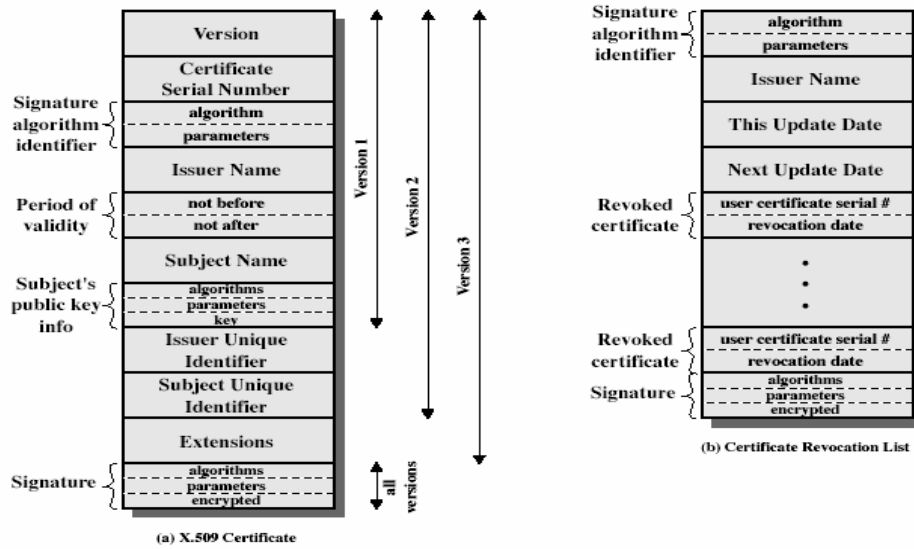
X.509 Authentication Service

- ❑ Part of CCITT X.500 directory service standards
 - distributed servers maintaining some info database
- ❑ defines framework for authentication services
 - directory may store public-key certificates
 - with public key of user
 - signed by certification authority
- ❑ also defines authentication protocols
- ❑ uses public-key crypto & digital signatures
 - algorithms not standardised, but RSA recommended

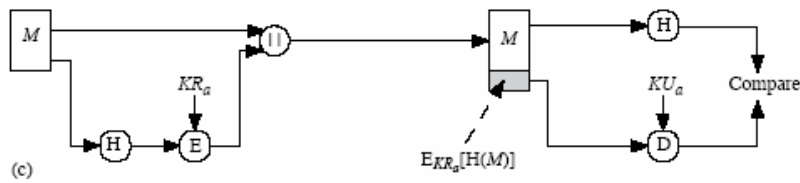
X.509 Certificates

- ❑ Issued by a Certification Authority (CA), containing:
 - version (1, 2, or 3)
 - serial number (unique within CA) identifying certificate
 - signature algorithm identifier
 - issuer X.500 name (CA)
 - period of validity (from - to dates)
 - subject X.500 name (name of owner)
 - subject public-key info (algorithm, parameters, key)
 - issuer unique identifier (v2+)
 - subject unique identifier (v2+)
 - extension fields (v3)
 - signature (of hash of all fields in certificate)
- ❑ notation CA<<A>> denotes certificate for A signed by CA

X.509 Certificates



X.509 Certificates



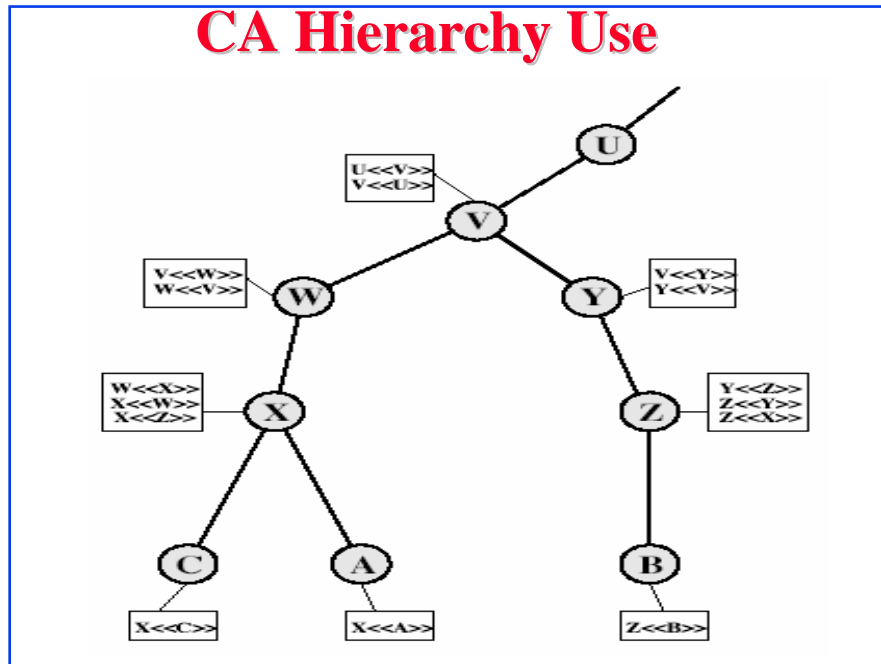
Obtaining a Certificate

- ❑ Any user with access to CA can get any certificate from it
- ❑ only the CA can modify a certificate
- ❑ because cannot be forged, certificates can be placed in a public directory

