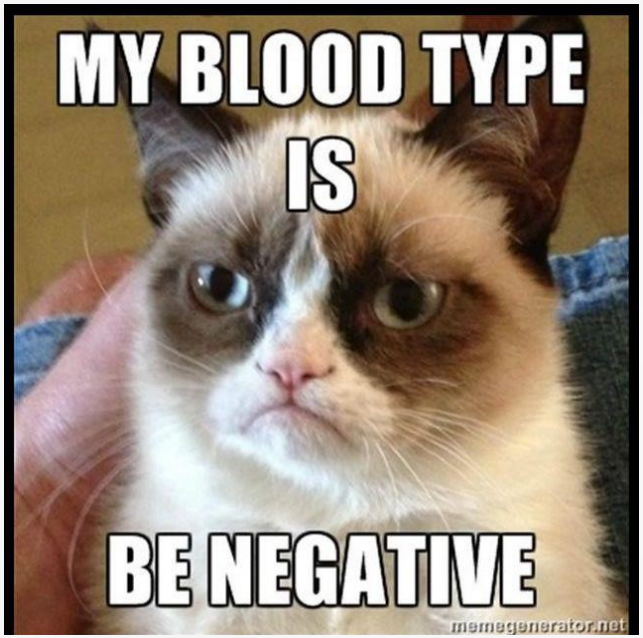
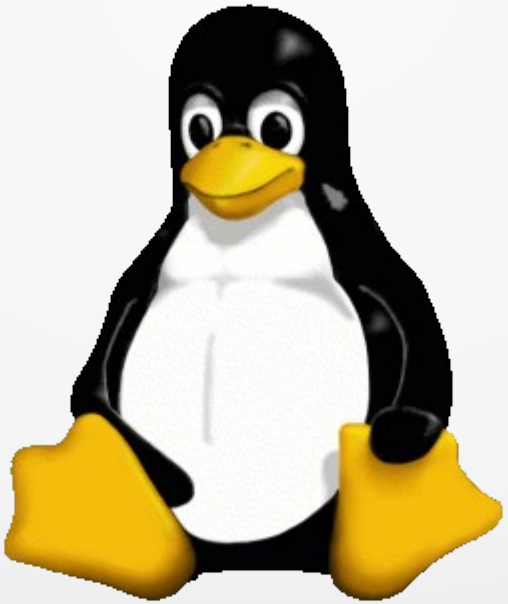
Protecting your privacy, anonymity and security with Linux and Open Source tools



Jeremy (bneg)
@beyondnegative


HOW FUCKING FASCINATING!
COME CLOSER AND TELL ME MORE

About me



/* Disclaimer */

- Please hold questions until end
- There are dozens of combinations of tool presented in the following slides, choose what works for you
- None of these methods should be construed as “bullet proof”
- Bullet points are stupid, I'll avoid them as much as possible

Who is this for?

Threat modeling

- Who is your adversary?
- What are you trying to protect?
- What can they do to find it?
- What are the consequences of a security fail?

Threat Modeling

“The threat model describes the risk, and the goal of the security plan is to reduce that risk as much as possible.”

- University of Hong Kong School of Journalism

Journalists

Glenn Greenwald (born March 6, 1967) is an American journalist, political commentator, lawyer, columnist, blogger, and author. He has been a columnist for *Guardian US* since August 2012.[1][2] Greenwald has practiced as a lawyer. He was a columnist for Salon.com from 2007-2012, and is an occasional contributor to *The Guardian*.[3][4][5] Greenwald worked as a constitutional and civil rights litigator. At *Salon* he contributed as a columnist and blogger, focusing on political and legal topics.[6] He has also contributed to other newspapers and political news magazines, including *The New York Times*,[7][8][9] the *Los Angeles Times*,[10] *The American Conservative*,[11] *The National Interest*,[12] and *In These Times*.[13][14]

Three of the four books authored by him have been *New York Times* bestsellers. Greenwald is a frequent speaker on college campuses, including Harvard Law School, Yale Law School, the

Glenn Greenwald

Born	March 6, 1967 (age 46) New York City, U.S.
Occupation	Political commentator, lawyer, columnist, blogger, and author
Nationality	United States
Citizenship	United States
Education	B.A., 1990 J.D., 1994
Alma mater	Nova High School George Washington University New York University Law School
Genres	Non-fiction, political and legal commentary
Subjects	US politics, law
Notable work(s)	*How Would a Patriot Act?* *A Tragic Legacy*
Partner(s)	David Miranda

http://en.wikipedia.org/wiki/Glenn_Greenwald

James Rosen (journalist)

From Wikipedia, the free encyclopedia

Not to be confused with the American journalist for The New York Times *James Risen.*

James Rosen is an American journalist and television correspondent. He currently works as a Washington, D.C. correspondent for the Fox News Channel.

Contents

1 Early life
2 Career
3 Justice Department investigation
4 Personal life
5 References
6 External links

Early life [edit source]

Rosen was born in Brooklyn to parents Myron and Adele Rosen. His parents moved when he was young to neighboring borough Staten Island and he went to public schools there. He graduated from Johns Hopkins University with a bachelor of arts degree in political science. He then attended the Medill School of Journalism at Northwestern University, graduating with a master's degree in journalism.[1]

Career [edit source]

Rosen's first job after graduating from journalism school was as a producer for the New York television channel NY1. He then worked at CBS News as a researcher for lead anchor Dan Rather.[2] Rosen also worked for WREX-TV, the local NBC affiliate in Rockford, IL.[*citation needed*]

Rosen joined Fox News as an on-air correspondent in February 1999. According to his Fox News biography, he has since reported "from 49 states and more than three dozen foreign countries across five continents".[1]

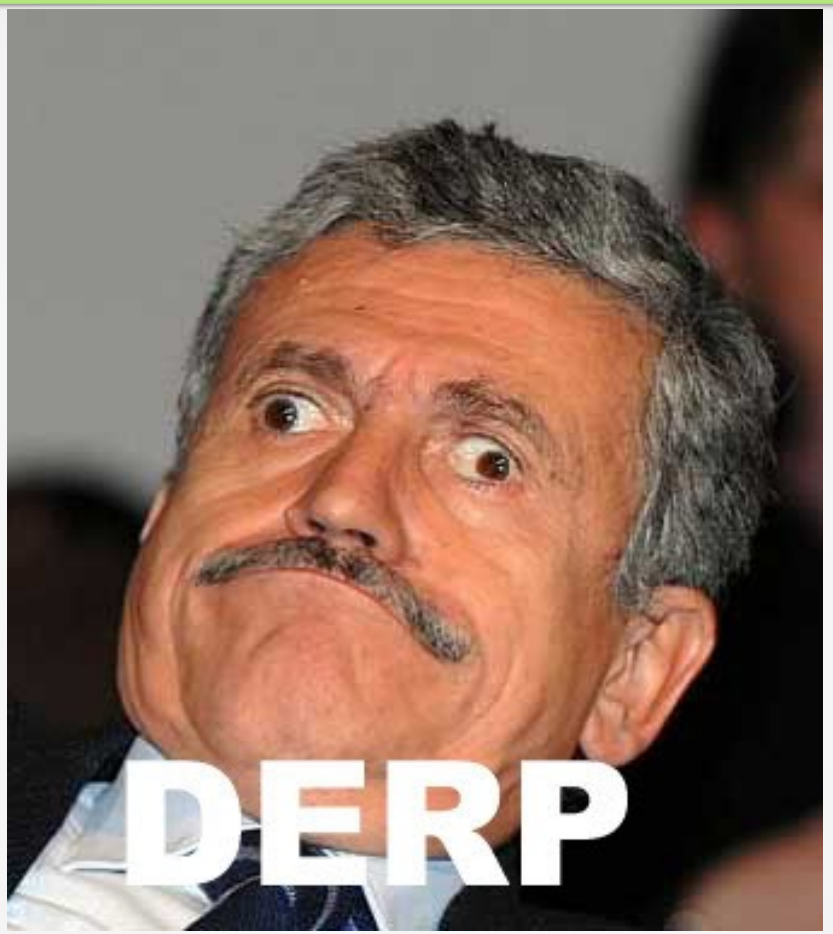
http://en.wikipedia.org/wiki/James_Rosen_(journalist)

Activist(s)

