



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



Dave Barry On Civilization ...

Fields -> Trees



Dave Barry On Civilization ...

Fields -> Trees -> Caves



Dave Barry On Civilization ...

Fields -> Trees -> Caves -> Houses



Dave Barry On Civilization ...

Houses



Dave Barry On Civilization ...

Houses -> Windows



Dave Barry On Civilization ...

Houses -> Windows -> Glass



Dave Barry On Civilization ...

Glass -> Drapes



Dave Barry On Civilization ...

Glass -> Drapes -> Tents



Dave Barry On Civilization ...

Glass -> Drapes -> Tents (in Fields!)



Dave Barry On Civilization ...

Fireplaces



Dave Barry On Civilization ...

Fireplaces -> Microwaves



Dave Barry On Civilization ...

Fireplaces -> Microwaves -> Bean Burritos



Dave Barry On Civilization ...



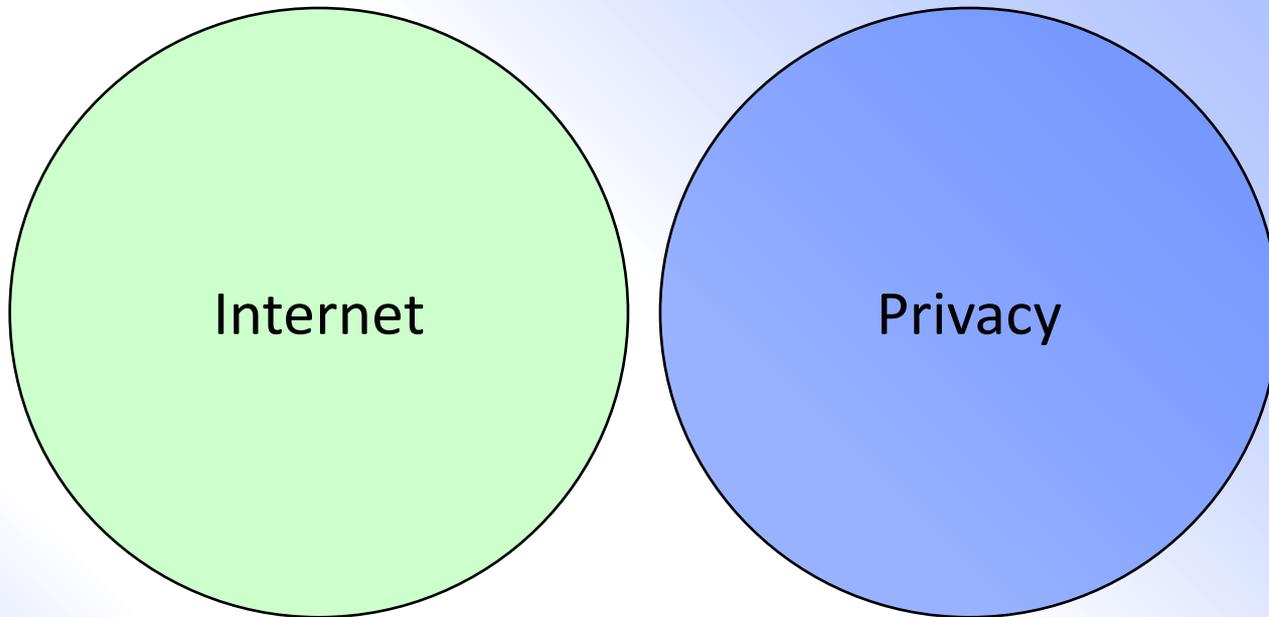


Computer Security ...

