Collaboratory Needs *versus* the Security Infrastructure

James A. Rome

Oak Ridge National Laboratory

jar@ornl.gov

http://www.ornl.gov/~jar

Presented to the "Open Environment" Security Workshop
January 17, 2001

Facilities must be accessible but secure

DOE facility users are a diverse bunch

- **Industry, university, labs**
- **Domestic and foreign**

Facilities should be behind the strongest protection, e.g., firewalls—they are expensive!

- **Users often come in for one short session**
- **They may not be US citizens**
- **Data might be proprietary**

A facility at one Lab might be owned by another Lab (ORNL beam line at BNL)

Security barriers raise difficulties

DOE is encouraging each Lab to wrap itself in firewalls, to create enclaves, and to “know” its users.

Who should be allowed into these enclaves?

- **Should the authentication instruments of one Lab be accepted at others?**
- **Is it reasonable to say “come get your crypto card at our office during business hours” for remote users?**
- **The DOE cross-realm Kerberos may not be attractive because of policy issues, not technology.**
- **What if the "who" is a computer?**

Access restrictions

Effective February 15, 2001, all foreign nationals and nonemployees, including remote "cyber only" users (no on-site presence) that require access to ORNL cyber resources must have the appropriate Nonemployee Processing (NEP) system authorization/approval. On-site presence for this function is defined as an active, non-visitor badge for the Oak Ridge Reservation.

- ***How about people from other Labs?***
- ***I need my FTP server that gets article submissions for my newsletter from places like Russia.***
- ***What is the exact definition of "cyber resources?"***

This regulation implies that DOE needs to "trust" (at some level) all of its computer users. Is this necessary?

Trust levels

Type of access	Authentication	Authorization	Trust
Static Web server	No	No	No
Dynamic Web server	No	No	Maybe
Dynamic Web servers have never withstood a "hack me" attack			
FTP server	Probably	No	No
Remote microscopy	Yes	Yes	No
Remote beam line	Yes	Yes	Yes
Supercomputer	Yes	Yes	Yes
Telnet	Yes	No	Yes

The level of trust needs to be commensurate with the activities allowed and the value and protection level of the resource.

Safe access without trust

- **The touch screen information computer in an airport**
- **The computer in automated phone access systems**

These all have one thing in common:

The software and input mechanisms are severely constrained.

Can you control access if there is any?

- **Groove (www.groove.net) is a collaborative environment that encrypts all traffic and files and claims to penetrate firewalls by using http if necessary.**
- **VPNs (not the Lab ones) that use NAT transparency mode.**
- **Remote computers (the Grid, CORBA services)**

One great competitive edge of the USA in the cyber arena has been cheap available remote access to remote computers. We need to preserve this.

- **I paid a almost 1 DM/minute the last time I was in Germany for access from my apartment.**

Encryption changes things

Soon all network traffic will be encrypted, solving the user's "network security problem." (However, the problem of securing the network infrastructure remains...)

- **A proposed DOE policy is that DOE should be able to decrypt everything. This is reasonable but**
  - ⇒ **Totally ignored**
  - ⇒ **Unenforceable**
  - ⇒ **Impractical (PGP, S/MIME, Groove, SSL, PCAnywhere,…)**

The more worrisome problem is how can one detect attack or theft in an encrypted stream?

The security vulnerabilities and protections must occur at the clients, not in the network infrastructure.

Viruses are now encrypted

Hybris uses encrypted plug-ins to change features and is able to establish its own Internet connections for the purpose of upgrading itself. Among other functions, its 32 possible components can encrypt its copies to avoid detection; infect all ZIP and RAR archives on a computer's hard drives; send messages with encoded plug-ins to the virus research newsgroup alt.comp.virus; find and infect machines that have already been compromised with the well-known SubSeven backdoor; and create random subject, body and file names in English, French, Spanish or Portuguese.

VPNs are a partial solution

The ORNL implementation (Compatible/Cisco) has free clients for most platforms and uses Radius authentication.

- **Can create static tunnel addresses so I can access my home DHCP machine from work.**
- **Can use groups that can access only certain resources at the Lab (used for subcontractors).**

But there is no guarantee of the security of the remote machine. Microsoft got hacked through their VPN from a compromised home PC.

Securing a platform

If the computer is at the Lab, in principle (over my dead body), the machines can be placed under central control and they can be subjected to relentless scans, software control, etc.

But the remote user's PC is an unknown quantity and must be assumed to be "hostile." It may have

- **Viruses, worms, Trojan horses**
- **Keyboard sniffers**
- **Remote users (Gnutella, the SETI screen saver, networked family members)**

Access from a hostile environment

Can we allow access from such a platform without compromising DOE or its resources?

- **We MUST find out how to do this or else access will be severely restricted.**
- **Requirements for hostile access:**
  - ⇒ **Strong authentication. Is it really who you think it is?**
  - ⇒ **Encryption or secure hashes to prevent man-in-the-middle attacks.**
  - ⇒ **Ability to control which resources are accessed.**
  - ⇒ **Knowledge of what software is being run remotely.**

SSH as an example

SSH has

- **Strong authentication (can be certificate based)**
- **Encryption**

It does not have

- **The ability to control what is accessed. (Telnet essentially assumes that the user is trusted.)**
- **The knowledge that a non-modified SSH is being run.**
  - ⇒ **Because SSH has full access to the host machine, a Trojan can be launching attacks in the background.**

Custom client/server software

One way of doing this is to

- **Download a signed Java applet and have some way of knowing that is it the one that you downloaded.**

Scalability issues

The current security infrastructure does not scale well to

- **Greatly-increased bandwidths**
- **Massively parallel distributed computing**
- **Encrypted traffic**
- **Distributed attacks**
- **Computers that change their operating systems**
- **Embedded operating systems**
  - ⇒ **No ability to control their security (e.g., unable to put DOE warning banner in our Axis camera servers)**

Possible approaches

Biological systems seem to scale well

- **Stephanie Forrest (http://www.cs.unm.edu/~immsec)**
- **Can you detect what is abnormal in a research-oriented computer system?**

Applying patches is a full-time occupation if you are responsible for many systems http://windowsupdate.microsoft.com

- **is a big step forward.**
- **Application patching is harder because users are unaware of the vulnerabilities. http://officeupdate.microsoft.com**

Enclaves

An Enclave is a collection of information and information resources with similar protection concerns and that need to interoperate.

- **DOE's unclassified cyber security program defined this(DOE N 205.1).**
- **Instantiating enclaves could serve as the basis for the inter-Lab and external user access issues.**