



Security Essentials for Desktop System Administrators



Civilization Is Made Of People ...

Civilization is Risk.

-- Not Big Brother



Dave Barry On Civilization ...

New Technology Is Invented Largely
To Overcome Previous "Advances"



Dave Barry On Civilization ...

Fields -> Trees -> Caves -> Houses



Dave Barry On Civilization ...

Houses -> Windows -> Glass



Dave Barry On Civilization ...

Glass -> Drapes -> Tents



Dave Barry On Civilization ...

Fireplaces -> Microwaves -> Bean Burritos



Dave Barry On Civilization ...



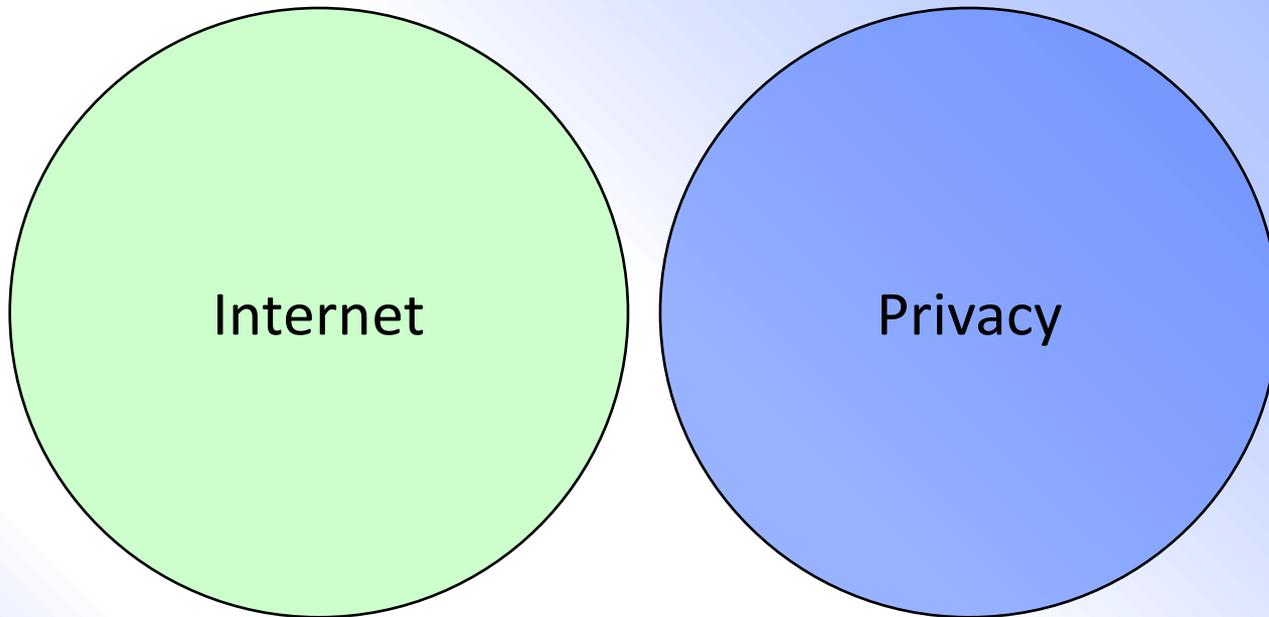


Computer Security ...