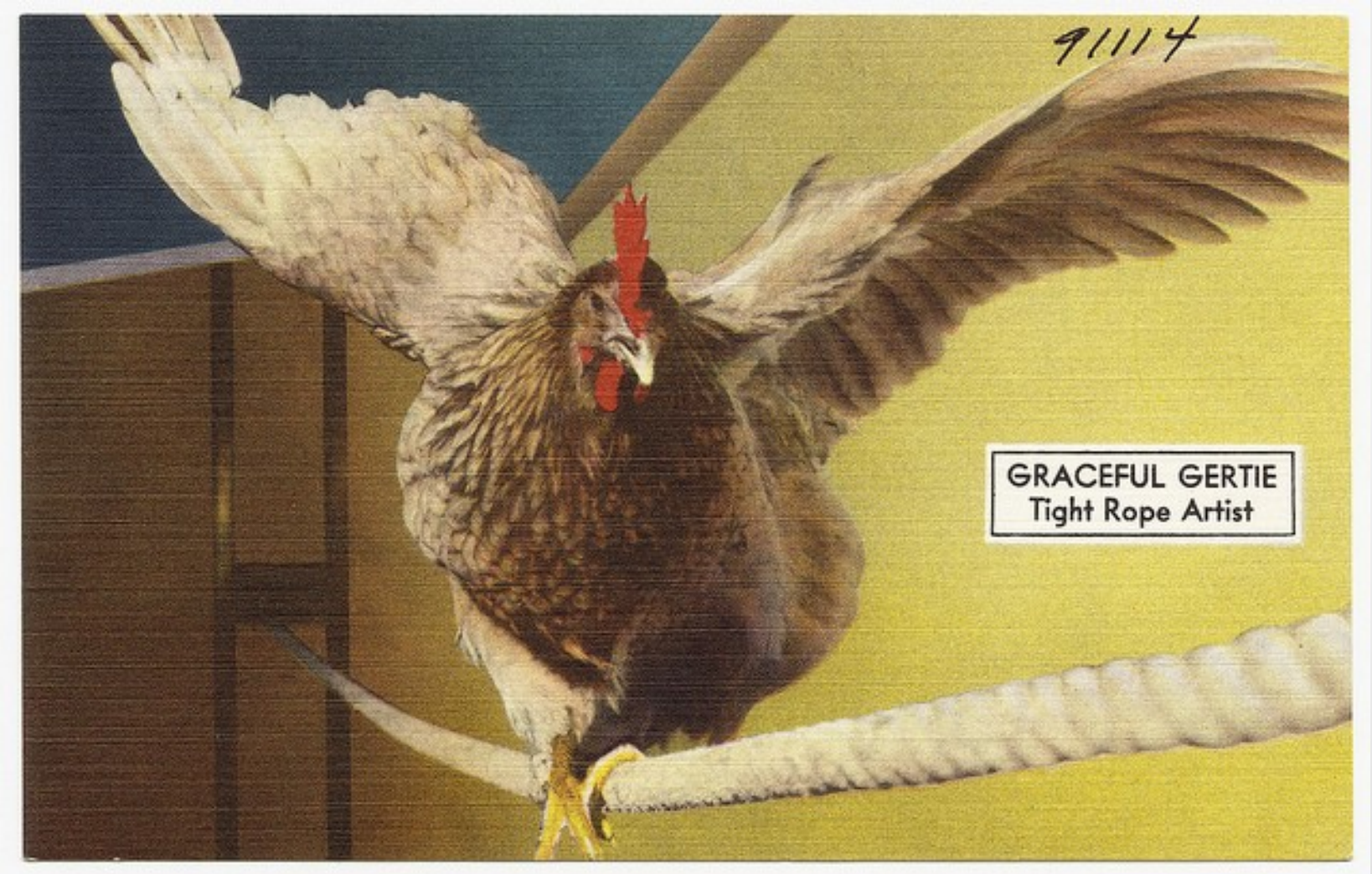
Copyright Jeremy Johnson

Dissidents

Everybody Else



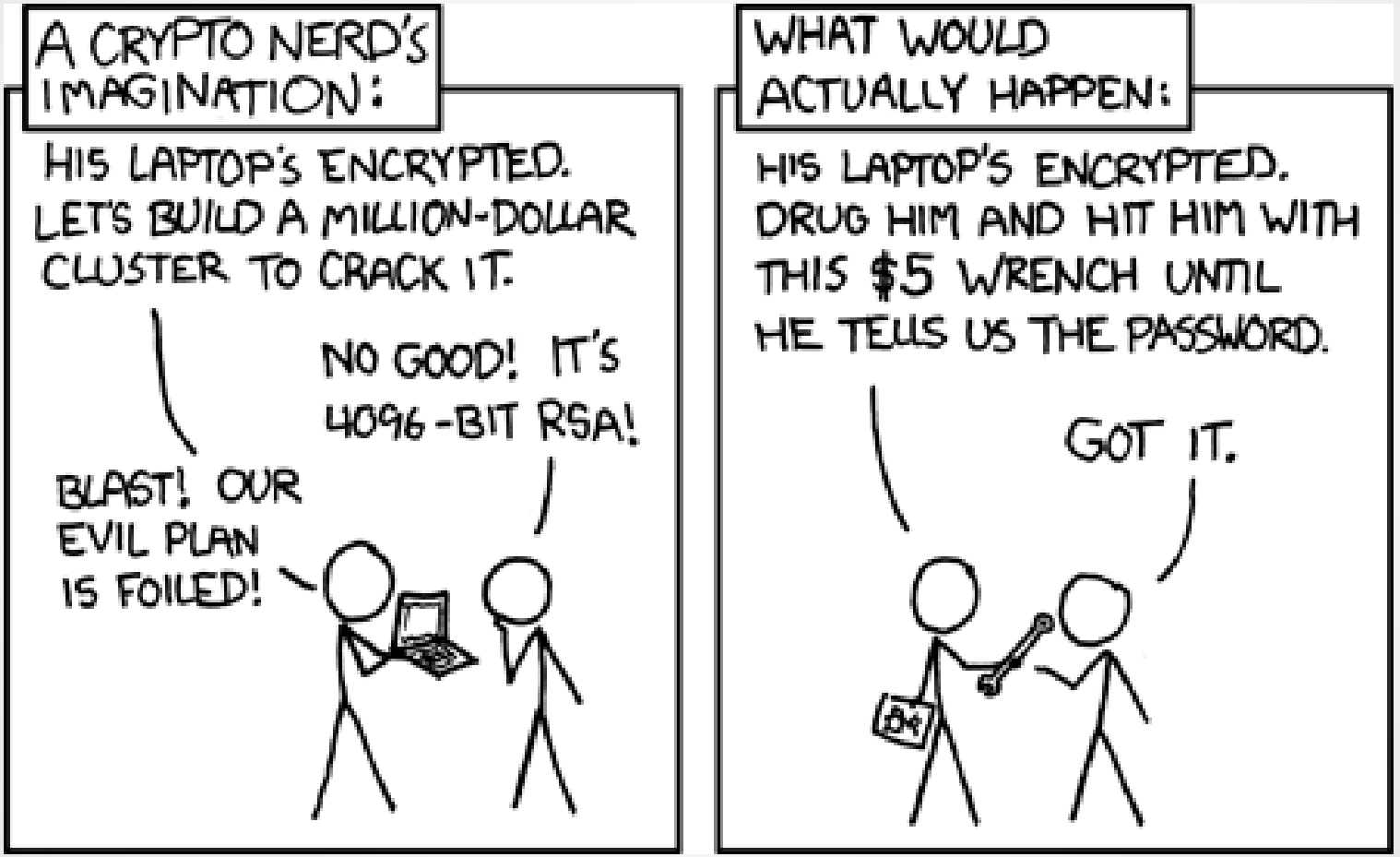
Security vs. Usability



Quick primer on physical attacks

- Ugh, bullet points :(
- Evil Maid
- Cold Boot
- “Snatch & Grab”
- Hardware keylogger
- Rubber Hose
- Firmware backdoor

Install an Operating System



http://xkcd.com/538/

Install - Basic

* BIOS Password
* Encrypt /home/user folder

http://www.flickr.com/photos/fragmentfi/5033666682/

Install - Intermediate

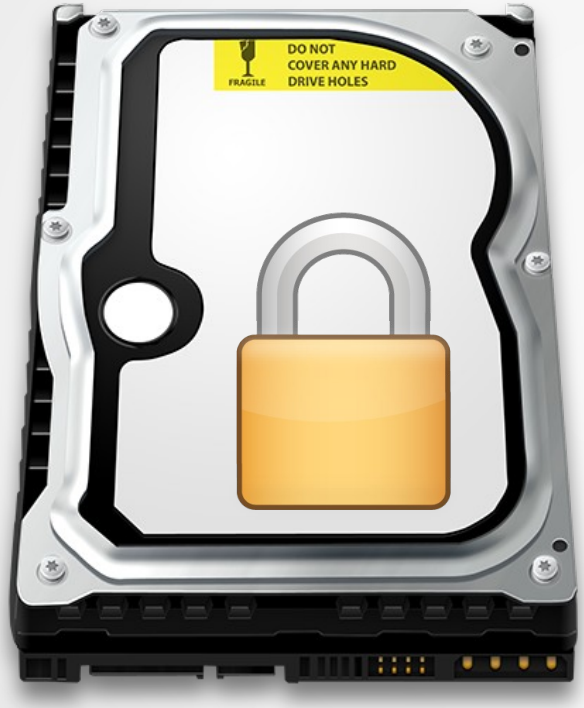
- Whole drive encryption (including swap)
- Use a LTS version of your preferred platform

