Public Key Infrastructure

Mark Earnest
Lead Systems Programmer
The Pennsylvania State University

"PKI is the world's only application written entirely in Powerpoint" - Larry Riffle

Symmetric Key

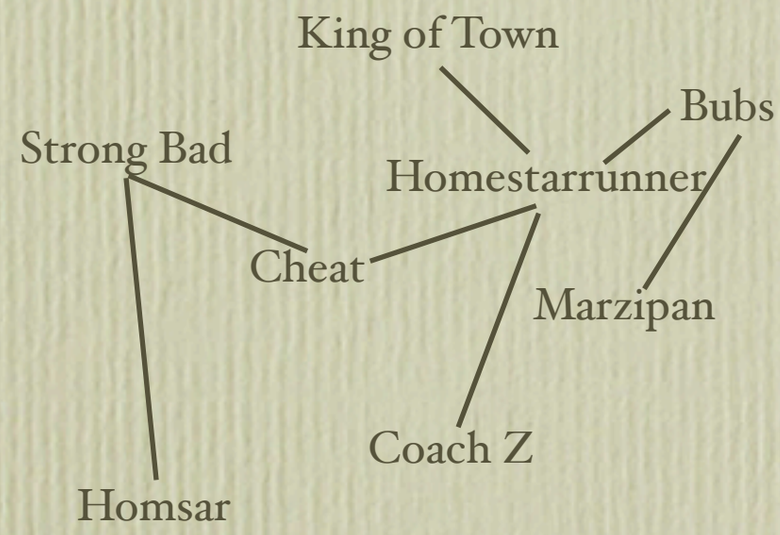
- "Shared Secret"
- ROT13, DES, IDEA, RC5, AES
- Need for secret key exchange leads to scaling problems ($n^2/2$ problem)
- Encryption/decryption only
- Fast

Public Key

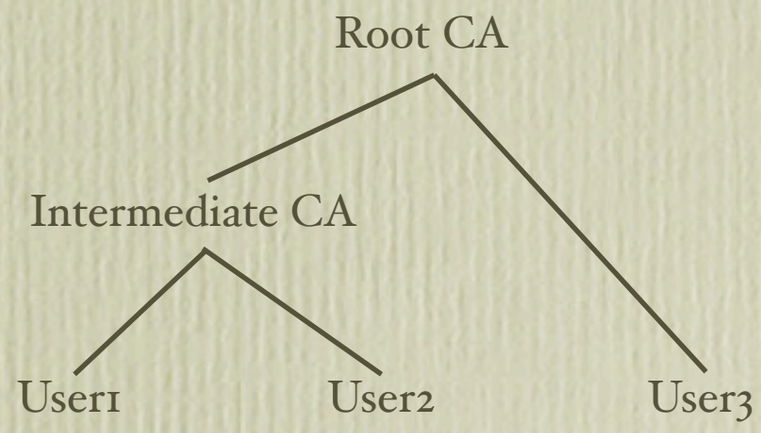
- "New Directions in Cryptography" - Diffie & Hellman
- Public and private key pairs
- Encryption/decryption, digital signature, & data integrity
- RSA, DSA, & DH
- Slow

Trust Models

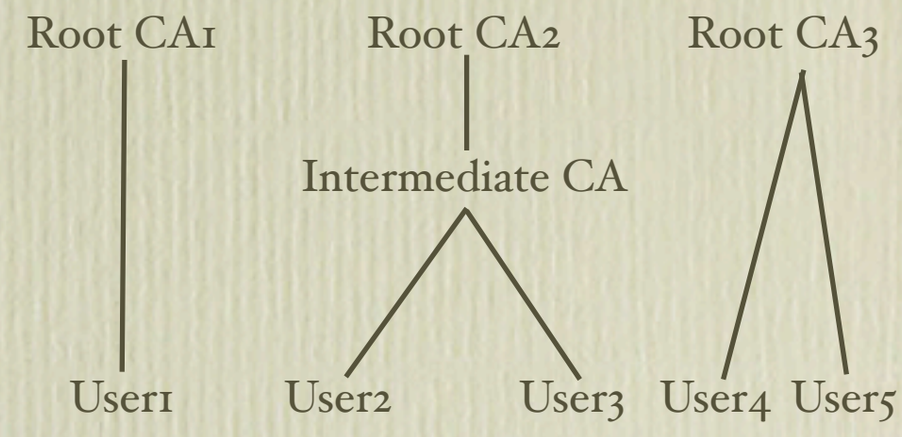
User Centric (PGP)



