PKI

Digital Signatures

- Binds a message with the sender’s identity
- **Signing algorithm**: takes a message and a (private) signing key, outputs a signature
- **Verification algorithm**: takes a (public) verification key, a message, and a signature, generates True/False outcome

- Provides:
  - Authentication
  - Data integrity
  - Non-Repudiation (MAC does not provide this)

Digital Signatures and Hashes

- Digital signatures are used with hash functions, hash of a message is signed, instead of the message
- **Hash function must be**:
  - Pre-image resistant
  - Weak collision resistant
  - Strong collision resistant

Digital Signatures with RSA

**Signing message M**
- Compute \( S = M^d \mod n \)
- Equivalent to RSA decryption operation
- Requires private key (hence slower)
- RSA is slow, so instead of signing message, compute hash of message (e.g., SHA) and sign hash!

**Verifying signature S**
- Uses public key \((e, n)\)
- Compute \( S^e \mod n = (M^d \mod n)^e \mod n = M \)
- Similar to encryption operation (faster than signing)

Digital Signatures with Asymm. Encr

**Signing message M**
- Compute hash \( h_1 = h(M) \)
- Apply decryption function \( \text{Signature} = D(h_1) \)
- Send \( M, \text{Signature}(M) \) to verifier

**Verifying signature S**
- Compute hash \( h_2 = h(M) \)
- Apply encryption function \( \text{h1} = E(\text{Signature}(M)) \)
- Verify if \( \text{h1} == h_2 \)

**DSA** is another popular signing algorithm
- Uses discrete logarithm hardness assumption
Public-Key Infrastructure (PKI)

- Goal: establish trust relationship based on certification of identity
- A Certificate binds identity to public key
- Contents signed by a trusted Certificate Authority (CA)
  - Can be verified by anyone using public key of CA
- There is a chain of trust established that leads to a CA
- PKI enable authentication, key exchange and digital signatures

X.509 Certificates

- Certificates contain:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - issuer X.500 name (CA)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - signature of all fields in certificate
- Commonly used standard to represent certificates is PEM

Certification Authority

- Well-known entity, trusted by other parties
- Must implement well-defined, standard processes for identity vetting
- Provides online access to all certificates issued
- Provides Certificate Revocation Lists (CRL): certificates that are no longer valid (e.g., private key was compromised)
  - These must be kept up-to-date!
- Private key of CA requires highest levels of security
  - 2048-bit or higher
  - Certificate of CA is self-signed
  - Private key stored Hardware Security Module (HSM)

Obtaining a certificate (1/2)

- Generate a private/public key
  - Several tools exist, e.g., openssl
- Must keep private key secure!
  - Typically encrypt with symm. encryption, e.g., AES/DES
- Create a certificate signing request (CSR) which includes public key as well as identifying information
  - CSR sent to CA (e.g., VeriSign)
- CA must ensure that the requester is indeed the entity in the CSR
  - This is called identity vetting
  - May require physical presence, presenting paper documents
- If identity is verified, CA signs the CSR and the resulting certificate is sent back to requester

Validity of Certificates

- Certificates are valid if:
  - Signature of CA verifies
  - Dates of the certificate are valid
  - Certificate was not revoked
- Certificates can be revoked before expiration if
  - user's private key is compromised
  - user is no longer certified by this CA
  - CA's certificate is compromised
Trust Chain

- Typically a hierarchy of trust is maintained
  - Too much overhead for CA to vet identity of everyone
- CA deals with higher-level organizations
  - E.g., enterprise, university
- Example:
  - Verisign (CA) signs certificate for state of MA
  - State of MA authority signs certificate for UMass System
  - UMass System signs certificate for UMB
  - UMB signs certificates for its employees
  - Employees are vetted by UMB only, chain of trust formed
  - Verification must check all signatures in the chain