Non-Encrypted /boot

Encrypted Root /

Install - Advanced

Encrypted Root /



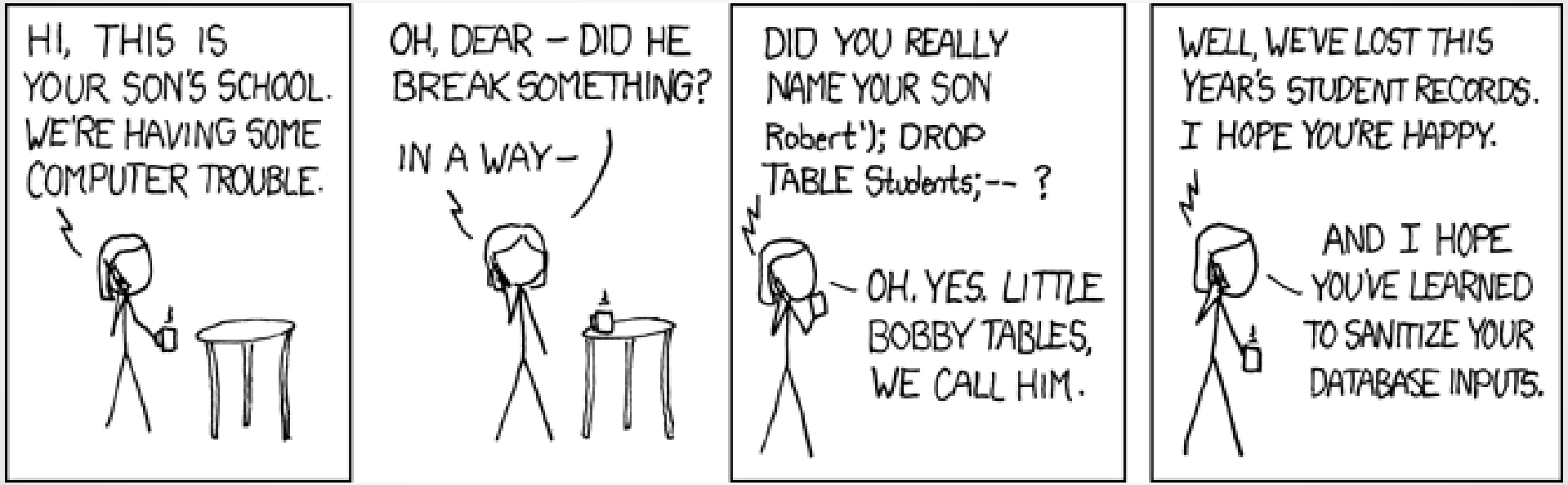
/boot

HD: http://bogo-d.deviantart.com/

USB Drive: http://gorganzola1.deviantart.com/

OS/App Hardening

(Another) relevant XKCD

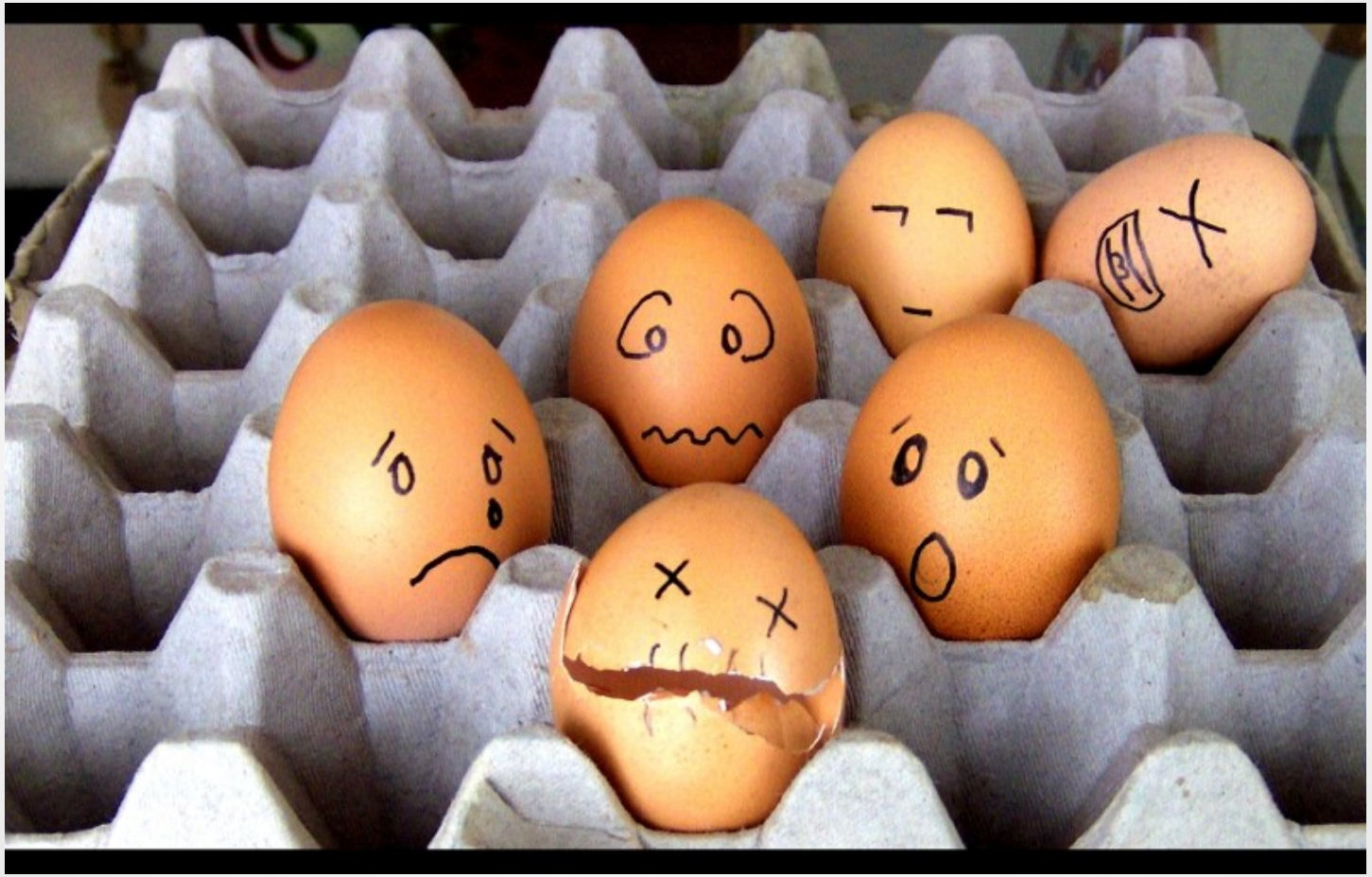


http://xkcd.com/327/

Primer on OS / App Attacks

- Application Flaws
  - 0-Day (unpatched/unknown) Vulnerabilities
- Privilege Escalation
- Information leakage
- Stupid Mistakes (EPICFAIL)