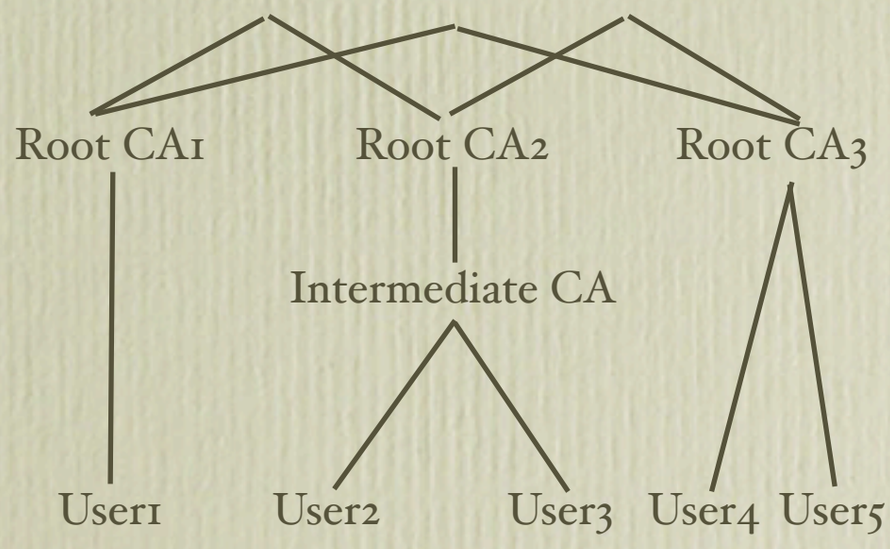
Strict



Web Model



Distributed



Public Key Encryption

- Randomly generated symmetric key used to encrypt message
- Public key used to encrypt symmetric key
- Recipient's private key decrypts the symmetric key
- Message decrypted by symmetric key

Message Hashing

- Hashing - taking binary input and creating fixed size binary output (message digest)
- Same message always yields same results
- Digest value contains no information that could be used to determine origin (one way)
- Small changes in input create many changes in the message digest
- MDC2, MD2, MD4, MD5, SHA1, and RIPEMD-160

Digital Signature

- Used to validate source of message (non-repudiation) and verify integrity of message
- The signer hashes the message to a fixed value size, then encrypts this hash with their private key
- The verifier decrypts the message with the signer's public key, then compares the result with their own hash of the message

Pretty Good Privacy

- Created by Phil Zimmermann in the early 90s
- Primarily used to encrypt and sign email
- “Web of Trust” - Users sign each other’s public keys to assert trust.
- Undesirable in most enterprise settings due to its ad hoc and unstructured trust model

Public Key Infrastructure

- "A PKI is a pervasive security infrastructure whose services are implemented and delivered using public key concepts and techniques"

- x.509 v3 Digital Certificates

- Certificates must be signed by a Certificate Authority to assure validity, creating a strict hierarchical trust model

- Common uses include SSL, S/MIME, Java applet & windows device driver signing, and VPN authentication

x.509 v3

Version	Serial Number	Signature	Issuer	Validity	Subject	Subject Public Key Info	Issuer Unique ID	Subject Unique ID	Extensions
Identifies the version of the certificate	Unique integer identifier for the certificate	Algorithm ID used to sign the certificate	Unique name of the certificate issuer	Lists valid start and end times for cert validity	Unique name of the owner	Public key & algorithm ID of the owner	Optional unique ID of issuing CA	Optional unique ID of subject	

Extensions

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- CRL Distribution Point
- Private Key Usage Period
- Subject Alt Name
- Basic Constraints

Key Usage

- Digital Signature
- Non-repudiation
- Key Encipherment
- Key Agreement
- Certificate Signature
- CRL signature
- Encipher/Decipher only

Comprehensive PKI

Certification Authority	Certification Repository	Certificate Revocation
Key Backup	Key Recovery	Automatic Key Update
Key History Management	Cross-Certification	Client Software
Authentication	Integrity	Confidentiality
Secure Time Stamping	Notarization	Non-Repudiation
Secure Data Archive	Privilege/Policy Creation	Privilege/Policy Verification

Certificate Revocation

- CRL - Certificate Revocation List: A digital certificate containing the serial numbers of revoked certificates
- Delta CRL - Incremental posting of revocation certificates
- Indirect CRL - CRL that covers multiple CAs within a single PKI domain
- OCSP - Online Certificate Status Protocol - Client/Server CRL mechanism

Politics

- Certificate Authority Oligopoly
- CA Browser Cache
- Audits and Federal Regulations
- PGP and the Web of Trust vs x.509 and the strict hierarchy
- Who owns identity?

Beyond HTTPS and S/MIME

- SAML & Liberty Alliance
- WS:Security & WS:Federation
- Smart Cards
- TCPA & Palladium
- DRM

References

- Understanding Public Key Infrastructure - Carlisle Adams & Steve Lloyd - New Riders

- Network Security with OpenSSL - John Viega, Matt Messier, & Pravir Chandra - O'Reilly

- RSA Security's Official Guide to Cryptography - Steve Burnett & Stephen Paine - RSA Press

Questions?