CA Hierarchy

- ❑ If both users share a common CA then they are assumed to know its public key
- ❑ otherwise CA's must form a hierarchy
- ❑ use certificates linking members of hierarchy to validate other CA's
 - each CA has certificates for clients (forward) and parent (backward)
- ❑ each client trusts parents certificates
- ❑ enable verification of any certificate from one CA by users of all other CAs in hierarchy

CA Hierarchy Use



Certificate Revocation

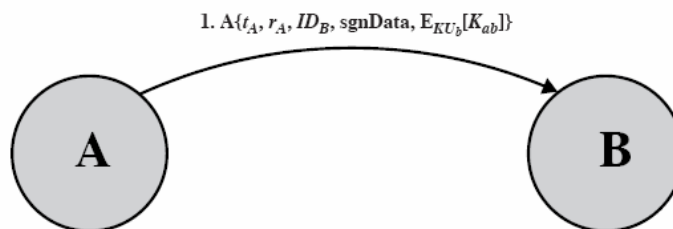
- ❑ Certificates have a period of validity
- ❑ may need to revoke before expiry, eg:
 1. user's private key is compromised
 2. user is no longer certified by this CA
 3. CA's certificate is compromised
- ❑ CA's maintain list of revoked certificates
 - the Certificate Revocation List (CRL)
- ❑ users should check certs with CA's CRL

Authentication Procedures

- ❑ X.509 includes three alternative authentication procedures:
 - ❑ One-Way Authentication
 - ❑ Two-Way Authentication
 - ❑ Three-Way Authentication
- ❑ all use public-key signatures

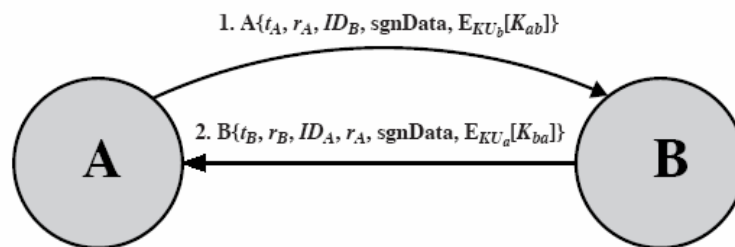
One-Way Authentication

- ❑ 1 message (A->B) used to establish
 - the identity of A and that message is from A
 - message was intended for B
 - integrity & originality of message
- ❑ Message must include timestamp, nonce, B's identity and is signed by A



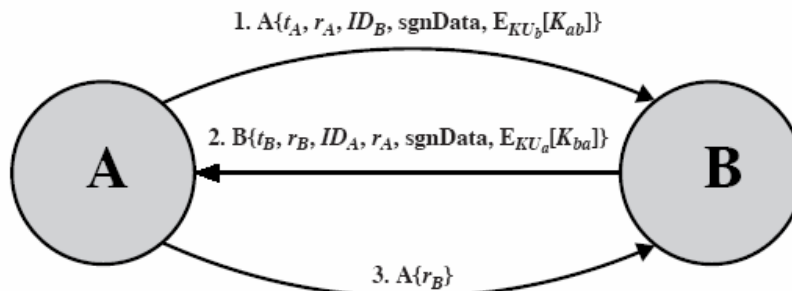
Two-Way Authentication

- 2 messages (A->B, B->A) which also establishes in addition:
 - the identity of B and that reply is from B
 - that reply is intended for A
 - integrity & originality of reply
- reply includes original nonce from A, also timestamp and nonce from B



Three-Way Authentication

- 3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks
- has reply from A back to B containing signed copy of nonce from B
- means that timestamps need not be checked or relied upon



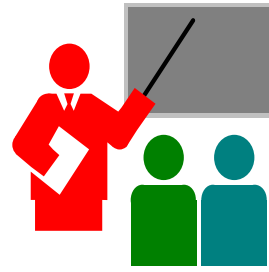
X.509 Version 3

- ❑ Has been recognised that additional information is needed in a certificate
 - email/URL, policy details, usage constraints
- ❑ rather than explicitly naming new fields defined a general extension method
- ❑ extensions consist of:
 - extension identifier
 - criticality indicator
 - extension value

Certificate Extensions

- ❑ Key and policy information
 - convey info about subject & issuer keys, plus indicators of certificate policy
- ❑ certificate subject and issuer attributes
 - support alternative names, in alternative formats for certificate subject and/or issuer
- ❑ certificate path constraints
 - allow constraints on use of certificates by other CA's

Summary



- ❑ PKI
- ❑ X.509 authentication and certificates