Essentially A People Problem

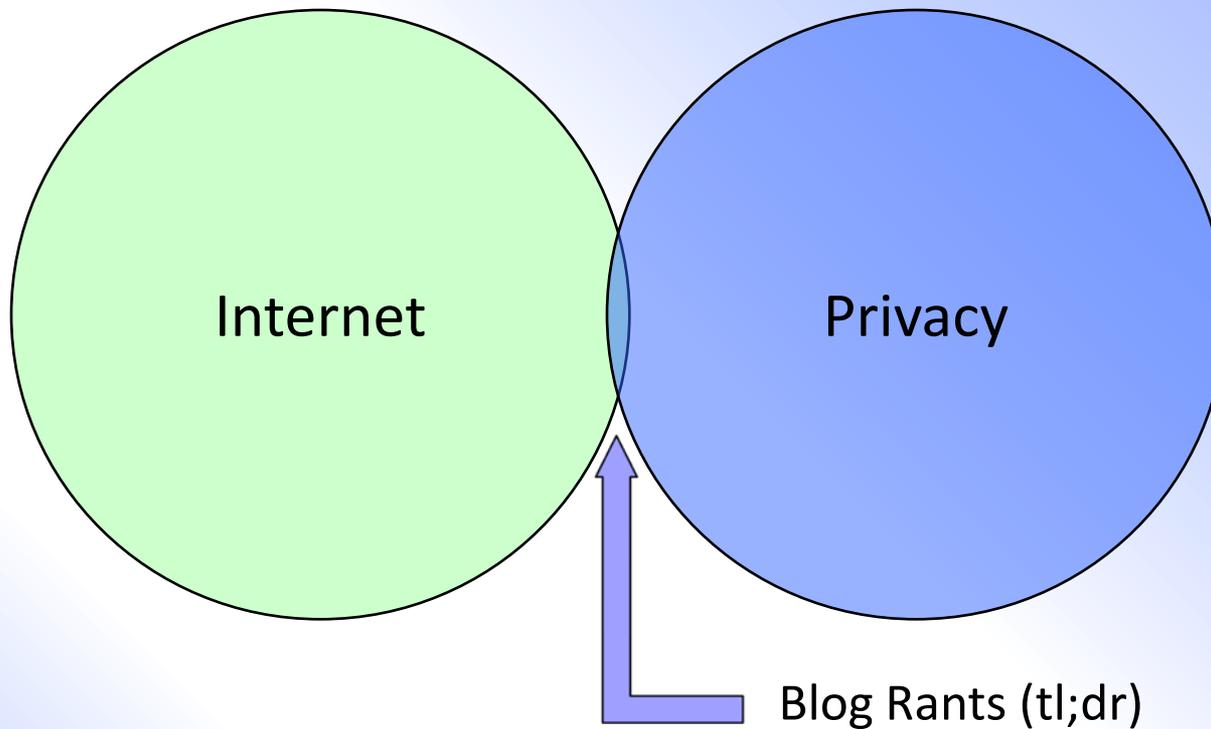


A Basic “People Problem”





A Slightly More Precise View





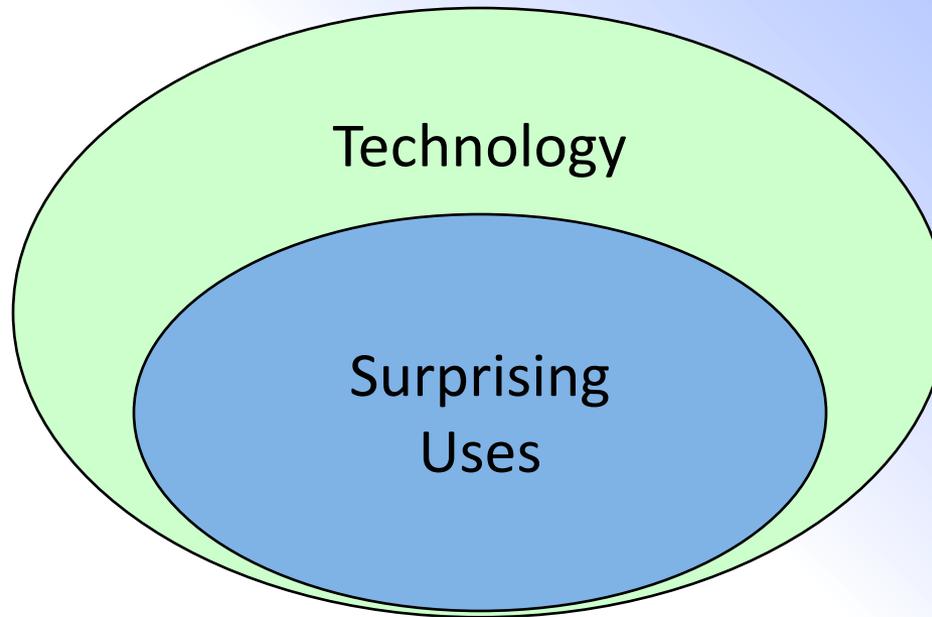
Bruce Schneier

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

(Secrets and Lies, 2000)



How Technology Works





Surprising Technology Use

Dollheads Revisited

Posted on December 4, 2011 by Bronc Drywall
Filed in [Whimsicle](#)

95

This post first appeared on Regretsy on December 10, 2010

Vintage 80s Cabbage Patch Ear muffs



\$15.00 USD

Great ear muffs - two little cabbage patch heads keep those ears toasty in these chilly months! They are adjustable and will fit a child or adult.