Essentially A People Problem

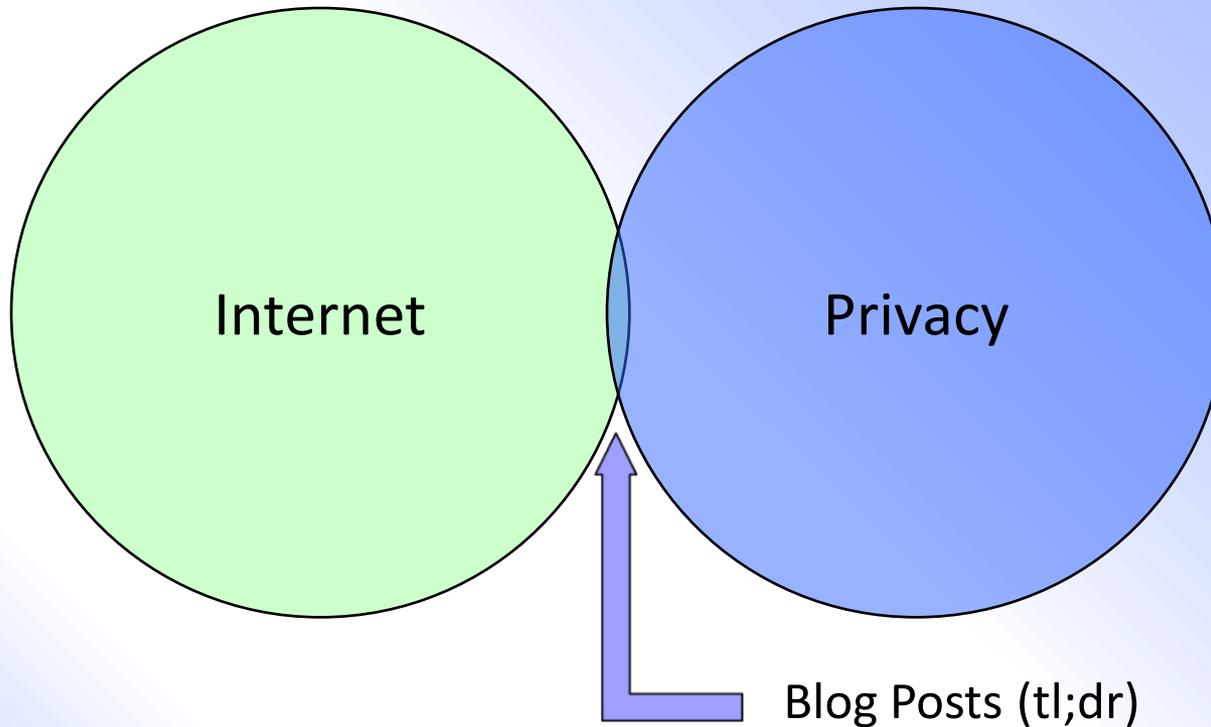


A Basic “People Problem”





A Slightly More Precise View





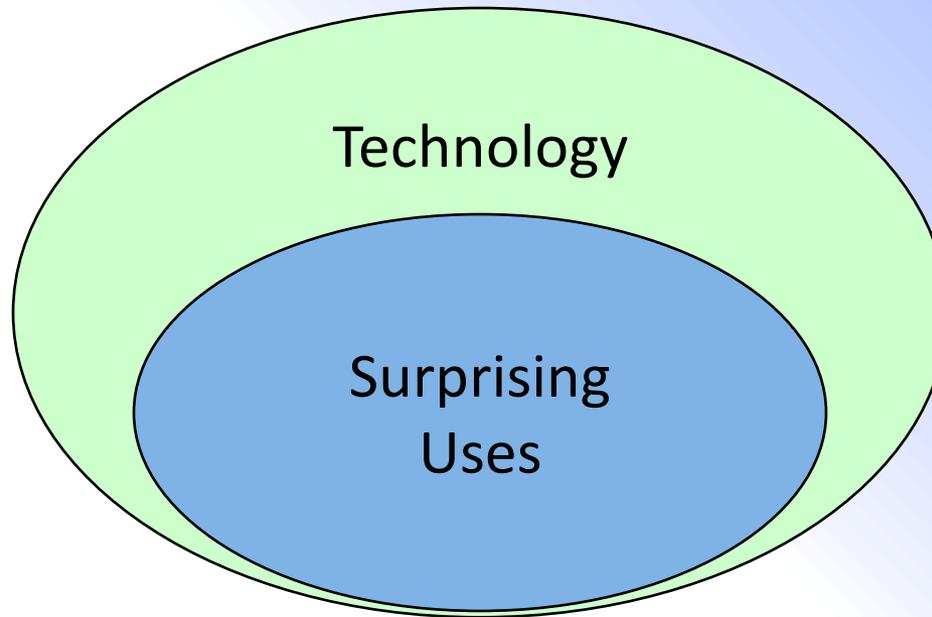
Bruce Schneier

Once the technology is in place, there will always be the temptation to use it ...

(Secrets and Lies, 2000)

