Security in the Ambient Computational Environment

S. Vidyaraman

Thesis defense for the degree of
Master of Science in
Computer Engineering
University of Kansas

August 14th, 2002

Committee:
Dr. Joseph B. Evans (Chair)
Dr. Gary J. Minden
Dr. Arvin Agah
Acknowledgements

Thanks to the ACE development team and the Management! I have had a wonderful time here at ITTC and KU.
Overview

• Background
• Security Issues Addressed
• Security Services Implemented
• Typical Scenarios
• Analysis
• Summary & Future Work
• Q&A
Background

- ACE: Ambient Computational Environment

- It's all about reinventing the 4 wheels of the car. But then ……

- Entities in ACE
  - ACE Services
  - ACE Users
ACE Services

- Databases
- ASD
- SRM
- HRM
- IButton

Database Storage & Retrieval

ACE Service Directory

System Resource Monitor

Host Resource Monitor
ACE User

Authentication Mechanisms

ACE Network

IButton

PDA

Access Mechanisms

FIU

Notebooks
Security Issues addressed

- Services communicate within themselves.
  - Network Commands
  - Data Streams (Audio and Video)
- Users
  - Authentication
- The Users Workspace is a VNC Session.
- How do we identify both Users and Services?
Security Services Implemented

- Remote Connection Manager
- Certificate Authority
- Certificate Distribution System
- Key Manager
Security Services Implemented

- **Remote Connection Manager**
  - Functionality
  - DH Key Establishment
  - SPEKE Protocol
- Certificate Authority
- Certificate Distribution System
- Key Manager
Remote Connection Manager

• Gateway to the ACE Domain from Outside
• Functions:
  • Authenticate the user
  • Establish a shared session key
• At present, it implements the SPEKE protocol
  • A Variant of the Diffie-Hellman Key establishment
  • One of the strong authentication mechanisms with (even) weak passwords
  • Minimum (3) number of passes
  • Protects against dictionary attacks
### Diffie-Hellman Key Establishment

- **Session Key Establishment**
- Assumes 2 known values
- Offers No Authentication

A prime number $p$ and a generator $g$ are known to Alice and Bob.

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Picks a secret number $R_A$</td>
<td>Picks a secret number $R_B$</td>
</tr>
</tbody>
</table>

**Key Set up**

- $Q_A = g^{(R_A)} \mod p$ $\rightarrow$
- $Q_B = g^{(R_B)} \mod p$ $\leftarrow$

- $K = Q_B^{(R_A)} \mod p$  
- $K = Q_A^{(R_B)} \mod p$
**SPEKE Protocol**

**Secure Password-authenticated Exponential Key Exchange**

The generator $g$ is now the squared hash of the password $S$

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>All operations are mod $p$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Q_A = S^{2R_A}$</td>
<td>$\rightarrow$</td>
<td>$Q_B = S^{2R_B}$</td>
</tr>
<tr>
<td>Key Exchange</td>
<td>$K = Q_B^{2R_A}$</td>
<td>$K = Q_A^{2R_B}$</td>
</tr>
<tr>
<td>Abort if $K &lt; 2$</td>
<td></td>
<td>Abort if $K &lt; 2$</td>
</tr>
<tr>
<td>Verification</td>
<td>$V_2 = h(K)$</td>
<td>$\rightarrow$</td>
</tr>
<tr>
<td>Abort if $V_1 \neq h(h(K))$</td>
<td>$\rightarrow$</td>
<td>Abort if $V_2 \neq h(K)$</td>
</tr>
</tbody>
</table>
Security Services Implemented

• Remote Connection Manager

• Public Key Infrastructure (PKI based Services)
  • Certificate Authority
  • Certificate Distribution System

• Key Manager
Certificate Authority

- Provides identification to users and daemons
- Issues X509 digital certificates to users & daemons
- Revokes the user / daemon certificate when necessary
  - Creates a CRL for all the certificates revoked
- Notifies the issued & Revoked Certificates to the Certificate Distribution Daemon
Certificate Distribution System

