



Strong Authentication at FNAL

Goals
Design
Status


Philosophy

"Scientific thinking and invention flourish best where people are allowed to communicate as much as possible unhampered."


-- Enrico Fermi



Goals

- 
- **Prevent disclosure of login passwords.**
 - Meet DOE expectations
 - ◆ Exercise due diligence to prevent unauthorized use of lab computers
 - ◆ Keep track of who is using lab computers
 - Secondary -
 - ◆ Provide a single-signon environment.
 - ◆ Simplify account management, especially terminations - take this burden off the system administrators.
 - ◆ Integrate AFS accounts & systems.
 - ◆ Enforce password policies.

Non-Goals

- 
- Perfection.
 - Solution of all computer security threats
 - ◆ OS patches will still be necessary
 - ◆ Social engineering still can subvert the system



Design Criteria


- Allow the work of the Laboratory to get done.
- Requiring some change in habits is acceptable. Radical changes would hinder successful deployment.
- Users without special software or hardware on their systems must be provided some way to authenticate.
- Systems that cannot be modified must be accommodated without compromising the principles of Strong Authentication
- Must be adaptable to changes in
 - ◆ System security requirements
 - ◆ Computing styles

What

- Separate authentication (who you are - centralized) from authorization (what you are allowed to do - local)
- Lab computers that are accessible from the outside internet will not allow password based remote logins, commands or file transfer
- Usage is only granted after central authentication, using non-disclosing methods



Specification: KERBEROS V5

- 
- On-site systems visible from the internet *must not prompt for or accept* a reuseable password. Access requires:
 - ◆ Kerberos credentials, *or*
 - ◆ Challenge-response one-time authenticator.
 - Unmodified on-site systems may be isolated from the internet by a gateway that meets the above criteria.
 - For off-site systems part of the FNAL.GOV realm, we compromise:
 - ◆ Other secure (e.g., encrypted) access allowed *to* those systems.
 - No restrictions on outbound connections.



Infrastructure

- ☞ KDCs run just the essential services.
 - ◆ AS/TGS, kadmin, 2 flavors of password changing, “5-to-4”, kprop, and secure encrypted login.
- ☞ KDCs physically secured, but those in less-secured areas won't store master database key on disk and run with no paging space.
- ☞ Account deactivation to be placed under control of CNAS.



Preliminaries


- Several rounds of consultation with the user communities. (Plural.)
- Test software on various platforms.
- Select Kerberos s/w for Win32 access to Unix.
- Enlist willing pioneers.
- Develop user and administrative tools.



Challenge – Unattended Processes

- Historical approaches have included:
 - ◆ Unauthenticated “.rhosts” access,
 - ◆ Passwords stored in files,
 - ◆ Passphraseless ssh keys
- Our new approach:
 - ◆ Permit users to create extra Kerberos principals associated with their ID, a host and a purpose.
 - ◆ Stash keys in a file with best feasible protection.
 - ◆ Grant those principals the minimum necessary access for the purpose.
- Added risk:
 - ◆ Minimum necessary exposure.

Challenge – Portal Access for the unKerberized

- 
- Cryptocard implements a known algorithm in a wallet-sized token.
 - Matching algorithm is now implemented in our KDCs.
 - Telnet and FTP servers now respond to unauthenticated connections with a Cryptocard challenge.
 - KDC delivers credentials encrypted in the service's key, rather than the user's.
 - Added risk:
 - ◆ Zero or negative!

Challenge – Windows2000

- ☞ Plan: Use Microsoft Active Directory/KDC infrastructure for Windows 2000 domain (WIN.FNAL.GOV) and synchronize with the FNAL.GOV realm using standard cross-realm protocols.
- ☞ Microsoft KDCs permit NTLMv2 authentication as a fallback and we will use this as the authentication method for legacy NT4/W9x systems
 - ◆ These legacy systems may not offer services to the network.





Modifications to the MIT Kerberos Distribution

- Alternate authentication (CryptoCard, S/Key, ...) to reusable passwords
- Kcron method for unattended authentication.
- ftp client enhancement to work with emacs efs mode.
- Graceful fallbacks when connecting over default encrypted links to non Kerberos systems.
- Most of these are included in current MIT 1.2.2 release. Very willing to take patches.

