A low auto payment is only a few clicks away

Refinance your auto loan—see if you qualify for a lower monthly payment in minutes.

Get started
X.509 Outline

- X.509 Overview
- Certificate Lifecycle
- Alternative Certification Models
What is X.509?

- The most commonly used Public Key Infrastructure (PKI) on the web
- Public Key Infrastructure
  - Create, manage, distribute, and store certificates
- Certification Validation Path Algorithms
- Certificate Lifecycle Management
  - Certificate Revocation Lists
Assumptions and Goals

- Users of certificates will utilize them in a variety of environments
  - Certificates should be nonspecific in regards to environment
- Users of PKI will not necessarily be technologically sophisticated
  - Need for automated and deterministic forms of authentication and identification
- Large number of security dimensions/attributes
  - Minimize chances that CA administration mistake will result in broad compromise
  - Decrease the number of configuration choices necessary
X.509 Architecture

- **End entity**
  - Subjects or users of PKI certificates
- **Certification Authority (CA)**
  - Issues and signs certificates
  - Certification Practice Statement determined by each CA
- **CRL issuer**
  - May be the same entity as CA
- **Repository**
  - System that stores certificates and CRLs
  - Distributes them as necessary to end entities
Commercial Certification

- On the local level:
  - Extremely fragmented

- For websites:
  - Most use SSL certificates
  - Significant barriers to entry
    - Symantec - 42.9%
    - Comodo Group - 26%
    - Go Daddy - 14%
    - Global Sign - 7.7%
Certificate Structure

- Certificate
  - Version
  - Subject
  - Issuer
  - Public key for Subject
  - Validity period
    - Not Before
    - Not After
- Signature Algorithm
- Signature Field

Must be Distinguished Names:
- Unique identifier in CA’s domain
- Can contain
  - Country
  - Organization
  - State or Province
  - Common name
  - Serial Number
Extensions

- Allow for flexibility of certificates to contain additional fields
  - Critical vs. Non-critical extensions

- Common Extensions:
  - Authority Key Identifier - means of identifying public key corresponding to private key used to sign
  - Subject Key Identifier - identify certificates that contain particular public key
  - Key Usage - defines purpose of key
  - Certificate Policy information
Certificate Lifecycle

- Once a CA verifies the credentials of a user, it can create and issue a certificate for that user
  - Policy matter - context dependent
- After certificates are issued, they are either renewed or allowed to expire
- Can be revoked if:
  - CA has been compromised
  - User’s secret key was leaked
  - Name was changed
Certification Revocation List (CRL)

- Two major types of CRLs
  - Complete CRL - signed and time-stamped list identifying revoked certificates
  - Delta CRL - used for updates to the complete CRL
- Published periodically at defined interval

- Issues
  - Mistakes in revocation list
  - Access to most current CRLs
  - No guarantee that all certificate copies will be revoked
Comparisons to X.509

- PGP (Web of Trust model)
  - Introducer Model - users are referred from one user to another (creating a “web”)
  - Updates to the web are found by users themselves
    - No guarantee if or when the web will be up-to-date
  - No centralized entity
  - Not scalable, but potentially preferable in a small group

- X.509
  - Users trust CAs, rather than each other (transitive trust)
  - Hierarchical certification validation from centralized entities
  - Updates managed by CAs
  - Scalable
Practical Implications of X.509

- Each browser has a built in set of predetermined “trusted root CAs” to facilitate SSL transactions
  - The browser developers determine the primary CA’s that are trusted third parties to the users

- The Internet is all about decentralization, but X.509 relies on a few number of centralized authorities.
  - Usage of duplicate RSA-moduli keys, man-in-the-middle attacks, etc. have all occurred in the last few years
  - Can we trust them? If not, what alternatives do we have?
  - Is this an issue? Do we need a large number of providers?