Security Tools Area Overview, Credential Management Services, and the PKI Testbed

Jim Basney
Senior Research Scientist
jbasney@ncsa.uiuc.edu
## Security Tools Area

<table>
<thead>
<tr>
<th>WBS No.</th>
<th>Project Title</th>
<th>Technical Lead</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Research Thrust: Security Tools</td>
<td>J. Basney</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.1</td>
<td>DC_Key Management</td>
<td>Khurana</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.2</td>
<td>Credential Management Services</td>
<td>Basney</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.3</td>
<td>Continuous Hardware Component Validation (CHCV)</td>
<td>Brown</td>
<td>PNNL/Battelle</td>
</tr>
<tr>
<td>2.4</td>
<td>Trusted Computing Exemplar (TCX)</td>
<td>Irvine</td>
<td>NPS</td>
</tr>
<tr>
<td>2.5</td>
<td>Multicast Survivability and Security</td>
<td>Yurcik</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.6</td>
<td>Cluster Security as an Emergent Property</td>
<td>Yurcik</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.7</td>
<td>Malicious Code Reverse Engineering and Analysis (MCREA)</td>
<td>Onderkirk</td>
<td>PNNL/Battelle</td>
</tr>
<tr>
<td>2.8</td>
<td>Secure Middleware/Services for Wireless Sensor Networks</td>
<td>Khurana, Welch</td>
<td>NCSA</td>
</tr>
<tr>
<td>2.9</td>
<td>Cryptographic Key Management System</td>
<td>Kimmel</td>
<td>InfoAssure, Inc.</td>
</tr>
</tbody>
</table>
Credential Management Services Project

• Goal: Provide secure, convenient access to security credentials for authentication, digital signatures, and encryption

• Approach: Develop open source software providing credential management services

• Results: SACRED credential repository implementation at http://sacred.sf.net/
  – Developed in collaboration with BYU
SACRED Credential Repository

• Securely Available Credentials (SACRED) Protocol (RFC 3767)
  – Published June 2004
• Enables user to acquire cryptographic credentials from a credential server
  – Authenticate with a password
• Authentication protocols now supported:
  – SASL DIGEST-MD5 (RFC 2831) over TLS
  – SASL SRP (RFC 2945)
SACRED: Next 6 months

- Community outreach: encourage adoption
  - Target grid computing community
  - Improve web site and documentation
- Develop graphical user interface
- Integrate with Mozilla web browser and email client
- Improve server configuration and management
PKI Testbed Project

- Started January 2005
- Equipment to be acquired:
  - Contact and contactless smartcards and readers
  - Fingerprint readers
  - iButtons, SecureID tokens, CRYPTOCard tokens
  - Secure co-processors for credential servers
  - Servers, laptops, workstations, and PDAs
- To support:
  - Credential Management Services Project
  - ITTF Credentialing Project (external collaboration)
  - Other NCASSR projects? (Please contact me.)
Illinois Terrorism Task Force

• Mission
  – Created May 2000 to implement a comprehensive coordinated strategy for domestic preparedness in the state of Illinois, bringing together agencies, organizations, and associations representing all disciplines in the war against terrorism.

• Members include:
  – American Red Cross
  – Associated Fire Fighters of Illinois
  – FBI
  – Illinois Governor’s Office
  – Illinois State Police
  – U.S. Attorney’s Office
  – FEMA (Region V)
ITTF Credentialing Project

• Goal: Pre-issue credentials to incident responders for identification and tracking at the incident perimeter
  – Smartcards printed with photo ID
  – Electronic authentication includes:
    • Fingerprint biometric
    • Identity certificate issued by State of Illinois PKI
    • Signed certifications (team, weapons, hazmat)
ITTF System Components

- **Secure Web Portal**
  - Enroll team members and manage certifications
  - Activate credentials and update credential data

- **Card Management System**
  - Print and issue cards

- **Field Application**
  - Laptop with smartcard/fingerprint reader
  - Verify identity with photo and fingerprint scan
  - Confirm certifications
  - Track incident check-in/check-out
ITTF Project Scope

- 5,000 initial credentials for pilot project
- Plan to grow to 100,000 credentials
  - Every Illinois firefighter, police officer, EMT
  - Pre-certified volunteers (Red Cross, etc.)
- Design for general-purpose statewide use
  - Secure building and computer system access
  - Interoperability with Federal standards
ITTF Project Roles

• ITTF: project management
• Entrust: main project contractor
• University of Illinois at Chicago: smartcard requirements development
• NCSA: acceptance testing and consulting on system design