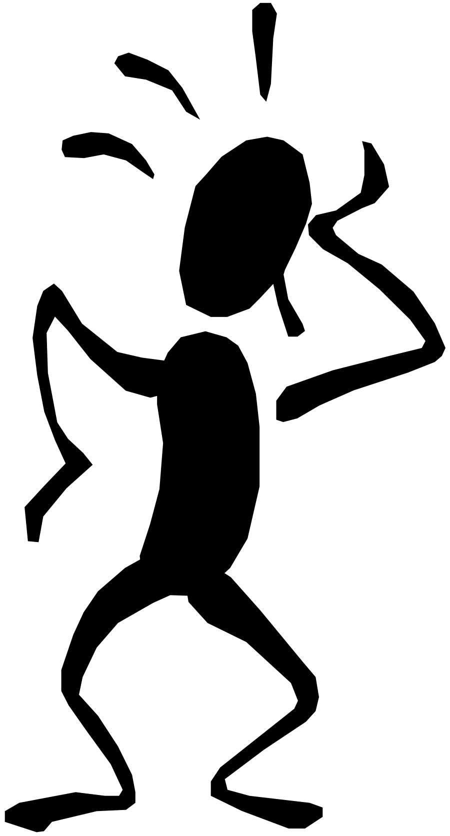
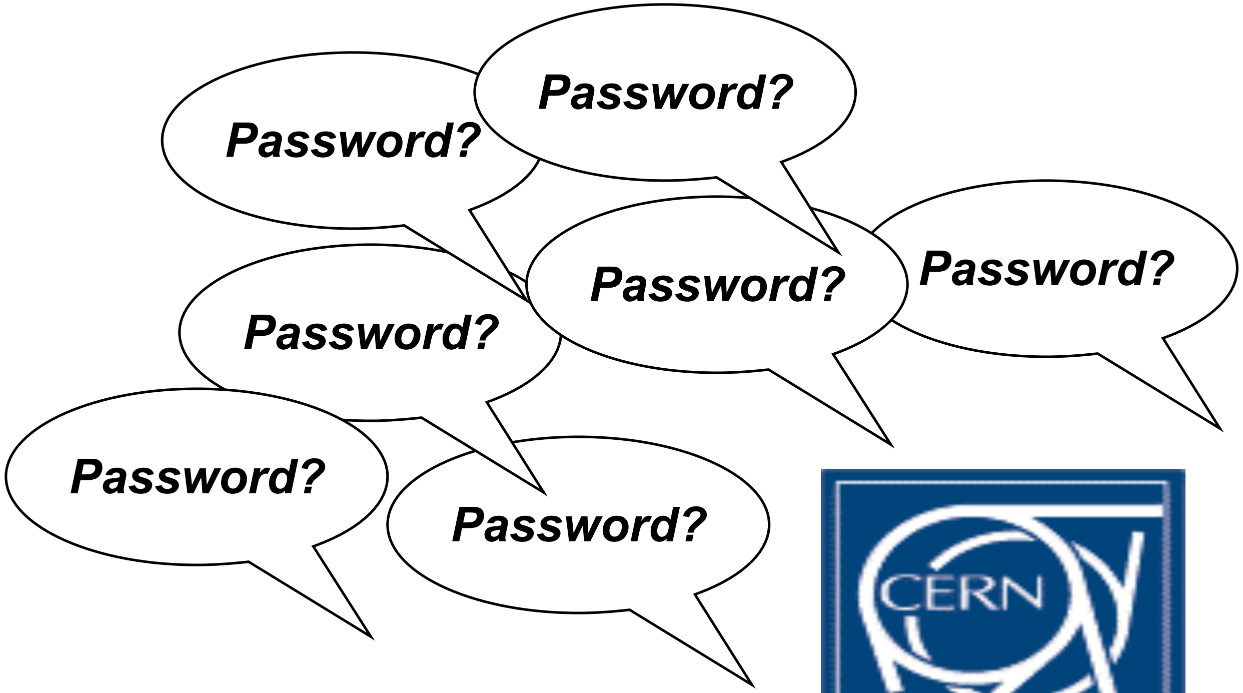
CLASP Project

