

Computer Security Update

- New Computer Security Executive (CSExec)
 - Vicky White
 - Dane Skow (deputy)
- New Fermi Computer Incident Response Team (FCIRT) Head
 - Mark Kaletka (replaces Don Petravick)

Strategy

- Core commitment to open collaborative environment and “default allow” remains.
- Security is (as much as possible) an integrated management function.
- Current policy working but needs to adapt to changing environment.
 - Ongoing reviews will guide incremental change.
 - Will try to avoid “step function” changes but may be overcome by events.

Environment has changed

- Threat Environment
 - Root DNS server attacks Oct, 2002
 - SQL worm network congestion (~8 seconds doubling) Jan, 2003.
- Political Environment
 - 2001 attacks on NY and Washington changed discussion from “threats” to “vulnerabilities”
 - Federal Government systems blasted as incompetent and insecure (see Horn report)
- Regulatory Environment
 - National Strategy on Securing Cyberspace

FNAL Experience

- FCIRT “rolls out” twice a week on average.
- Attacks targetted at Windows systems on the rise and gaining in sophistication and “value”.
- Most rapid spreading mal-ware exhibits “hunting behaviour” (rapid attempts to contact many sites and/or services).
- Patch release frequency continues to increase.
- Vulnerability exploit window continues to decrease.

Border Router Changes

- Have instituted block against inbound “hunters”
- Will institute block against outbound “hunters”
 - Automatic block persists until hunting behaviour stops (and is lifted after some modest delay)
 - Block pending notification method to registered admins (or next worm alarm)
- Planning “default deny” config for inbound NetBIOS access
 - Windows servers needing to provide services to offsite customers can apply to be unblocked.

Futures

- Expect that large portions of the lab can be behind a firewall block from the general internet.
 - Discussions underway now as to implementation options and costs.
- Expect that lab network will be restructured into levels of access.
 - This will likely include a registration requirement for network connection.