Computer security: authentication of principals and cryptographic protocols

6.033 Spring 2007
HKN Underground Guide


Link posted on 6.033 home page

Deadline: May 20
key distribution

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

1. M, Sign(M, KA_{priv})
2. Alice?
3. M = \{“A’s Ka_{pub} =…”\}, sign(M, KC_{priv})
• Shorter notation

1. \( \{M\}^{KB_{\text{pub}}}_{KA_{\text{priv}}} \)

2. Alice?

3. \( \{\text{“A’s } Ka_{\text{pub}} = \ldots\}\}^{KC_{\text{priv}}} \)

- Subscript for signing
- Superscript for encrypting
1. Authenticate Alice to Bob and Bob to Alice
2. Set up a shared-secret key
Impersonation Attack

Alice

\{A, K_{Apub}, T\}_{KCApriv} + \{\{K_{AB}, T\}_{KApri} \}_{KBpub}

Thinks Bob is Alice

Charles

\{A, K_{Apub}, T\}_{KCApriv}

\{\{K_{AB}, T\}_{KApri} \}_{KCpub}

Bob
Denning-Sacco (fixed)

Be explicit!
Example: Web (SSL simplified)

- U: https://www.amazon.com
- B → W: \{random_c, session-id, ciphersuites\}
- B ← W: \{random_s, session-id, \\
  \{amazon.com, K_{pub-amazon}\}K_{versign}\}
- B: verify(\{amazon.com, K_{pub-amazon}\}K_{versign}, \\
  K_{pub-verisign})?
- B → W: \{pre-master-secret\}\^{K_{pub-amazon}}
- ......
**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.
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.