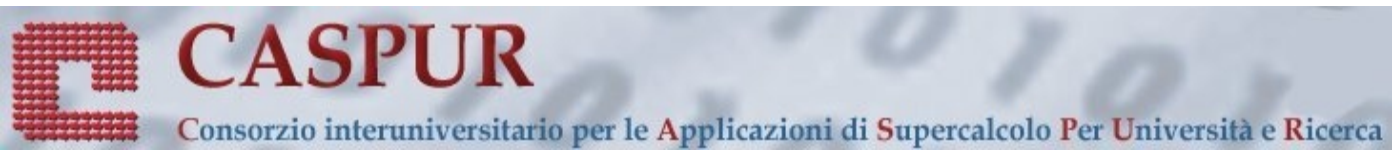
One-Time Password Integration at BNL

HEPiX at CASPUR
Spring 2006

Robert Petkus

RHIC/USATLAS Computing Facilities
Brookhaven National Laboratory



SSO – Current AA Structure (Authentication/Authorization)

Kerberos 5 authentication

- AFS token via klog or TGT+aklog
- SSH Authentication (AFS token via TGT+PAM)
  - PAM (via KRB5 password)
  - GSSAPI via TGT
- HTTP authentication with AuthPAM and WebAuth
- Subversion authentication via Apache w/mod_auth_kerb

SSH Keys (limited use)

- ssh-agent and authorized_keys
- Host-based authentication (!)

LDAP authorization

- System login access control
  - pam_check_service_attr, pam_check_host_attr

SSO With Kerberos

Benefits

- Single sign-on
- Strong mutual authentication using secret-key cryptography
- Cross-realm authentication
- User management
- Relatively mature implementation (compared to other systems)
- Industry adoption (e.g., Microsoft/Linux/Solaris)

Issues

- Impersonation with stolen password (keystroke logging)
- A compromised host allows user impersonation for the lifetime of their tickets
- A compromised KDC compromises all user accounts in the realm

SSO with SSH Keys

Benefits

- Single sign-on using keys
- Data encryption
- Secure TCP/IP tunneling

Issues

- Stolen passphrase (keystroke logging)
- Impersonation with stolen password (keystroke logging) or replaced credentials
- Copies of SSH keys
- Difficult to enforce passphrase policy (sensible passphrases, expiration)

One-Time Passwords

Why use One-Time Passwords (OTP) ?

- Relieve problems inherent in re-usable passwords
  - OTP expire the first time they are used
  - Reduce compromised user credentials
  - Can't snarf user passwords
  - Lost passwords – same passwords for all services
- Hard token/Smartcard: Two-factor authentication & one-time passwords

Many Implementations

- S/KEY
- OPIE
- OTP-PKCS#11
- Biometric
- CRYPTOCard, eToken, etc.

One-Time Passwords, continued

Issues

- User education
- Users at different OTP-enabled institutions may be forced to carry around multiple hardware tokens
  - Solution is integration within a larger authentication fabric
    - PMA (Regional Policy Management Authorities)
      - ESnet, DOEGrids
    - Federations – inter-realm trust
    - DOE One-Time Password Federation
    - Radius Authentication Fabric (project status?)
    - Internet 2 / Shibboleth
- Use of OTP results in loss of SSO
  - Solution is for a KRB5 TGT or Grid proxy serve an authentication token with a finite lifetime that can be used instead of the OTP

One-Time Password Integration at the RCF/ACF

Components

- Radius server
- CRYPTOCard (CRYPTO-Server + hard and soft tokens)
- GSI-enabled OpenSSH
  - http://grid.ncsa.uiuc.edu/ssh
- MyProxy (Credential Management Service)
  - http://grid.ncsa.uiuc.edu/myproxy/
- GUMS (Grid User Management System)
  - http://grid.racf.bnl.gov/GUMS/
- Certificate Authority (Globus SimpleCA)
- pam_myproxy_logon (in-house development)
- gssklog (obtain an AFS token using a GSS implementation)

Internal system
with GSI-Enabled
SSH Server

CRYPTOCard
Server

RADIUS Server

pam_myproxy_logon

SSH Gateway
MyProxy Server
GUMS client

GUMS Server

End User

One-Time Password Integration at the RCF/ACF

Pros

- Easy integration into our current architecture (GRID, AFS, FTP, archival storage; e.g., pFTP, HSI, SSH, batch processing)
  - CRYPTOCard
  - Hardware token
  - Two-factor authentication & one-time passwords
  - Challenge-response

Cons

- Cost – CRYPTOserver and CRYPTOCards
- MyProxy protocol
  - No challenge-response (in-house development)
  - Synchronization issues
- Soft tokens not as secure
- CRYPTOCard export issues – use of software tokens?
- GSI-enabled OpenSSH requires a second GSSAPI back-end

Conclusion / Considerations

- Hard tokens = $$$
- A well architected OTP solution will reduce the chance of compromised user credential
- OTPs are perhaps better integrated into Kerberos
  - Instead of using MyProxy, CRYPTOCard is embedded into the KDC.
  - Compatible with stock SSH
  - Can pam_krb5 handle OTP?
  - Since Kerberos is strong authentication, OTP will likely require 2 hardware tokens for each RHIC and USATLAS at BNL.
    - MyProxy can use GUMS to map same CRYPTOCard to different accounts on RHIC and ATLAS gateways.
- How can Kerberos integrate into a GRID-based environment?
  - MyProxy backended with Kerberos? Should work in theory.
  - KCA

Conclusion / Considerations, continued

- Integration of OTP and web inter-domain SSO
  - Globus-Shibboleth (GridShib)?
  - OTP-WSS-Token
- Re-usable passwords appear to be a current vulnerability vector and as a result the days for re-usable passwords are probably numbered.
- Is OTP even an issue at other sites?
- Will collaborating institutions participate in cross-realm authentication.? Are various OTP implementations compatible in such an authentication fabric? What are the trade-offs?