Advanced Cryptography and PKI

- *crypto service provider* - calls crypto functions as a service
- *master secret* - used to derive session keys
- A *Cipher Suite* is the combination of encryption, signing, and hashing algorithms supported
- *Pinning* - associating a host with a previous certificate or public key
- *Key Escrow* - third party with your private key

Three characteristics of *key strength*:

- randomness
- length
- cryptoperiod - expiration

  Need to explore about half of keyspace in order to break

Block Cipher Modes of Operation:

- Electronic Code Block (ECB)
  - Each plaintext block is ciphered separately - orthogonal map
- Cipher Block Chaining (CBC)
  - Block is ciphered, ciphertext is XORd with next plaintext block
- Counter (CTR)
- Galios / Counter (GCM)
  - Encrypts the plaintext and includes an encrypted MAC

PKI

Certificates

> binds an individual's identity to a public key, by transitive trust of a third party

- IETF X.509 Standard, version 3 (aka. PKIX - Public Key Infrastructure X.509)
  - version number
  - subject (owner of cert)
  - public key
  - issuer
  - serial number
  - validity
  - certificate usage
  - signature algorithm
  - extensions
    - iterated by Object Identifiers (OID), and critical / non-critical flag
    - unrecognized critical fields must cause rejection
- May contain network address, or domain name

  - Wildcard certs: *.foo.com
- *Subject Alternative Name* (SAN) / *Unified Communications Certificate* (UCC) - an *extension* to a certificate to include one or more domain names, or a user principal name (UPN), for added identity authenticity.
- *Domain Validation* - low-trust cert that validates control over the domain name
- *Extended Validation* - high-trust cert extension that allows enhancing the certificate with the company name
  - do not support wildcards

Four primary types:

- End-entity certs - end-users, like people, routers, firewalls, servers
- CA certs
- Cross-certification certs - peer-to-peer trusts
- Policy certs - CA-approved PKI policy

Encoding and format:

- Distinguished Encoding Rules (DER)
  - ASN.1, can encode any data object to a binary
  - .der
- Privacy-Enhanced Electronic Mail (PEM)
  - most common
  - Base64, text header and footer
  - .pem, .cer, .crt, .key
- Microsoft CER
  - Binary DER or ASCII PEM
  - .cer for Windows, .crt UNIX
- Key File
  - PKCS#8 Keys
  - DER or PEM
  - .key
- PFX
  - PKCS#12
  - Import and export on Windows - Binary - Storing server cert, intermediate certs, and private key
  - .pfx, .p12 . P7B
  - PKCS#7
  - Base64 ASCII
  - Certs and Cert Chains
  - Windows & Java Tomcat
  - .p7b, .p7c

Certificate Authorities

- issue digital certificates via a *Certificate Signing Request* (CSR) - how someone associates their identity to their public key

- comprised of:
    - software
    - hardware
    - procedures
    - policies
    - people
- *Certificate Practice Statement* (CPS) is a document detailing how a CA manages its certificates, and how to register for one
- *Intermediate CA* - transfers trust between CAs
    - aka “subordinate CA”
    - subordinate CA uses higher-level CA as a reference

Trust Models

- They may be arranged *heirarchical* (one master / root, self-signed CA)
    - unidirectional trusts
    - tree of root CA, intermediate CAs, leaf CAs
- *distributed* (group of CAs), aka “peer-to-peer”
    - no established trust anchor between CAs
    - bidirectional trust, *cross certification*
    - not scalable - fully connected mesh
- *hybrid*
    - roots are cross certified
    - *bridge* - link between multiple CA networks, with one acting as a *facilitator*

Certificate Revocation Lists

declare what certificates are no longer (or temporarily) invalid

- Maintained by owning CA
- Communication might be through the use of deltas after an initial set
- *Online Certificate Status Protocol* (OCSP)
    - checks a cert’s status via n OCSP server, rather than pushing distribution lists
- Suspension requests can also be enumerated in CRLs
- *Certificate Repositories* manage a centralized directory of digital certificates, aka. Key Escrow
- *Certificate Policies* are a set of rules that govern the operation of PKI
- *Web-Client Certificates* ensure for a web-browser that a web-server is authentic w.r.t. their domain.
- *destruction* - removing affiliation with a certificate, and private / public keys

Four stages of certificate life cycle:

- Creation
- Suspension
- Revocation
- Expiration

  Distributed trust is the basis for most trust models on the internet, but there exists others as well, including 3rd-party trust models.

- A distributed CA model, where only one CA facilitates all other CAs is considered a 3rd party trust model.

IPSec

- Authentication Header - Integrity
- Encapsulating Security Payload - Confidentiality
- *transparent* - nobody has to install anything to use it
- useful for VPNs
- manages Authentication, Confidentiality, and Key-Management