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

Jim Basney
Senior Research Scientist
jbasney@ncsa.uiuc.edu

Security Tools Area

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

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

- Misson
  - 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