The little faces measure ~4" across. Missing one ribbon tie for pigtails, other than that in very good vintage condition. Label reads 1984 OAA INC.

I'M SORRY I CAN'T HEAR YOU I'M AN IDIOT

[View Post \(95 comments\)](#)

[f Share](#)

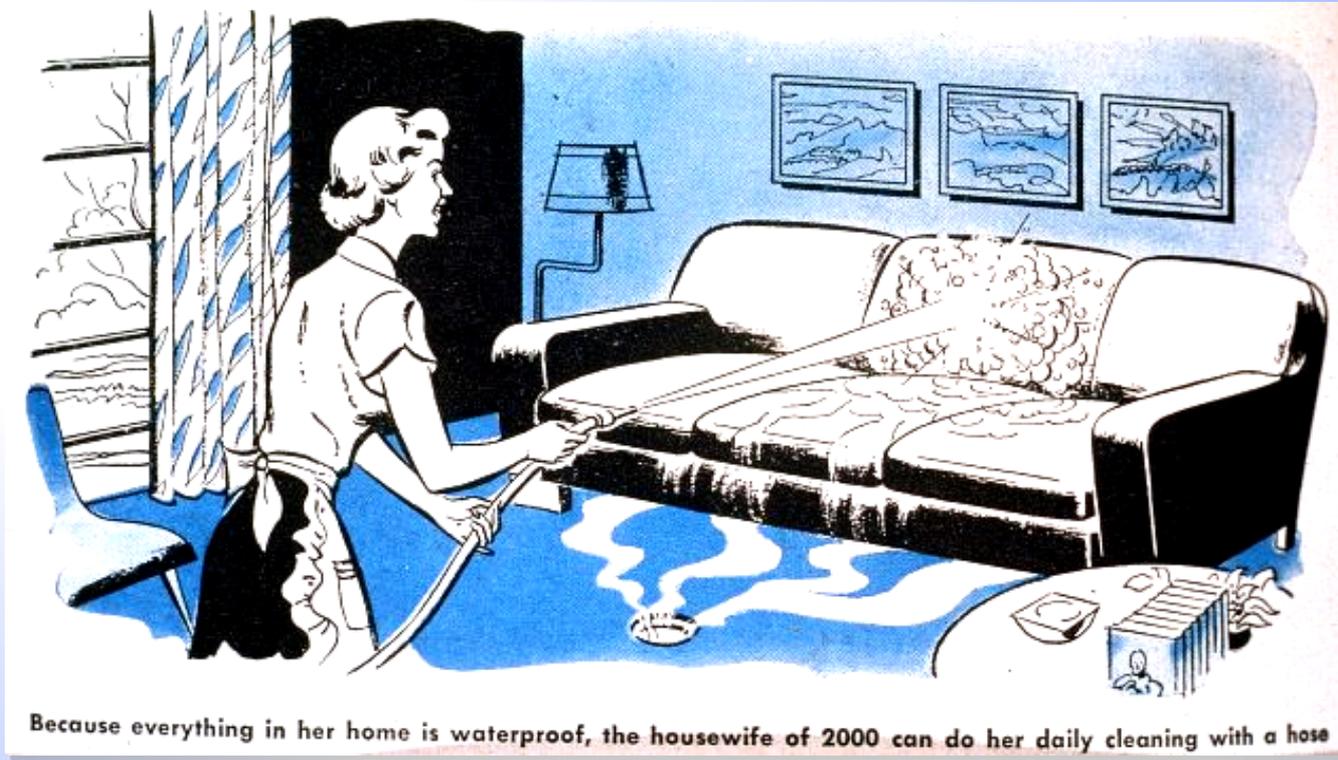
[Tweet](#)

[+1](#)

[Share](#)