- Function: To distribute all valid user / daemon certificates
- Answers queries from ACE services regarding validity of certificates
- Publishes the list of valid certificates and the Certificate Revocation List (CRL) on a publicly accessible LDAP service
ACE Root Certificate

- Same Issuer and Subject
- Essentially a self signed Certificate
- Signature Algorithm: md5withRSA
- Thumbprint Algorithm: sha1
ACE Certificate Revocation List

Certificate Revocation List Information

Field | Value
--- | ---
Version | V2
Issuer | Research & Development, ACE:
Effective Date | Wednesday, May 08, 2002 4:34:22 AM
Next Update | Tuesday, May 07, 2002 4:32:30 AM
Signature Algorithm | mc5RSA

Value:
OU = Research & Development
CN = ACE: ITTC Domain
T = Certificate Authority
C = USA
L = Lawrence
E = ace@ittc.ku.edu
O = University of Kansas

Certificate Revocation List

Revoke certificates:

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Revocation Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>Wednesday, May 08, 2002 4:34:22 AM</td>
</tr>
</tbody>
</table>

Revoke entry:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>03</td>
</tr>
<tr>
<td>Revocation Date</td>
<td>Wednesday, May 08, 2002 4:34:22 AM</td>
</tr>
</tbody>
</table>

Value:
Wednesday, May 08, 2002 4:34:22 AM
Security Services Implemented

• Remote Connection Manager

• Certificate Authority

• Certificate Distribution System

• Key Manager
Key Manager

- Service that issues cryptographic keys to services
- Supports of a wide variety of cryptographic algorithms
- Keys may be used as:
  - One time session
  - Conference
- All issued keys are stored in a PBE encrypted keystore
Typical Scenarios

• Remote Authentication

• Certification Process
### Possible Remote Authentication Procedure

| Send Prime Number P signed with RCM Private Key | Contact LDAP Service, verify the Prime P and compute Key
| Send h(h(k)) | Send h(k) |

**Remote Connection Manager**

**LDAP Service**

**Standalone application**
## Remote Authentication Process

<table>
<thead>
<tr>
<th>Send List of Protocols</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Send the chosen protocol (SPEKE), the User Name, a prime number P and the calculated Value</td>
<td></td>
</tr>
<tr>
<td>Verify Prime P properties, Calculate the Key K and send h(h(k))</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Remote Connection Manager**
- **Standalone application**
Certification Process

ACE Users & Daemons

Request Certificate
Issue Certificate

ACE Certificate Authority

Revoke Certificate

LDAP Service

Throws a notification of the Certificates (Issued and Revoked)

Certificate Distribution System

Admin

Publish Certificate & CRLs
Analysis

1. What problem are we trying to solve?
   - User and Daemon identification
   - User Authentication (Remote)
   - Secure Communications

2. How effective is the proposed solution?
   - X509 Digital Certificates
   - Password / IButton ID / Fingerprint ID
   - Standard encryption
3. What new problems have been added?

- Addition overhead of managing a limited PKI
- Additional vulnerability to social engineering problems
  - Passwords can be changed once a compromise is detected
  - Not true with IButton and Fingerprint data
- Extraneous issues!
  - Java
  - API calls & Key lengths
Summary

- The following services have been prototyped in this thesis
  - A Rudimentary Key Manager
  - A Certificate Authority
  - A Certificate Distribution System
  - A Remote Connection Manager
- But then ……Security is a process, not a product.
Future Work

- Implement a $(m,l)$-threshold b-secure t-group key distribution scheme
  - Number of centers: $m$
  - Minimum number of centers required: $l$
  - $(l-1)$ center & $b$ user compromise doesn’t compromise the system

- Better storage system for CA Keys and Certificates
Questions ?
## X.509 Digital Certificate Fields