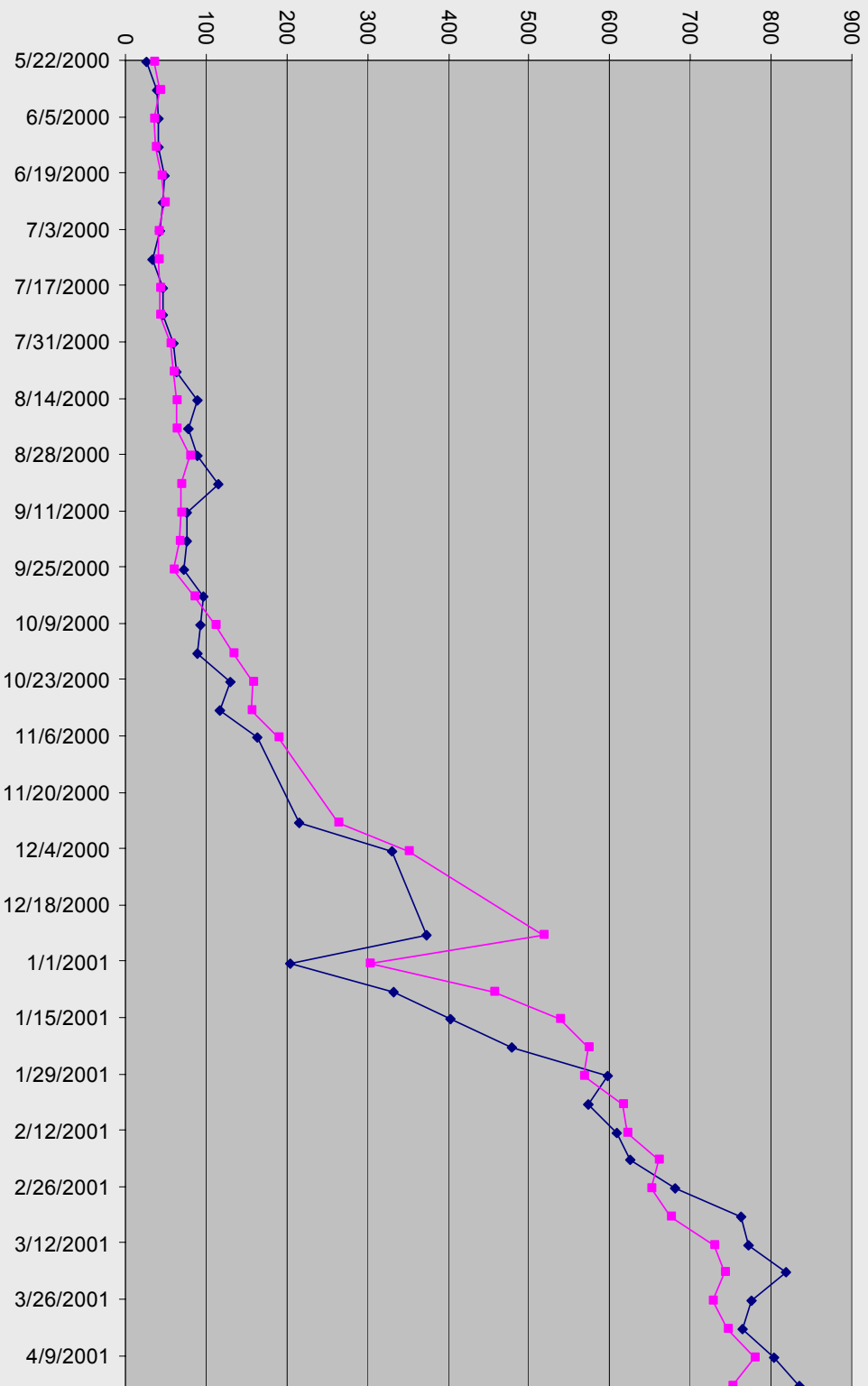


Deployment Status

- 2090 users
 - ◆ 1637 with Cryptocards
- 1609 service hosts
 - ◆ 57 off-site
- 468,000 TGT's issued in August
 - ◆ One service principal was granted 183615 tickets
- Kerberized applications include
 - ◆ CVS
 - ◆ FBS (batch job submission)
 - ◆ SSH (with Cryptocard access)

Kerberos User Load

Kerberos Weekly Users





Now the REST of the story

- ☞ There remain approx 2000 users to go (~2/3 of the lab users) with a larger population of legacy users and applications. This is to substantially complete (>95%) by December 31, 2001.
- ☞ Web, email, and most application authentication remain to be Kerberized.
- ☞ Have to grapple with how to isolate “unkerberizable” systems.



Deployment Plans – Unix

☞ September

- ◆ Complete dedicated experiment Unix cluster migrations
- ◆ Begin Windows 2000 Domain deployment.

☞ October

- ◆ Migration of central Unix facility (FNALU)

☞ November-December

- ◆ Migration of CAD systems
- ◆ Residual issues



Deployment Plans – Windows

☞ September

- ◆ Begin testing of strengthened W2k domain, first users.

☞ October-March

- ◆ Migrate divisions @ ~400 users/month



Deployment Plans – Others

☞ Macintoshes

- ◆ Mac OS X deployment is proceeding and appears to provide similar solutions as those for Unix. Proceeding along those lines.

☞ VxWorks single board computers

- ◆ Current approach is to isolate behind some gateway system or network firewall.
- ◆ Indications that kerberized clients may become available for this node.

☞ Embedded computers (web cameras, disk servers, etc.)

- ◆ Freeze systems such that upgrades require manual acts. Or
- ◆ Isolate behind some gateway system or network firewall.

What This Means To You (1)

- Does not affect email or web access
- Need not affect any outbound connections
- Does not prevent attaching visiting laptops to network (as long as they cannot be logged in to over the network)



What This Means To You (2)

- ☞ You will need to get a Kerberos account (principal)
- ☞ You may need to install some software on your desktop depending on how you use it
- ☞ System administrators will have additional software to install, but account management will be much easier



Desktop Considerations

- If desktop is dumb terminal: use Cryptocard to logon to other lab systems
- If desktop has minimal intelligence (PC) but does not accept remote logins: install local kerberos telnet and ftp clients, do local kerberos login, then proceed normally using kerberized versions of clients
- If desktop can be logged into remotely: install full local kerberos system, replace network services with kerberized versions





Conclusions

- Lab is on track for December 31, 2001 goal for sitewide deployment.
- Substantial work accomplished to date.
- Infrastructure scales.
- Regular deployment meetings ongoing.
- “GRID” integration issues are state of the art problem.