Computer security: authentication of principals and cryptographic protocols

6.033 Spring 2007

**key distribution**

1. M, Sign(M, KA

2. Alice?

3. M = {“A’s KA

• 3 is a certificate for Alice’s public key
• Charles is called a certificate authority
• The interaction is an example of a cryptographic protocol

**Shorter notation**

1. \([M]^{KA

2. Alice?

3. \([M]^{KA

• Subscript for signing
• Superscript for encrypting

**Denning-Sacco**

1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key

**Impersonation Attack**

Thinks Bob is Alice

1. \([A, K_{A,B}, T]_{K_{CA,B}}
2. \([K_{A,B}, T]_{K_{CA,B}}
3. \([K_{A,B}, T]_{K_{CA,B}}

Deadline: May 20

HKN Underground Guide


Link posted on 6.033 home page

Deadline: May 20
Denning-Sacco (fixed)

Example: Web (SSL simplified)

- U: https://www.amazon.com
- B → W: \{random\textsubscript{c}, session-id, ciphersuites\}
- B ← W: \{random\textsubscript{s}, session-id, {amazon.com, K\textsubscript{pub-amazon}}\textsubscript{Kversign}\}
- B: verify({amazon.com, K\textsubscript{pub-amazon}}\textsubscript{Kversign}\textsubscript{Kpub-verisign})?
- B → W: {pre-master-secret}\textsubscript{K\textsubscript{pub-amazon}}

Be explicit!

X509 certificate

- struct X509\_certificate {
  unsigned version;
  unsigned serial;
  signature\_cipher\_identifier;
  issuer\_signature;
  issuer\_name;
  subject\_name;
  subject\_public\_key\_cipher\_identifier;
  subject\_public\_key;
  validity\_period;
};

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.