Hardening - Basic



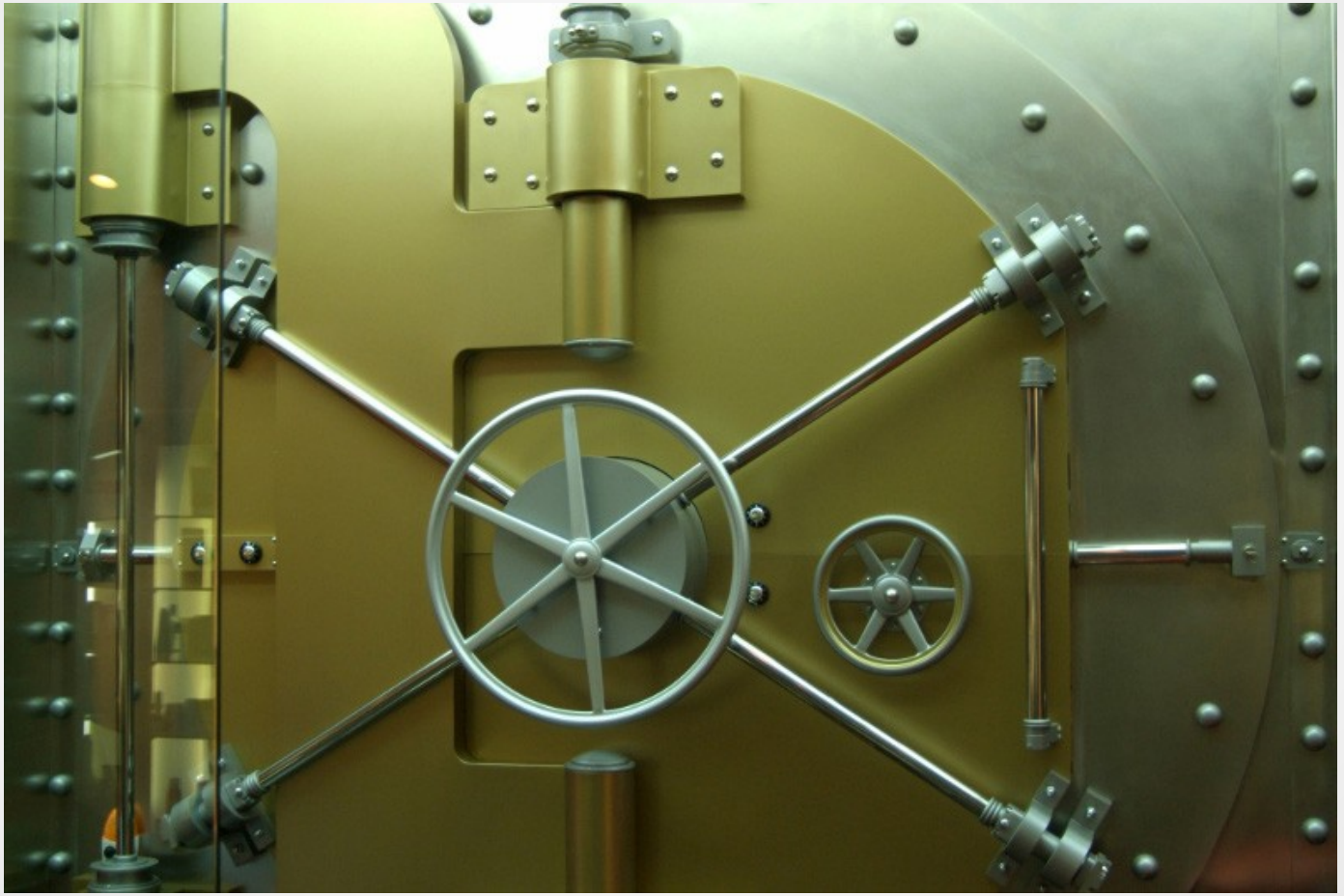
http://fav.me/d196lng

Hardening - Intermediate

- AppArmor
- Bastille Linux
- Grsec/PaX
- SELinux

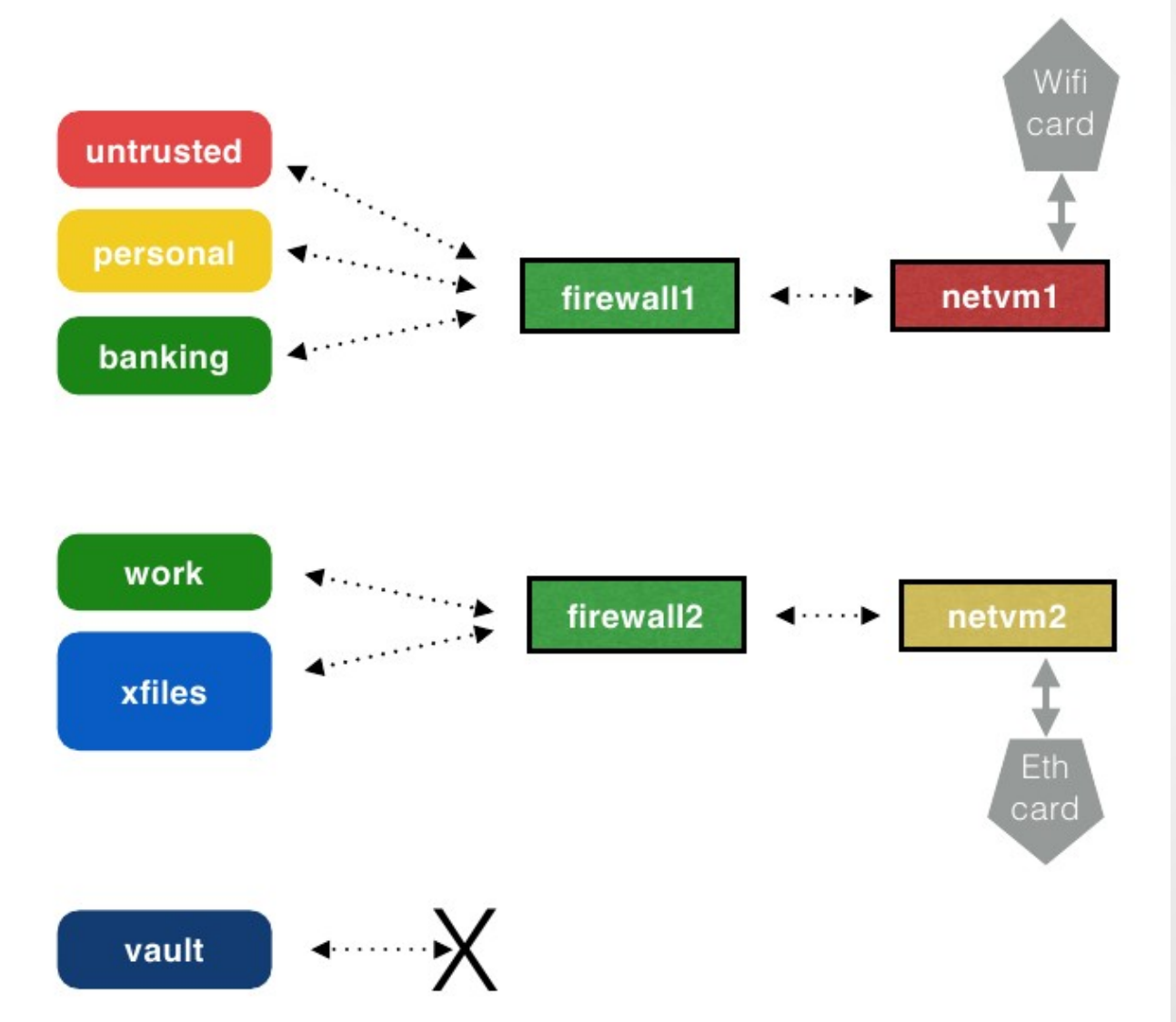
- Compartmentalize applications AND users -