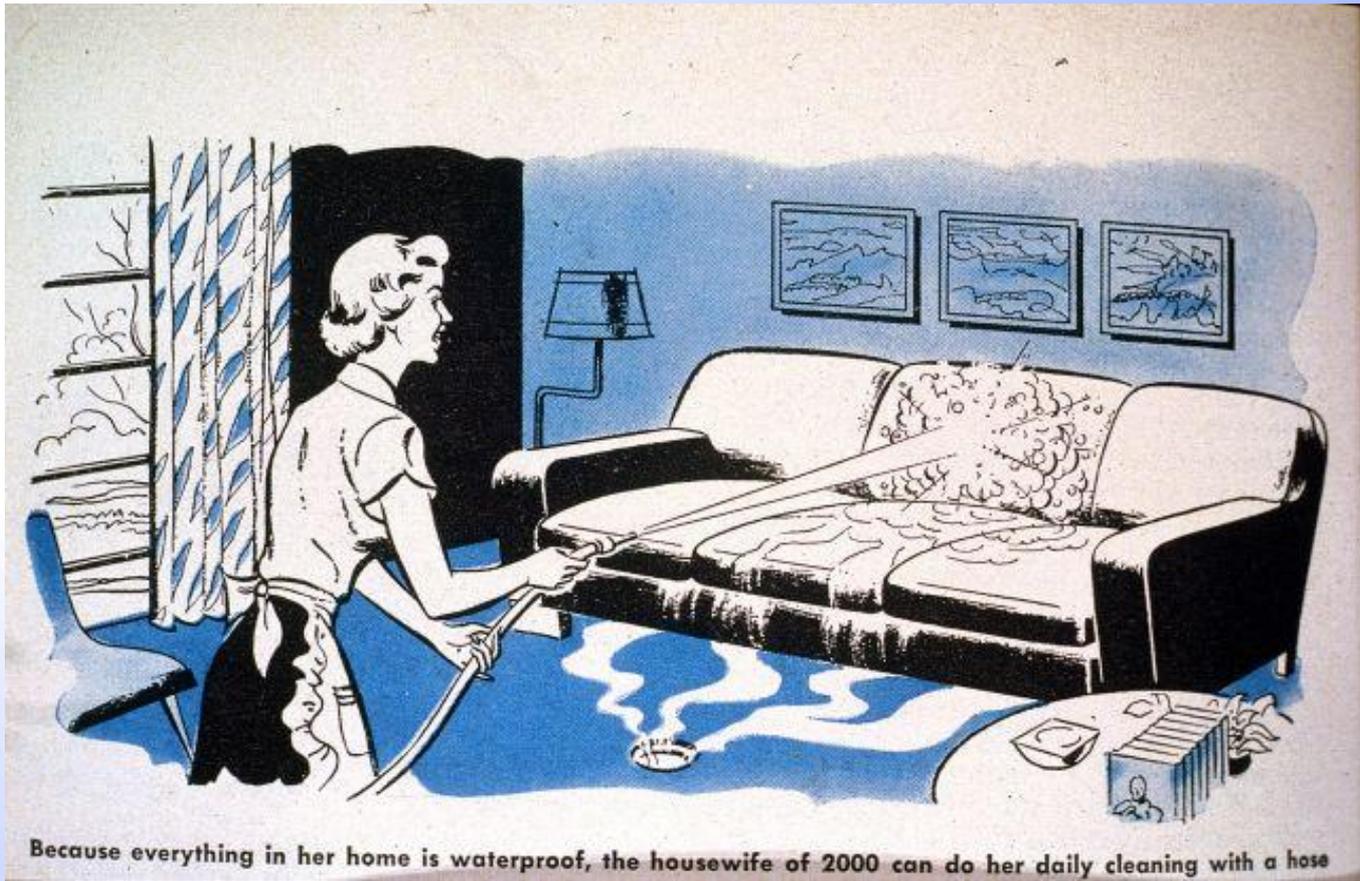


How Technology Works





(Unsurprising Useless Utopias)





Surprising Technology Use



MUDFLAPS

SO I HERD U LIEK THEM



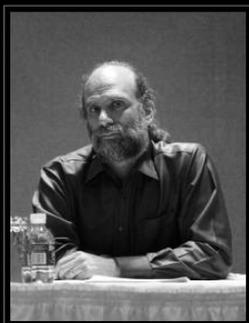
Surprising Technology Use



BastiatInst Bastiat Institute

Professors Give Up, Finally Embrace Wikipedia. Wikipedia Remains Unsure About Profs. - <http://bit.ly/90Lw0f>

4 Nov



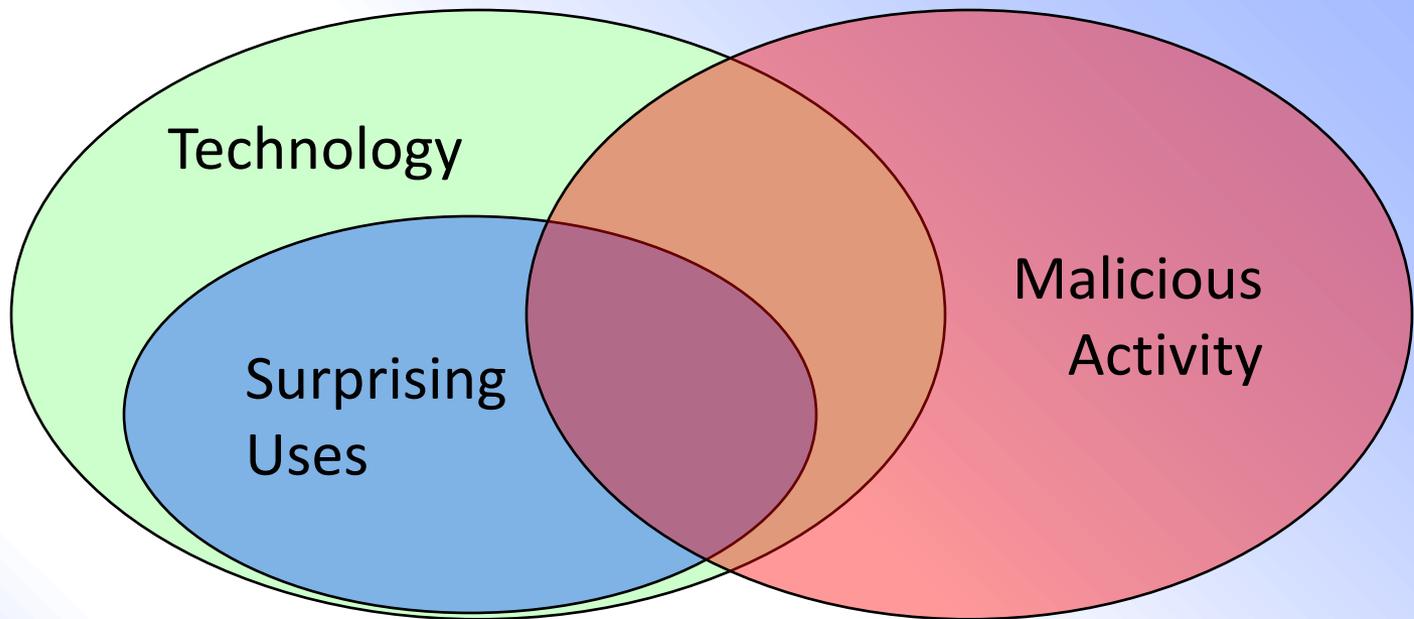
SECURITY
You're doing it wrong.

Bruce Schneier

And it is poor civic hygiene to install technologies that could someday facilitate a police state.



Technology And Risk





Grace Hopper

Life was simple before World War II.
After that we had *systems*.



xkcd ...





... xkcd





Dealing With Risk

Recognition | Reduction | Recovery



Recognizing Risks

High Bandwidth
Enormous Storage
Posh *.gov* Location

Nothing Marketable



Recognizing Risks

Caching warez
Sending SPAM
Spreading malware
Controlling bots



Recognizing Risks

Destruction Of Data
Waste Of Bandwidth
Waste Of Time
Frustration



Recognizing Risks

Default admin privs
Visiting malicious sites
Promiscuous USBing
Lack of gruntlement



Strategic TLA Reserves

TLAs not specifically delegated ...
are reserved to the States, or to the
people.

“BOR” (10th Amendment)



TCB? DID!

Integrated Security Management (ISM)

Defense In Depth (DID)



Reducing Risks: DID

Perimeter Controls
Auto-blocking
Mail virus scanning
Central Authentication
(via LDAP/Kerberos)



Reducing Risks: DID

Patch and configuration mgmt
Critical Vulnerabilities
Prompt response via FCIRT
Intelligent and informed users
General and special enclaves



Reducing Risks: DID

Computer Security not an add-on
Not “one-size-fits-all”
Largely common sense



Reducing Risks: ISM Perimeter

Exploitable protocols blocked
Registered web servers allowed
Dynamic blocks on exploits
Some carefully configured services
allowed (like Skype)



Reducing Risks: ISM Auth

Primary passwords off the net

Single turn-off point

No visible services without StrongAuth

Lab systems scanned for compliance



Recovery: ISM

General Computer Security Coordinators
Work with Computer Security Team
Disseminate information
Deal with incidents
See <http://security.fnal.gov/> for list



What About Us Users?

Malicious Surprises abound

Use reasonable caution

Use up-to-date virus scanning



Users: We Get Mail

Can you trust the so-called sender?

Received: from [123.28.41.241] (unknown [123.28.41.241]) by
hepa1.fnal.gov (Postfix) with ESMTP id 808F76F247 for
<baisley@fnal.gov>; Thu, 01 Apr 2010 09:41:02 -0500 (CDT)

From: Wayne E Baisley <baisley@fnal.gov>

To: Wayne E Baisley <baisley@fnal.gov>

route: 123.28.32.0/19

descr: VietNam Post and Telecom Corporation (VNPT)

address: Lo IIA Lang Quoc te Thang Long, Cau Giay, Ha Noi



Users: We Get Mail

You haven't won \$10M

Rampant account hijacking

Don't open (most) attachments

Best not to click links in mail

Disable scripting for mail



Access: ~~Hollywood~~

Royko any social engineering attempts

Protect your Kerberos password

and it will protect you

Don't run unkerberized network services
(like telnet or read/write ftp)



Users: Security Incidents

Report suspicious stuff to

x2345 or computer_security@fnal.gov

Follow FCIRT instructions during incidents

Keep infected machines off the network

Preserve system for expert investigation



Users: Data

Decide what data requires protection

How to be recovered, if needed

Arrange backups with Sysadmins

Or do your own backups

Occasionally test retrieval



The Incidental Computist

Some non-Lab-business Surprising Use
allowed in the guidelines:

<http://security.fnal.gov/ProperUse.htm>



Activities to Avoid

Anything that is illegal
Prohibited by Lab/DOE policy
Embarrassing to the Lab
Interferes with job performance
Consumes excessive resources



Activities to Avoid

Services like Skype and BitTorrent
not forbidden but very easy to misuse!

(Better off with iPhone/Droid/etc.)



Data Privacy

Generally, Fermilab respects privacy

You are required to do likewise

Exemptions for Sysadmins and Security

Others *must* have Directorate 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."



Offensive Materials

Material on a computer \approx Material in a desk

This is a line management concern

Not computer security issues *per se*



Software Licensing

Fermilab is strongly committed to respecting intellectual property rights
Use of unlicensed commercial software is a direct violation of lab policy

A vertical image of a metal adjustable wrench, showing its handle with a circular ring at the bottom and the adjustable head at the top. The handle has some faint markings and a logo.

Summary: User Responsibilities

Appropriate use of computing resources

Ensuring your data is backed up

Respecting others' privacy

Protecting Personal Information (course)

Reporting incidents promptly



Which Brings Us To Sysadmins

That wrench ain't gonna swing itself.



Sysadmins Get Risk-Roled

System manager for security
Assist and instruct users to do it right
Vigilant observer of your systems (and
sometimes user) behavior



Patch/Configuration Management

Baselines: Linux, Mac, Windows

All systems must meet their baseline

All systems must be regularly patched

Non-essential services off

Windows, especially, must run AV



Patch/Configuration Management

All systems must run up-to-date,
supported version of the OS

Exceptions/Exemptions:

Documented case why OS is “stuck”

Patch and manage as securely



Critical Vulnerabilities

Active exploits declared critical
Pose a clear and present danger
Must patch by a given date or be blocked
Handled via Tissue events



NOISE, *n.*

...

The chief product and authenticating sign of civilization.

Ambrose Bierce, *The Devil's Dictionary*



Computer Security Incidents

Must report all suspicious activity

If urgent -- Service Desk at x2345

Or to system manager

(if immediately available)

Not to be discussed!



Computer Security Incidents

Non-urgent to

computer_security@fnal.gov

Fermi Computer Incident Response
Team (FCIRT) will investigate



Recovery: FCIRT

Triage initial reports
Coordinate investigation
Work with local Sysadmins
Call in technical experts



Recovery: FCIRT

May take control of affected systems
Maintain confidentiality



Mandatory Sysadmin Registration

All Sysadmins must be registered
Primary Sysadmin is responsible for
configuring and patching

<http://security.fnal.gov> ->

“Verify your node registration”



Major applications

Critical to the mission of the Lab
Require *moderate* level security controls
Each MA has its own security plan with
enhanced / compensatory security controls



Security Essentials for Grid System Administrators *Course*

Credentials other than Fermilab Kerberos

Fermi Grid infrastructure (GUMS / VOMS)

Developer of grid middleware



Grid Security Training

Grid Resource Users also require training on PKI Authentication



Do Not Want: Prohibited Activities

Blatant disregard of computer security

Unauthorized or malicious actions

Unethical behavior

Restricted central services

Security & cracker tools

<http://security.fnal.gov/policies/cpolicy.html>



Role of Sysadmins

Manage your systems sensibly, securely

Services comply with Strong Auth rules

Report potential incidents to FCIRT

Act on relevant bulletins

Keep your eyes open

We Can Do It ...



We Can Do It. Statistically.





Questions?

nightwatch@fnal.gov

for questions about security policy

computer_security@fnal.gov

for reporting security incidents

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