AAI Workshop, 20-21 Nov 2000

Denise Heagerty, CERN



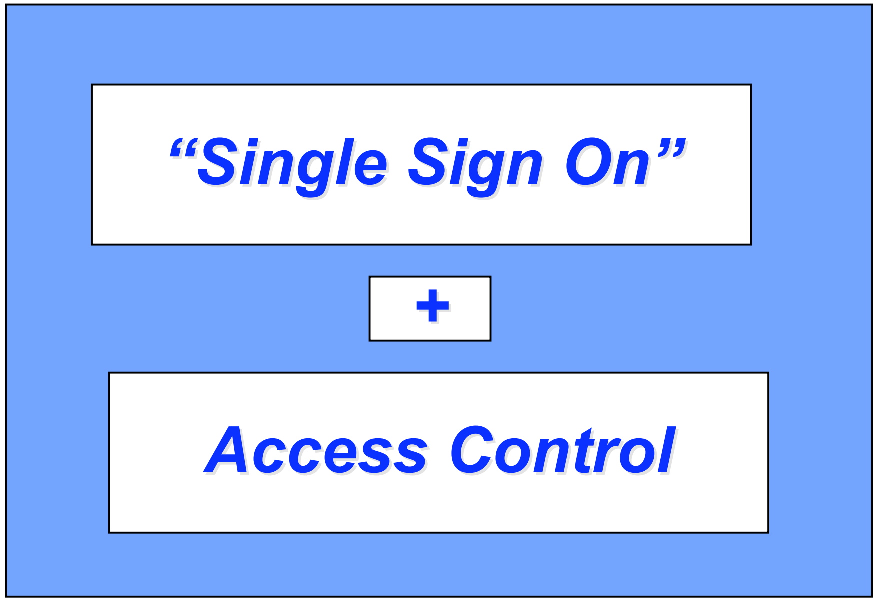


Outline

- Project goal
- Feasibility study results
- Key applications
- Kerberos v5 advantages
- Smart cards
- Platform independent access control
- Next steps for the project

Project Goal

- Propose a detailed plan to reduce the number of login/passwords entered by users to access services they are authorised to use



“Single Sign On”

+

Access Control

Feasibility Study Results

- Kerberos v5 provides a good basis for common authentication and Single Sign On
  - available in W2000, Linux RH v6.2, Solaris 8
  - standard application interfaces (RFC 2078, MS-SSPI)
- Some PKI (Public Key Infrastructure) is required for GRID applications
  - Can be integrated with Kerberos v5 Single Sign On
- Enhanced security is essential
  - to overcome the vulnerability of the initial sign on
- We need to control the explosion of web loginid/password pairs
  - need to consider non-Kerberos solution

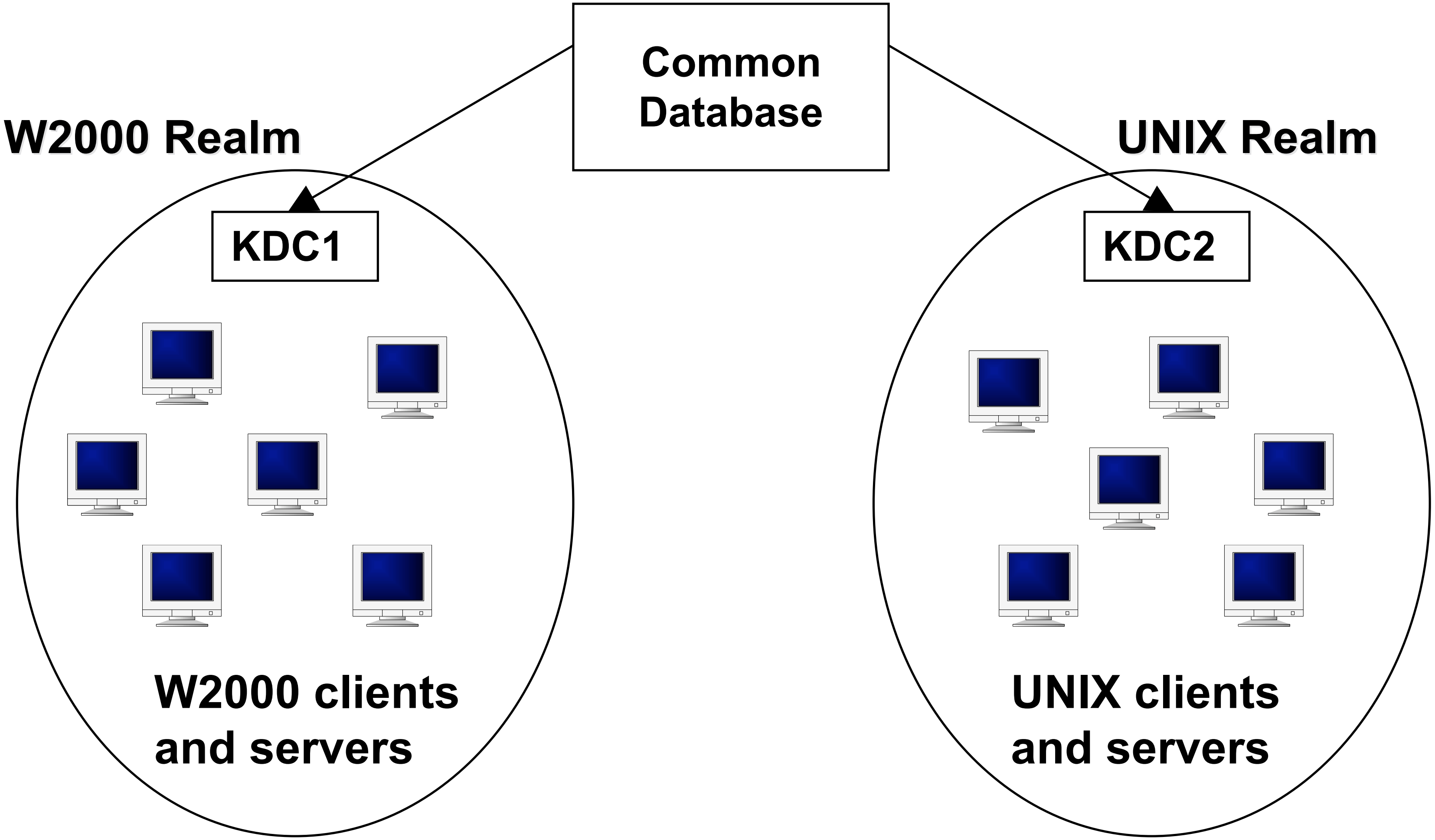
Key applications known to support Kerberos v5