Hardening - Advanced

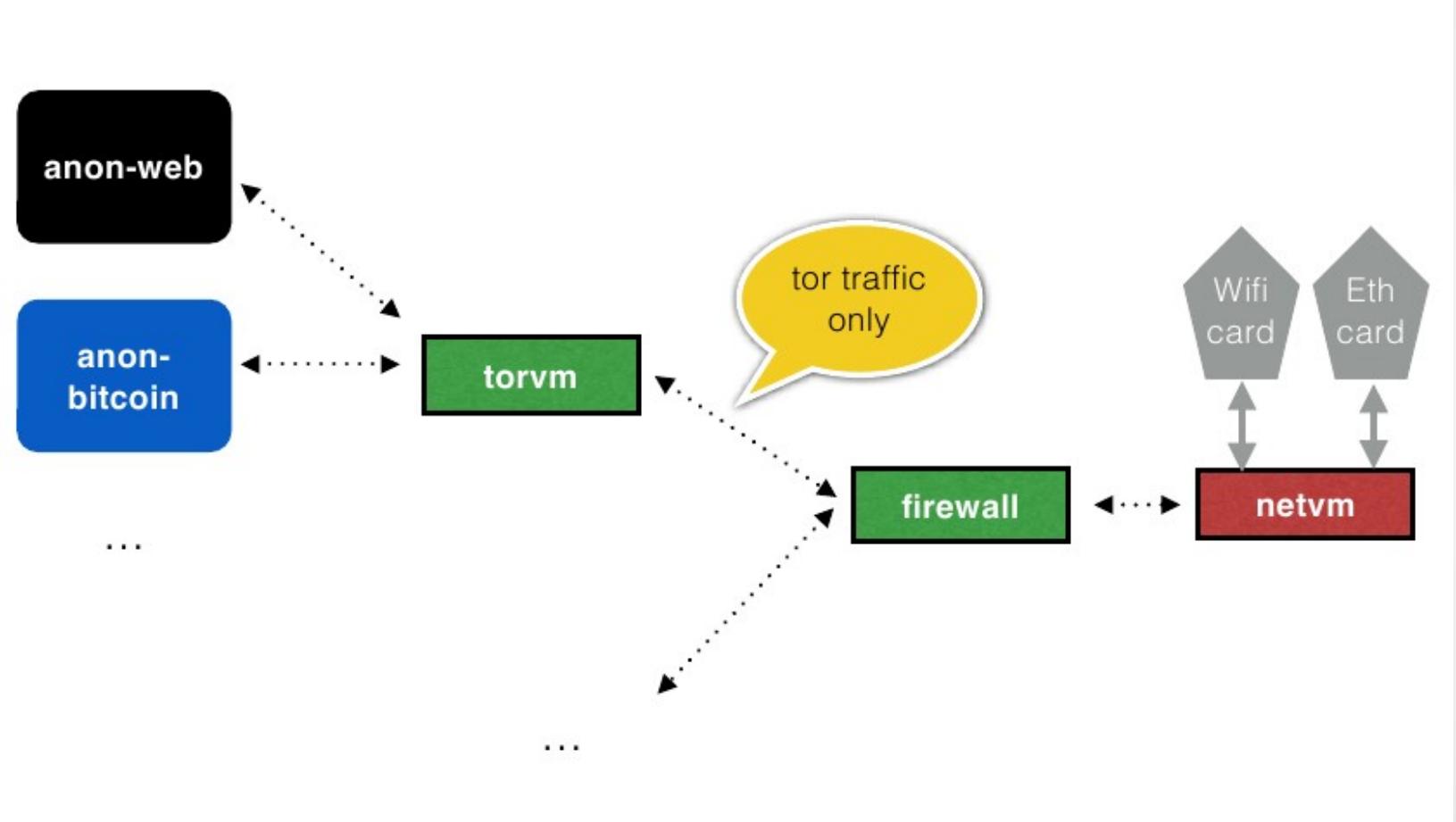


http://mjranum-stock.deviantart.com/art/Vault-Door-52681137

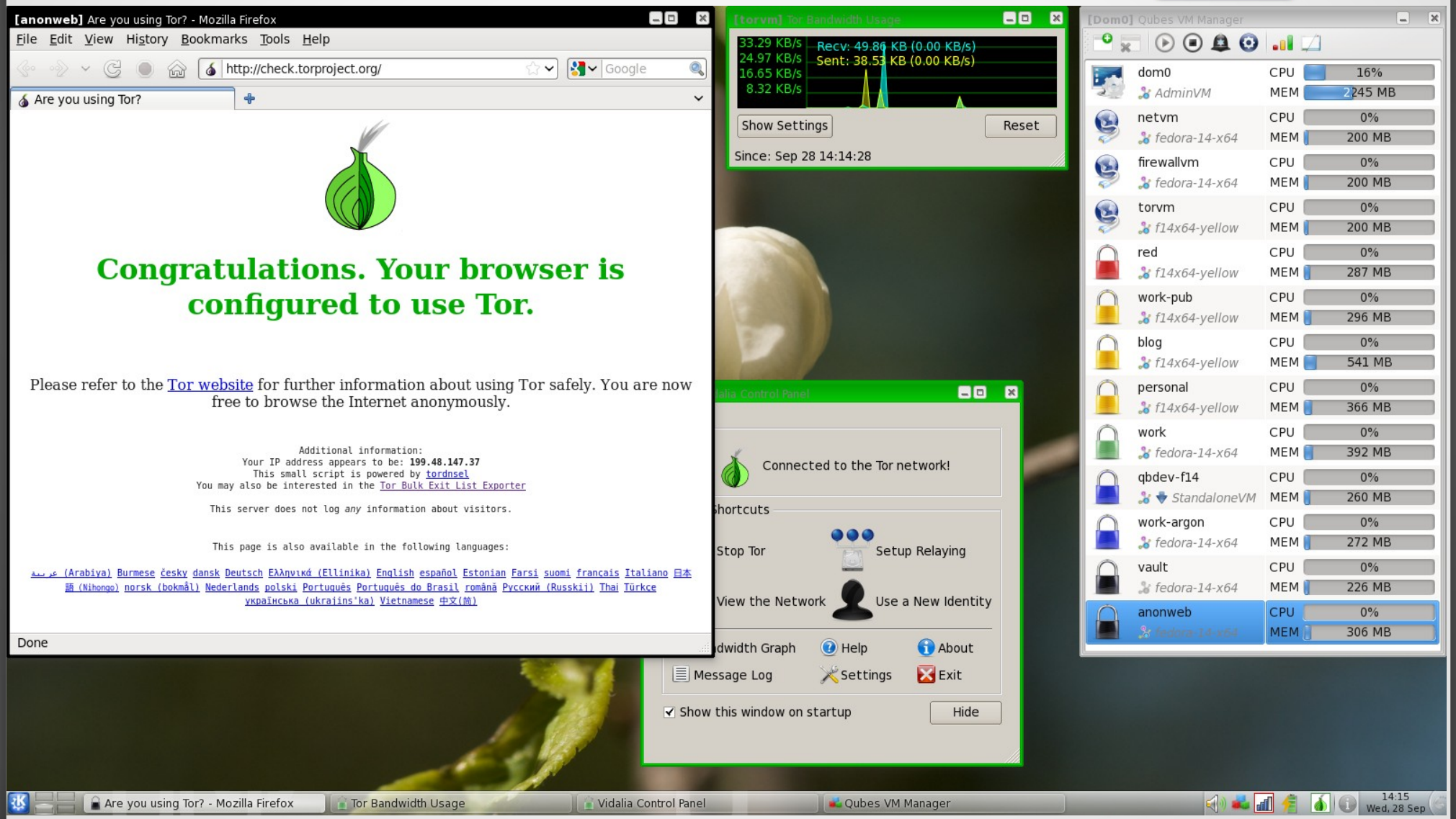
Hardening – Advanced - Qubes



Hardening – Advanced - Qubes



Hardening – Advanced - Qubes



Hardening - Extreme

Air Gap
Disable all the things

Communications

mQENBFEQTggBCAD1PQikd/85uYvBceqmZu+hi/jh5cCpPRSK8Fr575
GvGKMFKf9m4cHSG6T7Hb1OeBDMDPikvG28AQaMFtLqWvxOvAMn
KS4NnfgVeBoBX8w6i8Rz488TcaWERQUXz2c4QLJ+WzH5m0TGUdsp
9WlNX1ccJFf4M2bypZM7hprW4hmDcPAZAxaIuz9SkhvbSoFkRRLQxH
zUKB3rkgqN1sC4Ef996h0shz0SrwMm4+4dRqgMzIPleDFrZ+BAk96Fn
77kHsdXEm96smW9Y3KLrr26N5gYobYSL5tqdU6M/vqqQdNExJfjwQA
2ig/27yqQi5rQzBzGpwTUpFBRHafcSxQlo/hNABEBAAG0G0plcmVteS
A8amVyZW15QHNlY3RpdmEuY29tPokBPgQTAQIAKAUCURBOCAIbI
wUJCWYBgAYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQm
P9p0Ows3K5emQf+KpwauPK7EuOq3+3sUKPq3jvnwY535aHbtWa9Z+
NsnA9/4sg7r0TgNyEWVsR+quUDKx1iU/zHPoEbmPxrJeHgrkKfwoSIT
Cb/sLvP/UydJEwva5JnV32olEezrvWPMeJa/Sx+Vsz2umX5x0rmkujzAs
pHKKqOJFeamrMzjxth2D3BEoOSUxZBbZo5XHvtUVCxy//7LTfe/ZOtBx
o1b4lqZYVTiaHwtI8BoVrp6A7gXRMbPbjwXA8x7wAjc43U8yVSx208aE
QnhxQq90V/lrKCjTNidJhb8QpWlpB4AjkI3GAwdReRnjCqaW+NugVPqd
1bxp0FSzNZApDepPpyi4ohrkBDQRREE4IAQgAnEUnMdEoBMx1DFG
NdNer8uenXU/YsqqHb//BHv0LbybmxuxYRSM/zQ7opH6NNnBnKwXlo
Yb2FyiyYFSN6ia3JBTr/TtzuXZq6PhQd1zjxGp7FvKD1yZtV51124fpQ0f
75aRG2vtk//mgHH5XcG07oSfqgRDSIgca2JezN8vJ5X0BTRAogF4Exn
kz37+exTieAY8gedcdBXpAHP3vJfesjXQov/CBvKbbkyOO1+f2IsR6lK9S
Efd1gJc/IgcumFjZCK6PTzmRWPjICMjbzQeNNpN1S2hyOkatlYoj52xD3
6Pb9ZS1zT6exUM53LnWylnpSbPyacubCP/aY9skXkHjawARAQABiQE
lBBgBAgAPBQJREE4IAhsMBQkJZgGAAAoJEJj/adDsLNyuKMIH/3yscI
oKKepnyIQdMN2IfTxonRwUTyiGJVUw8Gqd5HRd70IrqX+HvUhLEPUZ
pQv+QhHXHZbu0d6lhHpqpEWb6SZzZ8aXNQxx9v9Kokv+GvT2etVIE
Nv7ApUAWrjQKx+TKr2wwSJW/VZCfVzrR6MD/AIeeGIvXhqTvWymm7
wtjH3/FctPRQ49sFsXWM+Mkcn4PTGkgFga5v7eEikSnnhX7TmPggDfn
TLacuujCwOct9keYd57EiMN/gQnn5YEoWLCLR32OoD5vS88KRlL5xe
RtnrdOQOWh894wJ1pl1sAlphFlXf9Fl7Nbr55IFlcqPKoieaUgRKdGvLFj
wWNImiZhh0==cOR6

