Authentication

Technologies in use at HEP

Wolfgang Friebel

Introduction

- Talk aims to review what has been achieved

Major areas of work

- Generic auth mechanisms (PAM, SASL, ...)
- Kerberos (4 and 5)
- Public key infrastructure (PKI)
- Single sign on (SSO)
- Password synchronization across architectures

Overview of Authentication in HEP

To not repeat what has been presented already:
create a central place of information for

- pointers to talks held at HEPiX
- recipes for dealing with the different mechanisms
- getting access to what has been developed by different sites (programs, patches, frameworks, ...)

Available information

I started to collect those info in a web page:

- http://www-zeuthen.desy.de/~friebel/hepix/auth
- it is a WIKI, you can (and should) contribute
- needs consolidation, a permanent place (plone?), a maintainer (volunteers?)

What is needed

- More on certificates
- More on Windows
- Resources from other sites
- ...

Problems and remarks

Just a few slides to point to some problems and give my opinion...

Generic authentication

- API's and libraries do exist in UNIX and Windows
- no single method covering all areas
- PAM is for local authentication (in UNIX)
- SASL is the equivalent for client/server applications
  - GSSAPI is one of the supported SASL plugins
  - used in cyrus-imap, sendmail, openldap, arcx, ...
  - usually comes with the OS, easy to use, powerful
- application specific modules (e.g. apache)

PAM and other generic methods

- problems during the practical use, e.g.
  - AFS and authentication using PAM modules
    - Redhat Kerberos PAM module does not generate tokens from forwarded tickets (ssh)
    - Other module (http://sourceforge.net/projects/pam-krb5) better, but no longer maintained?
  - authentication in UNIX/Linux easy with SASL, but
    - need also to deal with proofs of authentication within app:
      - already S/MIME support in pine painful
      - Kerberos5 support in batch not simple,...
  - SPNEGO support in Mozilla/Firefox not user friendly
- => continous source of interoperability problems

Kerberos

- Much work done, e.g. FNAL, INFN, CERN, DESY

but

- few sites have interoperability UNIX/Windows
- if SSO is the goal, only Windows can hold the combined database (this is not the fault of K5)
- hard to get SSO, many applications insist in (re)auth with password despite of valid K5 ticket

PKI

- The move to grids (e.g. LCG) made this extremely important
- becoming favored authentication method?
- => watch this track of talks

Single Sign On

- good for administrators (centralized and consistent handling of authentication, user registration etc.)
- Centralized user and password registry (DESY) has similar effects
- is it good for users too? (or: how often do you need to type in passwords?, how many passwords do you need anyway for bank accounts, internet providers, ...)
- especially dangerous if weak protocols are involved (remember Bob Cowles' demos?)

  => CERN is banning clear text auth (H. Meinhard)

Comments ?
Questions ?

and please contribute to

http://www-zeuthen.desy.de/~friebel/hepix/auth