MITHRIL:
Adaptable Security for Survivability in Collaborative Computing Sites

Jim Basney, Patrick Flanigan, Jin Heo, Himanshu Khurana, Joe Muggli, Meenal Pant, Adam Slagell, Von Welch

National Center for Supercomputing Applications
Mithril

- ONR-funded project under the National Center for Advanced Secure Systems Research

- Mithril is a fictional material from J.R.R. Tolkien's universe, Middle-earth. It is a precious silvery metal, stronger than steel but much lighter in weight. (from Wikipedia)

- A mithril coat of mail provides strong protection but is light and flexible

- Our project provides adaptable site security mechanisms that maintain usability
Collaborative Computing Sites

Examples
- NRL CCS, NSF centers (NCSA, SDSC, PSC, NCAR), DOE Labs (NERSC, LBNL)

Characteristics
- Enable pooling of distributed resources
- Provide a variety of general-purpose and specialized computing services
- Support large, geographically distributed user communities
  - NCSA has 7000+ users from all over the world

Threats
- Determined, skilled adversaries and script kiddies
- Open nature of services
Challenges for Site Security

- Contention between openness, usability and control at user level
  - Services accesses via Internet => open nature
  - Off-site user machines => lack of control
  - Limited user security knowledge => need usable tools

- Performance and efficiency of site security mechanisms

- Compatibility of security tools with site software systems
  - Neither commercial tools nor research tools work

- Limitations of current site security mechanisms
  - Demonstrated by cyber attack of 2004 - Incident 216
Incident 216: Cyber Attacks of 2004

- Series of attacks against a number of sites - DOE, NSF, commercial, Universities

- Attacker compromised hosts, installed SSH trojans, and collected usernames and passwords
  - Was careful not to otherwise disturb system so went undetected to a large degree

- Used usernames and password to gain access to NCSA and other places, then other vulnerabilities to escalate privileges, install SSH trojan and repeat
Mithril Approach

- Adaptable site security mechanisms to ensure survivability
  - Raise security levels when needed, but only temporarily
  - Ensure continuity albeit at reduced levels
    - E.g., 85% of cycles are used by top ten PI’s at NCSA

- Architecture components for survivable security
  - Core management system: Prelude
  - Prevention tools: E.g., SSH authentication
  - Detection tools: E.g., Bro IDS, SEC correlation
  - Response tools: E.g., Secure Mailing Lists, Cfengine

- Case Studies (Incident 216)
  - Resolve account compromise by combining OTP with SSH remote agent
  - Resolve email compromise with Secure Email List Services (SELS)
Mithril Architecture

- Response Policy
- Correlation Rules
- Responses
  - cfEngine
  - Applications
    - SELS
    - SSH/PAM
    - Krb/PAM
    - IP Firewall
- Prelude
  - Prelude DB
    - Events
  - Logs
  - Sensors
    - bro
    - snort
    - syslog
- NCSA Systems

prewikka UI

LibPrelude
Managing Remote Login Services

- Remote login is arguably the most essential service provided by collaborative computing sites.

- SSH is very configurable site access control point:
  - Wide variety of authentication mechanisms
    - SSH public key authentication provides single sign-on
    - Many options for security restrictions

- SSH keys can be difficult to manage, leading to potential account compromise:
  - Keys scattered onto multiple machines
  - Unencrypted or encrypted with poor passwords
  - No lifetime restrictions, no revocation capability
Case Study I: Addressing account compromise

**SSH Remote Agent**
- Private keys generated and stored on locked-down key server, public keys distributed; provides revocation capabilities
- Authentication uses ssh-agent protocol link to server that retains private key
- Policy control via prelude toggles between password, OTP, and non single-sign on OTP depending on perceived threat
Case Study II: Secure Email Services

- Needed for intrusion detection and coordinating intrusion response
  - Monitoring and IDS processes send alerts via email
  - Need for system administrators to communicate securely (signed, encrypted) across-site when under ongoing attack
  - Need intrusion tolerant system so attackers can’t eavesdrop

- SELS: Secure Email List Services
  - Solution developed under NCASSR program with deployability and usability in mind
  - Provide encryption and signature support for Mailing Lists
  - Use GPG at client, Mailman plug-in at List Server
SELS: Secure Email List Services

Key Store: Members’ corresponding private keys $K'_{Ui}$

Key Store: (SK$_S$, PK$_{LK}$)

Sensor

Encrypt $(m,\text{Sig}(m))$ w/ $k$

Email Header

Encrypt $(k)$ w/ $PK_{LK}$

List Server

Email Plaintext $m$

Sig$(m)$ w/ $SK_S$

Key Store: (PK$_S$, SK$_A$)

Admin

Encrypt $(m,\text{Sig}(m))$ w/ $k$

Email Header

Transform $k$ W/ $K'_{A}$
(SELS Proxy Re-encryption)

Email Plaintext $m$

Sig$(m)$ w/ $SK_S$
Future Work

- Integration with NCSA’s systems for scalability testing

- Questions?

- Email: hkhurana@ncsa.uiuc.edu, vwelch@ncsa.uiuc.edu

- Project URL: http://security.ncsa.uiuc.edu/research/mithril/

- Work funded by ONR as part of NCASSR
  - http://www.ncassr.org