Communications

Privacy

Anonymity

Security

PSA: Cell Phones

PSA: “Cloud” Services

“If you are not paying for it, you're not the customer; you're the product being sold.”
- blue_beetle on metafilter

Communications - Privacy

“The state of being free from intrusion or disturbance in one's private life or affairs”

“Where only the intended recipients can read a message”

- http://dictionary.reference.com/browse/privacy

Communications - Cookies!

Communications - Privacy Tools

Adblock Edge – Firefox/Chrome Extension

HTTPS Everywhere – Firefox/Chrome Extension

NoScript – Firefox Extension

BleachBit – Remove history, cookies, temp files, etc.

OTR: Off-The-Record Chat

VPN: Depending your threat model

Communications – Privacy Tools

Encrypted Communications,
Plugins for popular email clients

Jitsi – supports ZRTP, encrypted voice

TextSecure
– Encrypted text messaging for Android (iPhone soon?)

Tomb file encryption, compartmentalize data

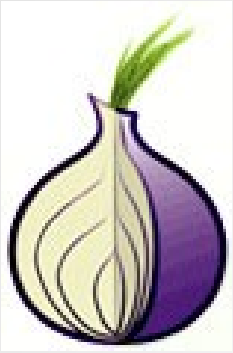
Communications - Anonymity

“without any name acknowledged, as that of author, contributor, or the like”

- http://dictionary.reference.com/browse/anonymous

http://www.flickr.com/photos/dfectuoso17/

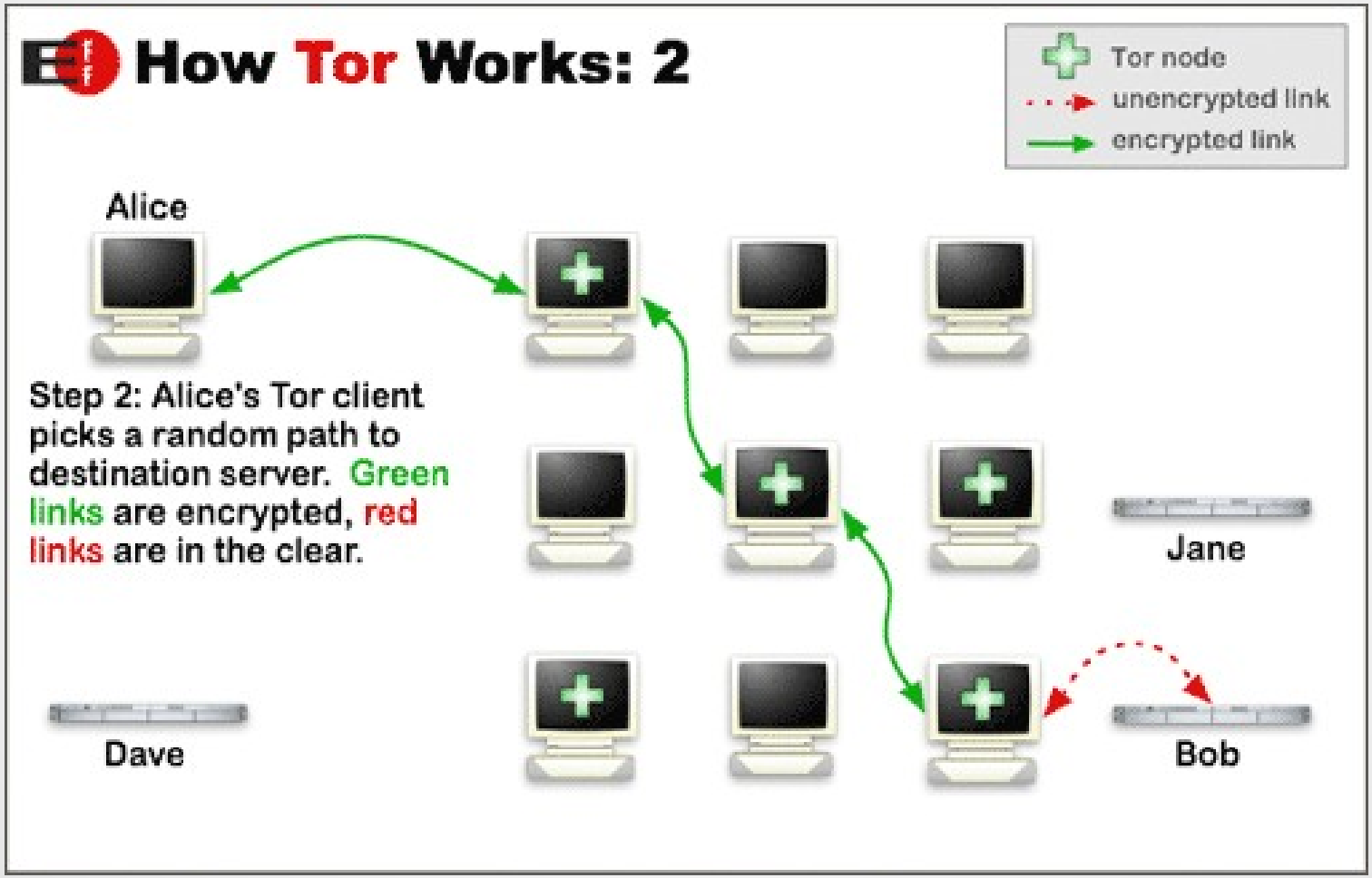
Anonymity - Tools



The Onion Router (Tor)

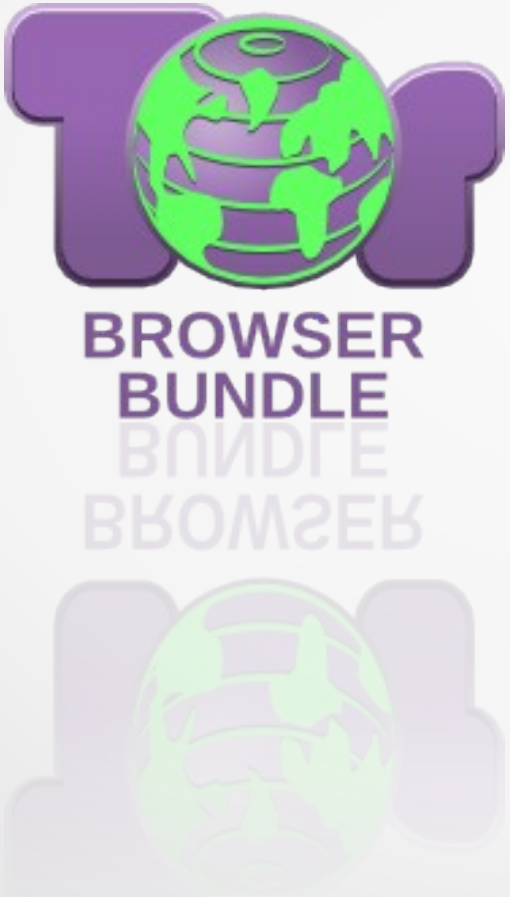
“The king of high-secure, low latency internet anonymity”
- NSA Top Secret Documents