- Mail
  - IMAP server (U of Washington) - Yes!
  - Outlook and Pine - Yes!
  - Netscape - No
- Interactive Commands
  - telnet, ftp, rcp, rlogin: UNIX - Yes! / W2000 - Yes?
  - Exceed: Yes!
- File Access (single platform)
  - AFS - Yes (via Kerberos v4 extension on UNIX KDC)
  - Microsoft DFS: W2000 - Yes!
- Web
  - Internet Explorer - Yes
  - Netscape - No

Kerberos v5 Advantages

- Common authentication technology across W2000 and UNIX platforms
  - can focus expertise on a single protocol
- A basis for cross-platform Single Sign On
  - Requires kerberized applications
- Allows authentication agreements with trusted remote sites
  - using cross-realm authentication
- Integrates with GRID Single Sign On
  - Proxy certificates generated from Kerberos TGTs
- Integrates with PKI
  - PKINIT: from a certificate you can obtain a TGT

Kerberos Realms



Common Database

W2000 Realm

UNIX Realm

KDC1

KDC2

W2000 clients and servers

UNIX clients and servers

Smart Cards

- can store a user certificate and private key
  - protected by a PIN code, normally requested each time the certificate is used
  - Could be combined with new CERN physical access cards (at extra cost for the chip and writer)
  - UBS smart card could be used for CERN authentication
  - Globus works with Netscape on a PC (PKCS#11)
- readers connect to PCMCIA, serial, USB ports
- integrates with Kerberos v5 using PKINIT
- early technology - compatibility problems
- Not a general solution for off-site access
  - requires card readers at all remote sites and systems

Platform-Independent Access Control

- **Centrally defined “e-groups”**
  - electronic grouping of people/accounts
  - defined centrally and made available to applications
  - web interface with access to personnel database
  - LDAP / Active Directory play a key role
- **Key/Initial applications:**
  - e-mail distribution lists
  - web page protection
  - file protections

Next Steps

- Implementation plan for the base authentication service (Feb 2001)
  - Kerberos v5 with support for AFS/v4 and certificates
- Implementation plans for services (Feb2001)
  - mail, web, interactive (login, telnet, ftp, Exceed, ssh), file (AFS, Windows DFS), batch (LSF), Oracle and future GRID services
- Final Recommendations (May 2001)
  - security review, password (check and change) policy, opt-out mechanism, off-site access, platform independent access control for web pages, files and email lists

http://cern.ch/proj-clasp

CLASP studies have been made in collaboration with many colleagues both inside and outside CERN - Thanks!