Surprising Technology Non-Use





Surprising Technology Use

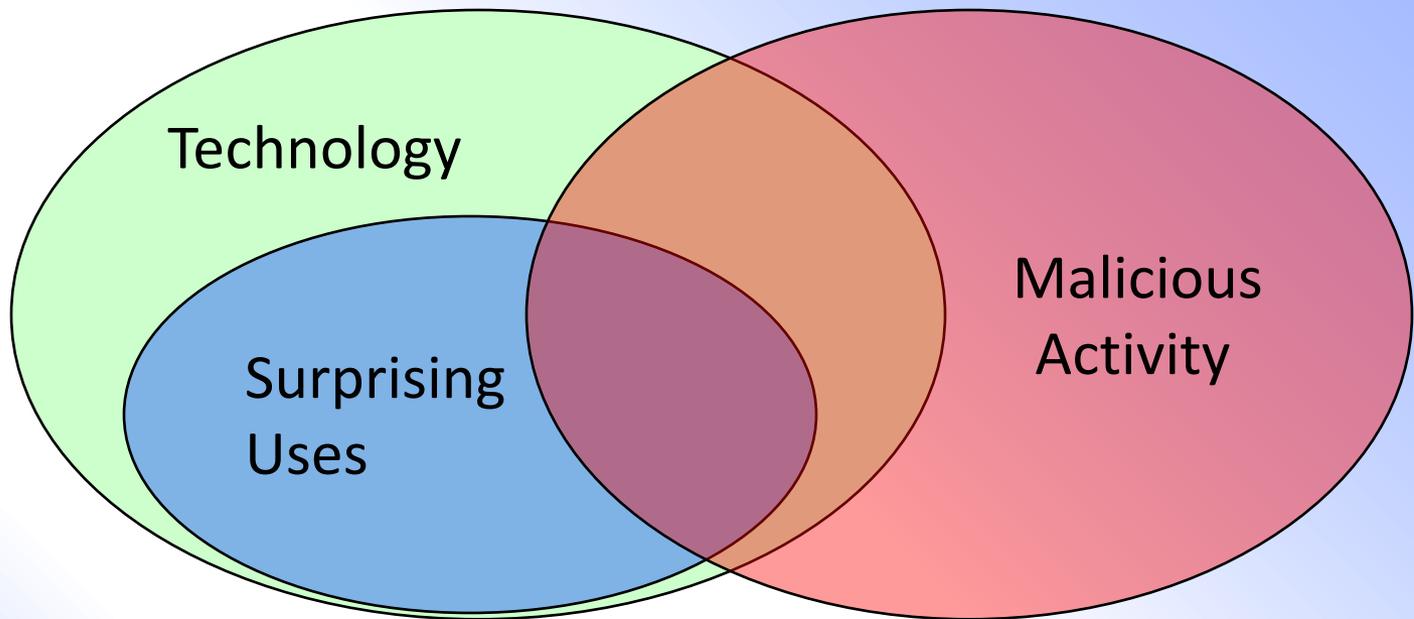


MUDFLAPS

SO I HERD U LIEK THEM

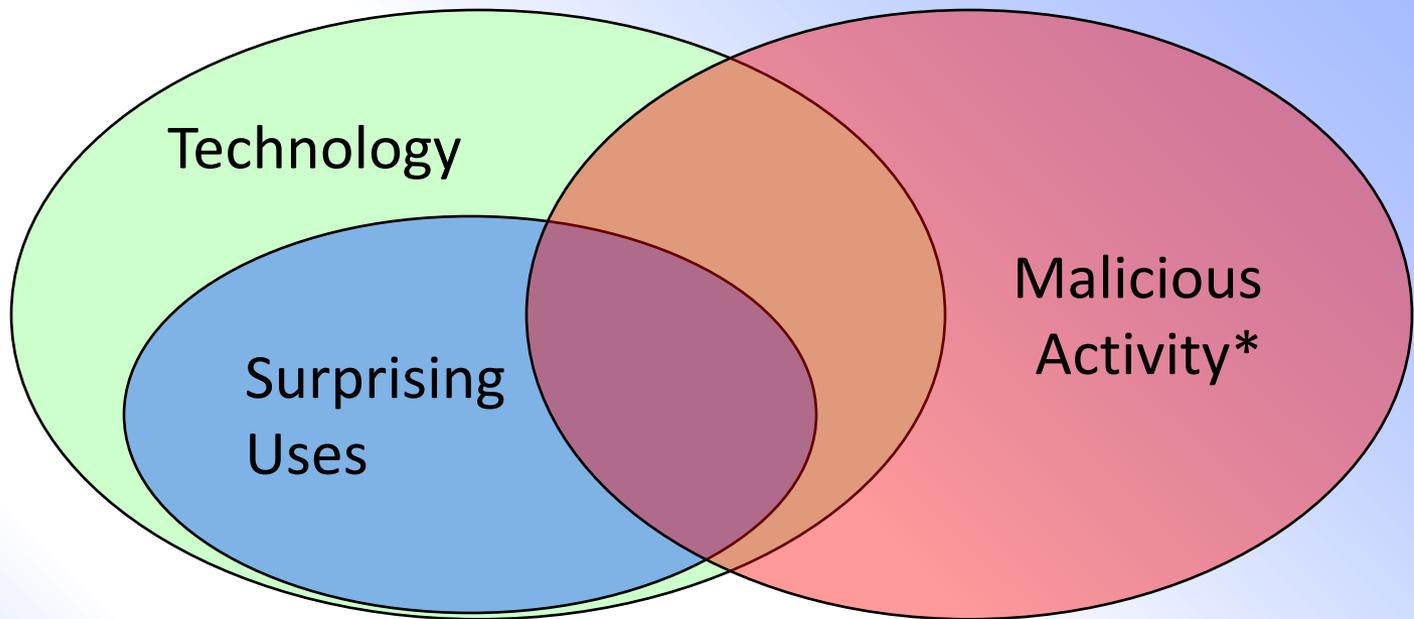


Technology And Risk

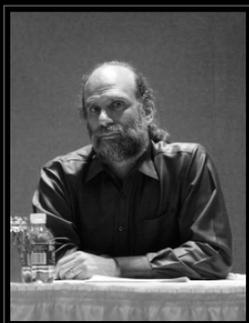




Technology And Risk



* not to scale



SECURITY
You're doing it wrong.

Bruce Schneier

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



xkcd ...





... **xkcd**





Dealing With Risk

Recognize | Reduce | Recover



Dealing With Risk

Protect | Detect | React



Recognizing Risks

High Bandwidth

Enormous Storage

Posh *.gov* Location

Nothing Marketable



Recognizing Risks

High Bandwidth

Enormous Storage

Posh *.gov* Location

Nothing Marketable*



Recognizing Risks

Caching warez

Sending SPAM

Spreading malware

Being/controlling bots

Committing/suffering DDoS attacks



Recognizing Risks

Destruction Of Data
Waste Of Bandwidth
Waste Of Time
Frustration



Recognizing Risks

Default admin privs

Visiting malicious sites

Promiscuous USB sharing

Lack of gruntlement



Newer Threats

CarrierIQ / mobile device surveillance
QR Code attacks





Newer Threats

~~DigiNotar~~ Gemnet

Stuxnet, Critical Infrastructure attacks

Advanced Persistent Threats



Grace Hopper

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



TLAs for TCB: ISM? 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



