



Computer Security Essentials for Fermilab Sysadmins

Irwin Gaines and Matt Crawford

Computing Division



Outline

- Introduction: why are we here, special role of system administrators
- Computer Security Essentials: technical details
- Fermilab security policy for sysadmins



“Open” Philosophy

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

-- Enrico Fermi



“Open” Philosophy

- Like an academic institution, we want to maintain an atmosphere which encourages free exchange of ideas;
- Yet, we have an obligation to protect our data and systems;
- We allow wide latitude within certain limits
 - Computer security should not prevent lab business
 - Ignoring computer security most certainly will!
(hackers and regulators)



Critical role of sysadmins:

- Sysadmins are on the “front line” of computer security:
 - “Fermilab’s continuing policy has been to put its first line of defense at the individual responsible for the data and the local system manager.”
- Three roles:
 - System managers;
 - examples for users;
 - vigilant observers of system (and sometimes user) behavior
- Sysadmins are expected to communicate computer security guidelines and policies to the users of systems they administer;



Role of sysadmins

- Manage your systems sensibly, remaining aware of computer security while conducting everyday business
- Advise and help users
- Keep your eyes open
- Report potential incidents to FCIRT
- Act on relevant bulletins

Technical Details

👉 newbies





Fermilab Computer Security Policy

- Integrated Security Management (and GCSCs)
- Critical systems vs. general security domain
- Strong rules
- Incidental computer use
- Embarrassment to the laboratory (the .gov issue)



Integrated Security Management

- ❏ Computer Security is not an add-on or something external, it is part and parcel of everything you do with computers (analogy with ES&H)
- ❏ Not “one-size-fits-all”, but appropriate for the needs and vulnerabilities of each system
- ❏ In most cases, it is simply common sense + a little information and care



GCSCs

- BD Paul Czarapata
- BSS Tom Ackenhusen
- CD Matt Crawford
- Dir Jud Parker
- ES&H Matt Arena
- LSS Kevin Williams
- PPD Allen Forni
- TD John Konc
- FESS Ken Fidler
- CDF Rob Harris
- D0 Mike Diesburg



Critical Systems

- ☞ Defined as “critical to the mission of the Laboratory”, i.e. disruption may have major impact on Laboratory operations;
 - Most things do *not* fall in this category;
- ☞ Special (more stringent) rules & procedures apply;
 - Including periodic reviews;
- ☞ You’ll know if you’re in this category;



General Systems

- ☞ “Everything else”;
- ☞ Emphasis on education, “best practices”;
- ☞ Small set of strongly enforced rules;
 - Divisions/Sections may add to these;



Strong Rules

- Incident Reporting
- Unauthorized and malicious access and actions
- Blatant disregard for laboratory computer security
- Restricted central services
- Possession of security (hacker) tools
- System manager registration
- Data Integrity and backup
- Strong Authentication



Rules for General Systems

- ☞ Mandatory incident reporting;
 - Report all suspicious activity:
 - *If urgent* to FCC Helpdesk, x2345, 24x7;
 - *Or* to system manager (if immediately available);
 - Non-urgent to `computer_security@fnal.gov`;
 - Incidents investigated by Fermi Computer Incident Response Team (FCIRT);
 - *Not* to be discussed!



FCIRT

- Investigate (“triage”) initial reports;
- Coordinate investigation overall;
- Work with local system managers;
- Call in technical experts;
- May take control of affected systems;
- Maintain confidentiality;



Rules for General Systems

- ☞ “Blatant disregard” of computer security;
 - First time warning, repeat offense disciplinary action;
- ☞ Unauthorized or malicious actions;
 - Damage of data, unauthorized use of accounts, denial of service, etc., are forbidden;
- ☞ Ethical behavior;
 - Same standards as for non-computer activities;



Rules for General Systems

- Restricted central services;
 - May only be provided by Computing Division;
- Security & cracker tools;
 - Possession (& use) must be authorized;
- Strong Authentication (Kerberos)
- System managers;
 - Must be registered with FCSC;
 - See: <http://www-miscomp.fnal.gov/sysadmindb>



Rules for General Systems

☞ Backup Policy - Users

- Users (data owners) responsible for determining:
 - What data requires protection;
 - How destroyed data would be recovered, if needed;
 - Coordinating backup plan w/ sysadmins;
 - or doing their own backups;



Activities to Avoid

- ☞ Large grey area, but certain activities are “over the line”;
 - Illegal;
 - Prohibited by Lab or DOE policy;
 - Embarrassment to the Laboratory;
 - Interfere w/ performance of job;
 - Consume excessive resources;



Appropriate Use

- Many “computer security” complaints are not;
- Material in a computer is like material in a desk;
 - Wrt to both privacy and appropriateness;
- This is a line management, not computer security, concern (except in egregious cases);



Privacy of Email and Files

- Fermilab normally respects the privacy of electronic files and email;
- Employees and users are required to do likewise;
- Certain exemptions for system managers and computer security response;
- All others *must* have Director(ate) approval;



Privacy of Email and Files

- ✎ May not use information in another person's files seen incidental to any activity (legitimate or not) for any purpose w/o either explicit permission of the owner or a “reasonable belief the file was meant to be accessed by others.”
 - Whether or not group/world accessible;
 - “Group” files implicitly may be used by the group for the mission of the group;

Questions?

Irwin Gaines

x4022

nightwatch@fnal.gov

<http://www.fnal.gov/cd/security/>