Anonymity – Tools - Tor



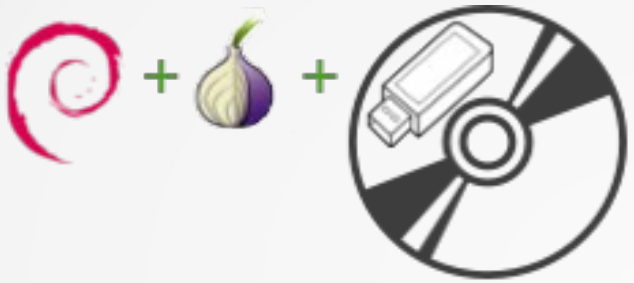
Anonymity - Tools

Tor Browser Bundle



* Windows
* Mac OS X
* Linux

Anonymity - Tools



T.A.I.L.S.*

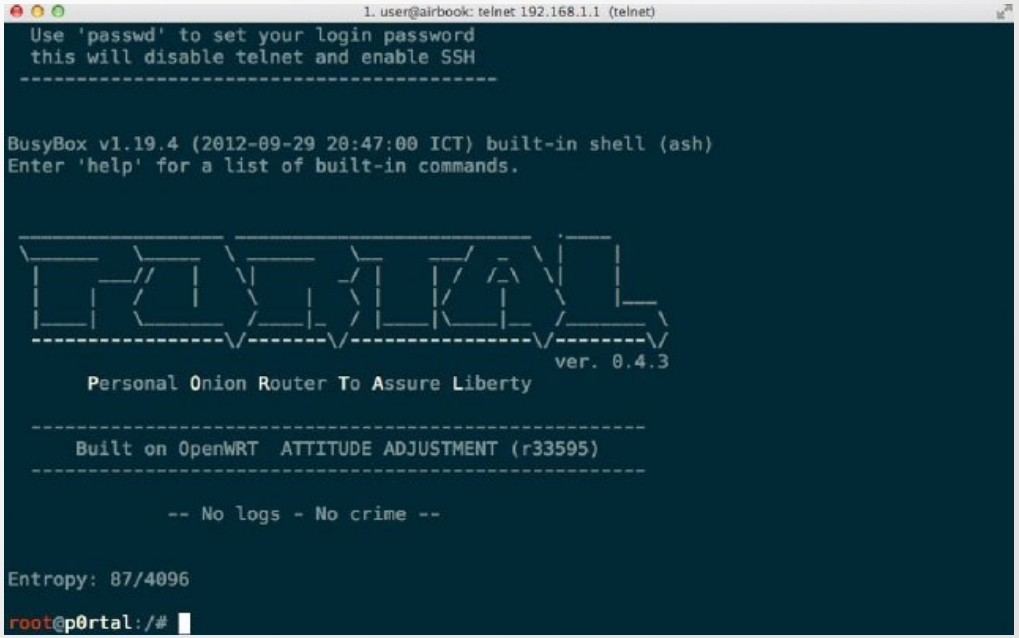
The Amnesiac Incognito Live System

* PITA 4 NSA

Anonymity Tools

Anonymity Tools

P.O.R.T.A.L.



Security

Freedom from risk or danger; safety.

- http://www.thefreedictionary.com/security

Security - Encryption

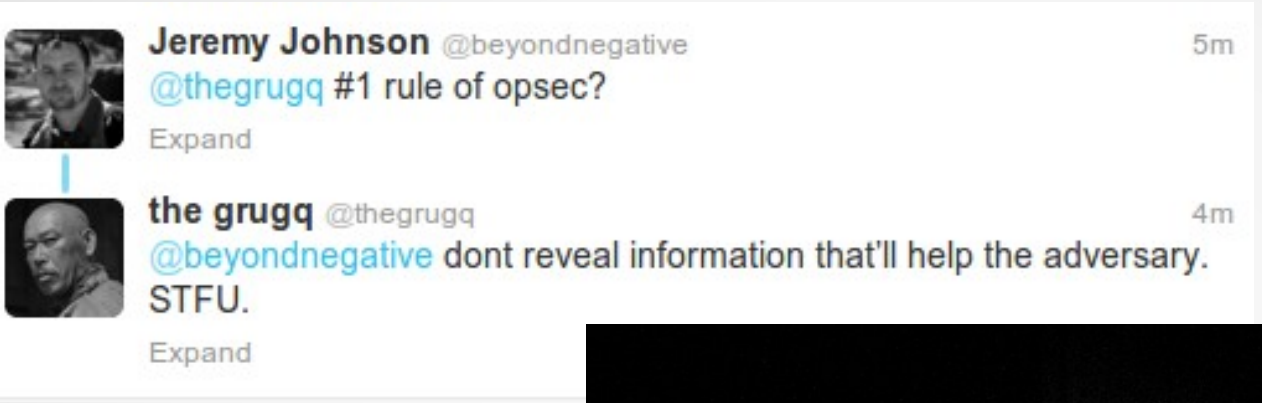
Encrypt all the things.

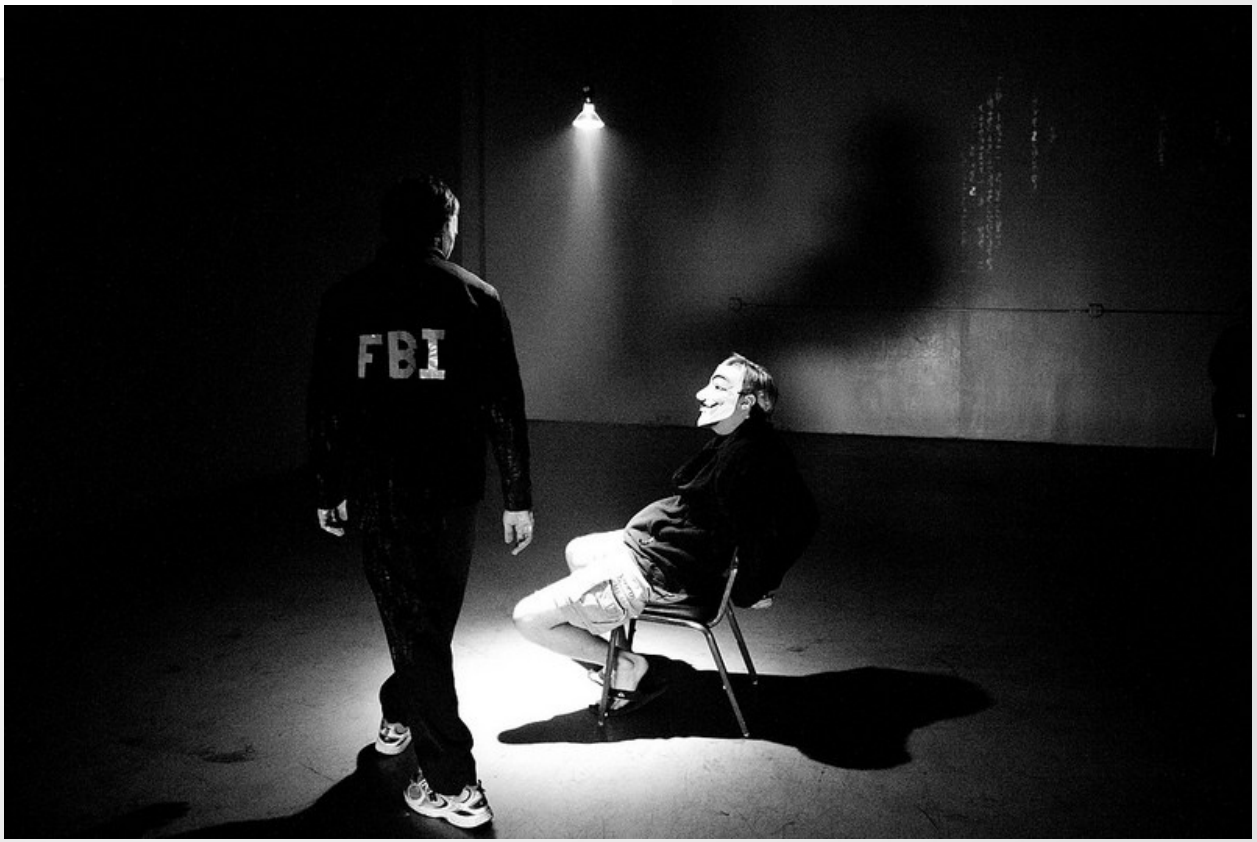
mQENBFEQTggBCAD1PQikd/85uYvBceqmZu+hi/jh5cCpPRSK8Fr575GvGKMFKf9m4cHSG6T7H
b1OeBDMDPikvG28AQaMFtLqWvxOvAMnKS4NnfgVeBoBX8w6i8Rz488TcaWERQUXz2c4QLJ+W
zH5m0TGUdsp9WlNX1ccJFf4M2bypZM7hprW4hmDcPAZAxaIuz9SkhvbSoFkRRLQxHzUKB3rkgq
N1sC4Ef996h0shz0SrwMm4+4dRqgMzIPleDFrZ+BAk96Fn77kHsdXEm96smW9Y3KLrr26N5gYob
YSL5tqdU6M/vqqQdNExJfjwQA2ig/27yqQi5rQzBzGpwTUpFBRHafcSxQlo/hNABEBAAG0G0plcmV
teSA8amVyZW15QHNlY3RpdmEuY29tPokBPgQTAQIAKAUCURBOCAIbIwUJCWYBgAYLCQgHA
wIGFQgCCQoLBBYCAwECHgECF4AACgkQmP9p0Ows3K5emQf+KpwauPK7EuOq3+3sUKPq3jv
nwY535aHbtWa9Z+NsnA9/4sg7r0TgNyEWVsR+quUDKx1iU/zHPoEbmPxrJeHgrkKfwoSITCb/sLvP
/UydJEwva5JnV32olEezrvWPMeJa/Sx+Vsz2umX5x0rmkujzAspHKKqOJFeamrMzjxth2D3BEoOSU
xZBbZo5XHvtUVCxy//7LTfe/ZOtBxo1b4lqZYVTiaHwtI8BoVrp6A7gXRMbPbjwXA8x7wAjc43U8yVSx
208aEQnhxQq90V/lrKCjTNidJhb8QpWlpB4AjkI3GAwdReRnjCqaW+NugVPqd1bxp0FSzNZApDep
Ppyi4ohrkBDQRREE4IAQgAnEUnMdEoBMx1DFGNdNer8uenXU/YsqqHb//BHv0LbybmxuxYRSM/
zQ7opH6NNnBnKwXloYb2FyiyYFSN6ia3JBTr/TtzuXZq6PhQd1zjxGp7FvKD1yZtV51124fpQ0f75aR
G2vtk//mgHH5XcG07oSfqgRDSIgca2JezN8vJ5X0BTRAogF4Exnkz37+exTieAY8gedcdBXpAHP3v
JfesjXQov/CBvKbbkyOO1+f2IsR6lK9SEfd1gJc/IgcumFjZCK6PTzmRWPjICMjbzQeNNpN1S2hyOk
atlYoj52xD36Pb9ZS1zT6exUM53LnWylnpSbPyacubCP/aY9skXkHjawARAQABiQElBBgBAgAPBQ
JREE4IAhsMBQkJZgGAAAoJEJj/adDsLNyuKMIH/3yscIoKKepnyIQdMN2IfTxonRwUTyiGJVUw8G
qd5HRd70IrqX+HvUhLEPUZpQv+QhHXHZbu0d6lhHpqpEWb6SZzZ8aXNQxx9v9Kokv+GvT2etVIE
Nv7ApUAWrjQKx+TKr2wwSJW/VZCfVzrR6MD/AIeeGIvXhqTvWymm7wtjH3/FctPRQ49sFsXWM+
Mkcn4PTGkgFga5v7eEikSnnhX7TmPggDfnTLacuujCwOct9keYd57EiMN/gQnn5YEoWLCLR32Oo
D5vS88KRlL5xeRtnrdOQOWh894wJ1pl1sAlphFlXf9Fl7Nbr55IFlcqPKoieaUgRKdGvLFjwWNImiZhh
0==cOR6