Recognizing Risks: ISM

Computer Security not an add-on

Not “one size fits all”

Largely common sense



Reducing Risks: ISM

Primary passwords off the net

Single turn-off point

No visible services without

Strong Authentication

Lab systems scanned for compliance



Recovery: ISM

General Computer Security Coordinators
(Listed at <http://security.fnal.gov/>)

Work with Computer Security Team

Disseminate information

Deal with incidents



What About Us Users?

Malicious Surprises abound
Use reasonable caution



Users: We Get Mail

You haven't won \$10M

Don't open (most) attachments

Best not to click links in mail

Disable scripting for mail



Users: We Get Mail

Can you trust the (so-called) sender?

Received: from [123.28.41.241] (unknown [123.28.41.241]) by
hepa1.fna1.gov (Postfix) with ESMTP id 808F76F247 for
<baisley@fna1.gov>; Thu, 01 Apr 2010 09:41:02 -0500 (CDT)
From: Wayne E Baisley <baisley@fna1.gov>
To: Wayne E Baisley <baisley@fna1.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: Pass the Word

Use strong passwords

Longer is better

Use different passwords

Or *variants*, at least



Access: ~~Hollywood~~

Royko any social engineering attempts



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
is allowed:

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

(I prefer personal iPhone/iPad/Droid
via an external network ...)



