Computer security: authentication of principals and cryptographic protocols

Frans Kaashoek
6.033 Spring 2007
HKN Underground Guide


Link posted on 6.033 home page

Deadline: May 20
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. ${M}^{KB_{pub} \cdot K_{A_{priv}}}$
2. Alice?
3. \{“A’s $K_{a_{pub}} = \ldots$”\}$^{K_{C_{priv}}}$

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

Thinks Bob is Alice

\[ \{A, K_{A_{pub}}, T\}_KCA_{priv} \]

\[ \{\{K_{AB}, T\}_Kapriv\}_KC_{pub} \]

\[ \{A, K_{A_{pub}}, T\}_KCA_{priv} + \{\{K_{AB}, T\}_Kapriv\}_KB_{pub} \]
Denning-Sacco (fixed)

Be explicit!
Example: Web (SSL simplified)

- **U:** [https://www.amazon.com](https://www.amazon.com)
- **B → W:** \{random\_c, session-id, ciphersuites\}
- **B ← W:** \{random\_s, session-id, \{amazon.com, K\_pub-amazon\}\}
- **B:** `verify({amazon.com, K\_pub-amazon\_Kversign, K\_pub-verisign})`?
- **B → W:** \{pre-master-secret\}\_Kpub-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;
};
**www.amazon.com**

Issued by: RSA Data Security, Inc.

- **This certificate is valid**

### Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject Name</strong></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>State/Province</td>
<td>Washington</td>
</tr>
<tr>
<td>Locality</td>
<td>Seattle</td>
</tr>
<tr>
<td>Organization</td>
<td>Amazon.com Inc.</td>
</tr>
<tr>
<td>Common Name</td>
<td><a href="http://www.amazon.com">www.amazon.com</a></td>
</tr>
<tr>
<td><strong>Issuer Name</strong></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Organization</td>
<td>RSA Data Security, Inc.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>Secure Server Certification Authority</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>5C B4 2C EE 43 52 64 86 1A A2 F5 D7 02 BC 5A 01</td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)</td>
</tr>
<tr>
<td>Parameters</td>
<td>none</td>
</tr>
<tr>
<td><strong>Not Valid Before</strong></td>
<td>Thursday, December 22, 2005 7:00:00 PM US/Eastern</td>
</tr>
<tr>
<td><strong>Not Valid After</strong></td>
<td>Saturday, December 23, 2006 6:59:59 PM US/Eastern</td>
</tr>
<tr>
<td><strong>Public Key Info</strong></td>
<td></td>
</tr>
<tr>
<td>Algorithm</td>
<td>RSA Encryption (1 2 840 113549 1 1 1)</td>
</tr>
</tbody>
</table>
Advisories

Jan 2001 - Advisory from VeriSign, Inc.

VeriSign, Inc, discovered through its routine fraud screening procedures that on 29 and 30 January 2001, it issued two digital certificates to an individual who fraudulently claimed to be a representative of Microsoft Corporation. VeriSign immediately revoked the certificates. The updated certificate revocation list (CRL) is available at http://crl.verisign.com/Class3SoftwarePublishers.crl or through VeriSign real-time Online Certificate Status Protocol (OCSP) Services.

The certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name "Microsoft Corporation". The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation.