CESNET 2008

Survey of Authentication Mechanisms for Grids

Daniel Kouřil, Luděk Matyska, Michal Procházka

Outline

- Introduction

- PKI
- Kerberos
- Identity Federations
- Passwords

- Credential Transitions
- Conclusion

Introduction

- Security problems in Grids
  - Grids are fully decentralised
  - Data flows across multiple components, organizational domains
  - Data are not under control of the data owner
- Grids are usually bound with only one authN mechanism
  - AuthN mechanisms at local sites can be various
- Users are confused about various types of authN mechanisms
  - It is not flexible, convenient and safe
- Automatic translation
  - Promise solution

PKI

- Based on asymmetric cryptography – public and private keys
- Does not require pre-distributed secret
- Usable in loosely-coupled distributed environment
- Plain key-pair
  - SSH
  - Missing identification information and revocation functionality
- PKIX
  - X.509 certificates used to identify holder of the key
  - Mechanism to maintain keys (issuing, revokeing, ...)
- PGP
  - Does not require centralized authorities
  - Users build their own Web of trust

PKI in Grids

- PKIX is widely used in todays Grids
- UNICORE case
  - Jobs are signed by the user's private key
- Proxy certificate
  - Proxy certificate signed by the user's private key
  - Supports delegation
  - Supports SSO
  - Lack of revocation and support for long jobs
- Complicated for the user
  - Private key file handling

Kerberos

- Central aunthetication service - KDC
- Each authN request involves contacting KDC
- Supports SSO
- Scalability problems – cross-realm support
- Does not scale even if cross-realm is used
- Suitable for local authN for sites
- Not suitable for Grid

Identity Federations

- Very popular recently
- Consists of IdP and SP
- User management is at the users' institutions
- Does not rely on specific authN mechanism
- Users use only their ”home” credentials
- Support for authorization based on attributes
- Web environment only

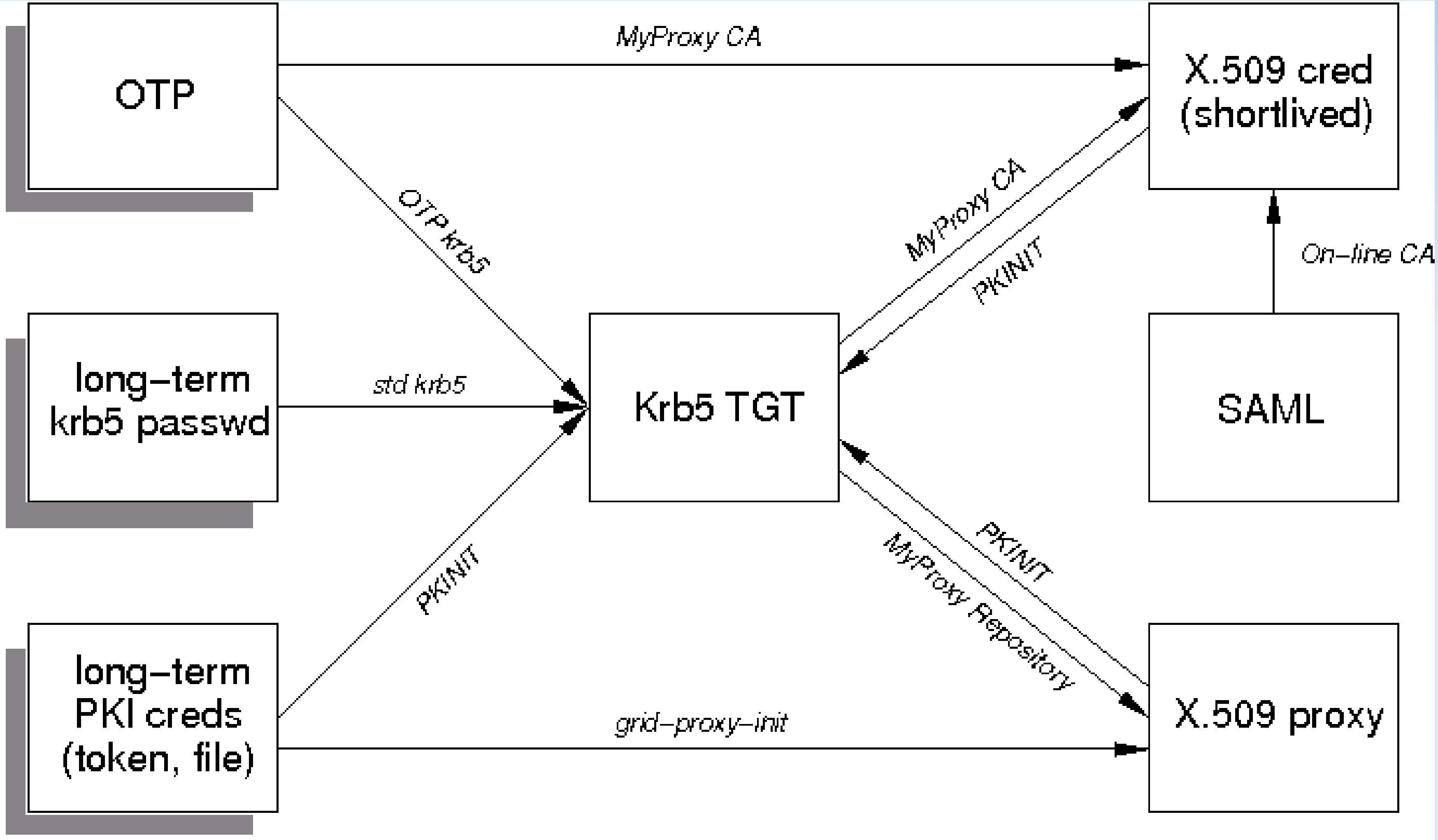
Identity Federations and Grids

- GridShib
  - Globus <-> Shibboleth
  - Federated Online CA
  - Push and Pull mode
- ShibGrid
  - Used at NGS – UK
  - Uses MyProxy CA
  - Two modes of operation
    - Users with UK eScience certificate – client app.
    - Other users – portal uses autogenerated proxy cert.

Passwords

- Very often used
- Does not support SSO
- Initial authN in Grids
  - MyProxy, proxy certificate, Kerberos
- OTP
  - Secure even in untrusted environment
  - Special devices generating OTP

Transition of authN mech.



Transition of authN mech.

- User can choose from various authN
- Easy to use => safer
- Types of transition
  - OTP -> X.509
  - OTP -> Kerberos
  - Kerberos -> X.509
  - SAML -> X.509
  - X.509 -> Kerberos

Transition of AuthN mech.

- OTP → X.509
  - MyProxy server in CA mode
  - OTP PAM authentication module
  - Two PAM modules implementing two OTP mechs.
  - Java client application which can be loaded into the mobile device
- OTP → Kerberos
  - IETF Draft
  - Not yet implemented

Transition of AuthN mech.

- Kerberos → X.509
  - Users do not need to learn how PKI works
  - Transparently obtain X.509 certificate
  - KCA
    - Supports only this type of transition
  - MyProxy CA
    - Supports another authN methods and modes

Transition of AuthN mech.

- SAML → X.509
  - Online CA as an SP in federation
  - Attributes as an extension in the X.509 certificate
  - GridShib
    - Java applet which stores new certificate on the computer
  - Web based Online CA
    - The key-pair is generated inside the browser
  - CAT
    - Uses web based Online CA
    - Provides certificate management in Windows OS

Transition of AuthN mech.

- X.509 → Kerberos
  - IETF standard PKINIT
  - X.509 used to obtain TGT
  - First open source implementation was contributed by CESNET developers to the Heimdal implementation of Kerberos
  - Current Heimdal also supports proxy certificates
- Transitive transition

Conclusion

- Overview of today's authN mechanisms used in Grids
- Posibility of transition among authN mechs.
- We have tested all transitions methods mentioned before
- and we have contributed to development of several components and mechanisms

This is the end ...