Activities to Avoid

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



Activities to Avoid

Anything that:

- Is illegal

- Is prohibited by Lab/DOE policy

- May embarrass the Lab

- Interferes with job performance

- Consumes excessive resources



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 users') behavior



NOISE, *n.*

...

The chief product and authenticating sign of civilization.

Ambrose Bierce, *The Devil's Dictionary*



Data Privacy

Generally, Fermilab respects privacy

You are required to do likewise

Special cases for Sysadmins during

Security Incidents

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 explicit permission of the owner or "reasonable belief the file was meant to be accessed by others."



Offensive Materials

Material on computer \approx Material on desk

A line management concern

Not a computer security issue *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.



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

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



Computer Security Incidents

Report suspicious events to x2345 or
computer_security@fnal.gov

Follow FCIRT instructions during incidents

Keep infected machines off the network

Preserve system for expert investigation

Not to be discussed!



FCIRT

Triage initial reports

Coordinate investigation

Work with local Sysadmins, experts

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”



Do Not Want: Prohibited Activities

Blatant disregard of computer security

Unauthorized or malicious actions

Unethical behavior

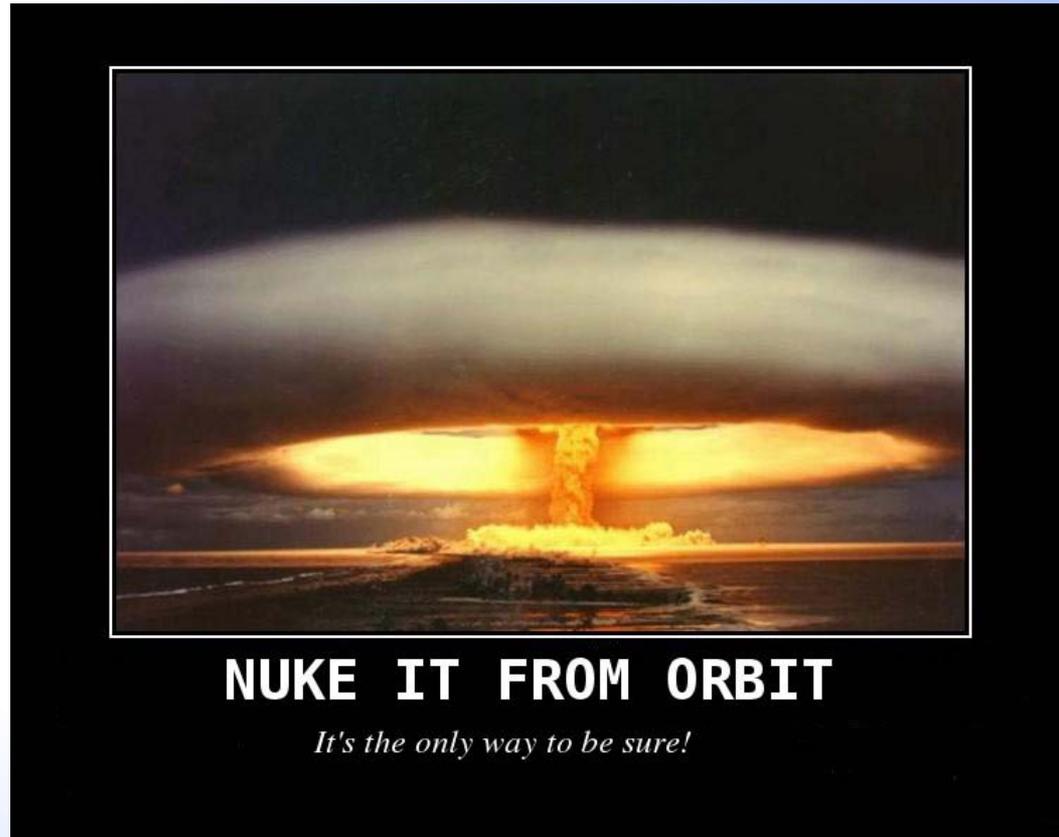
Restricted central services

Security & cracker tools

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



We Want To Avoid This ...





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/>



Security Essentials for Desktop System Administrators



Security Essentials for Desktop System Administrators