<table>
<thead>
<tr>
<th>Certificate field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The X.509 version number.</td>
</tr>
<tr>
<td>Serial number</td>
<td>The unique serial number that the issuing certification authority assigns to the certificate. The serial number is unique for all certificates issued by a given certification authority.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>The hash algorithm that the certification authority uses to digitally sign the certificate.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Information regarding the certification authority that issued the certificate.</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the individual or certification authority to which (whom) the certificate is issued. This may be a full name and e-mail name or some other personal identifier.</td>
</tr>
<tr>
<td>Public key</td>
<td>The public key type and length associated with the certificate.</td>
</tr>
<tr>
<td>Thumbprint algorithm</td>
<td>The hash algorithm that generates a digest of data (or thumbprint) for digital signatures</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>The digest (or thumbprint) of the certificate data.</td>
</tr>
</tbody>
</table>
## SPEKE Vs DH-EKE

<table>
<thead>
<tr>
<th>Constraint</th>
<th>Prevents Attack by:</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>modulus p is huge</td>
<td>discrete log attack</td>
<td>D S</td>
</tr>
<tr>
<td>test Q&lt;sub&gt;x&lt;/sub&gt;: != 0, when un-encrypted</td>
<td>forcing K=0</td>
<td>D S</td>
</tr>
<tr>
<td>p-1 has large prime factor q</td>
<td>Pohlig-Hellman log computation</td>
<td>D S</td>
</tr>
<tr>
<td>encrypted Q&lt;sub&gt;x&lt;/sub&gt; randomly padded.</td>
<td>leakage from E&lt;sub&gt;S&lt;/sub&gt;(Q&lt;sub&gt;x&lt;/sub&gt;)</td>
<td>D</td>
</tr>
<tr>
<td>base is primitive root of p</td>
<td>partition attack on E&lt;sub&gt;S&lt;/sub&gt;(Q&lt;sub&gt;x&lt;/sub&gt;)</td>
<td>D</td>
</tr>
<tr>
<td>base is a generator of q</td>
<td>partition attack on Q&lt;sub&gt;x&lt;/sub&gt;</td>
<td>S</td>
</tr>
<tr>
<td>base = S&lt;sub&gt;x&lt;/sub&gt; mod p</td>
<td>password-in-exponent attack</td>
<td>S</td>
</tr>
<tr>
<td>first receiver of verification of K must encrypt Q&lt;sub&gt;x&lt;/sub&gt;</td>
<td>finding password S using chosen R&lt;sub&gt;x&lt;/sub&gt;, Q&lt;sub&gt;x&lt;/sub&gt;, E&lt;sub&gt;K&lt;/sub&gt;(x) and password dictionary</td>
<td>D</td>
</tr>
<tr>
<td>use one-way hash of K</td>
<td>narrowing attacks</td>
<td>D S</td>
</tr>
<tr>
<td>high bits of p must be 1</td>
<td>partition attack on E&lt;sub&gt;K&lt;/sub&gt;(Q&lt;sub&gt;x&lt;/sub&gt;)</td>
<td>D</td>
</tr>
<tr>
<td>Receiver of clear Q&lt;sub&gt;x&lt;/sub&gt; abort if K is small order. or Encrypt Q&lt;sub&gt;A&lt;/sub&gt;, Q&lt;sub&gt;B&lt;/sub&gt;</td>
<td>subgroup confinement of K</td>
<td>D</td>
</tr>
<tr>
<td>Abort if K has small order</td>
<td>subgroup confinement of K</td>
<td>S</td>
</tr>
</tbody>
</table>
Navigation

- ACE Entities
  - Services
  - Users
- Services
  - Remote Connection Manager
  - Certificate Authority
    - Certificate
    - Certificate Revocation List
  - Certificate Distribution System
  - Key Manager
- SPEKE
- Diffie-Hellman
- Scenarios
  - Remote Authentication
  - Certification
- Analysis
- Distributed Key Manager