Security – Air Gap

Don't do it. Don't connect, ever.

OPSEC





http://www.flickr.com/photos/dfectuoso17/

OPSEC

“Paranoia doesn't work retroactively”
- grugq

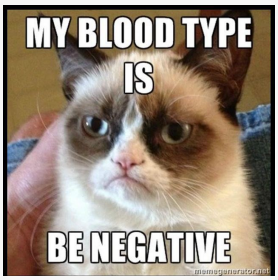
http://uberdiablo-pixels.deviantart.com/art/Disaster-Black-Box-120300934

Questions

@beyondnegative

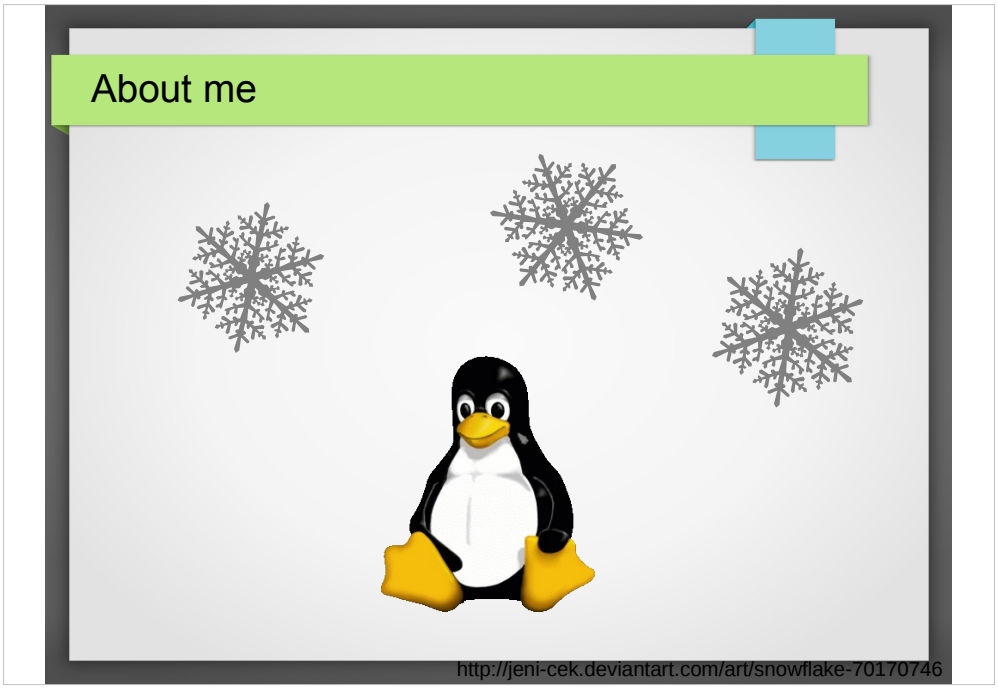
https://github.com/bneg/SeaGL

Protecting your privacy, anonymity and security with Linux and Open Source tools

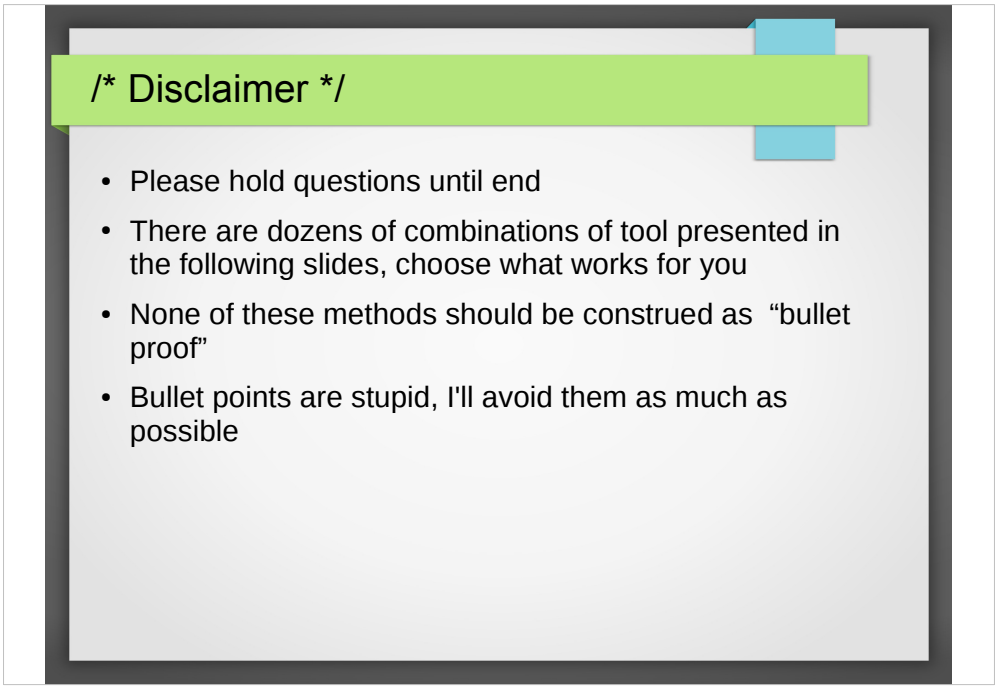


Jeremy (bneg)
@beyondnegative

This can be a very serious and dire presentation. I'm going to try and keep it light with some stupid memes because I've had enough depressing news for one summer



•This is usually the part where I would reveal my experience and awesomeness so that you'll be impressed and listen. However I'm not really a special snowflake and this presentation isn't about me. Its about /you/ and what you're going to do to protect your privacy, anonymity and security so that we may have a free and vibrant democracy.



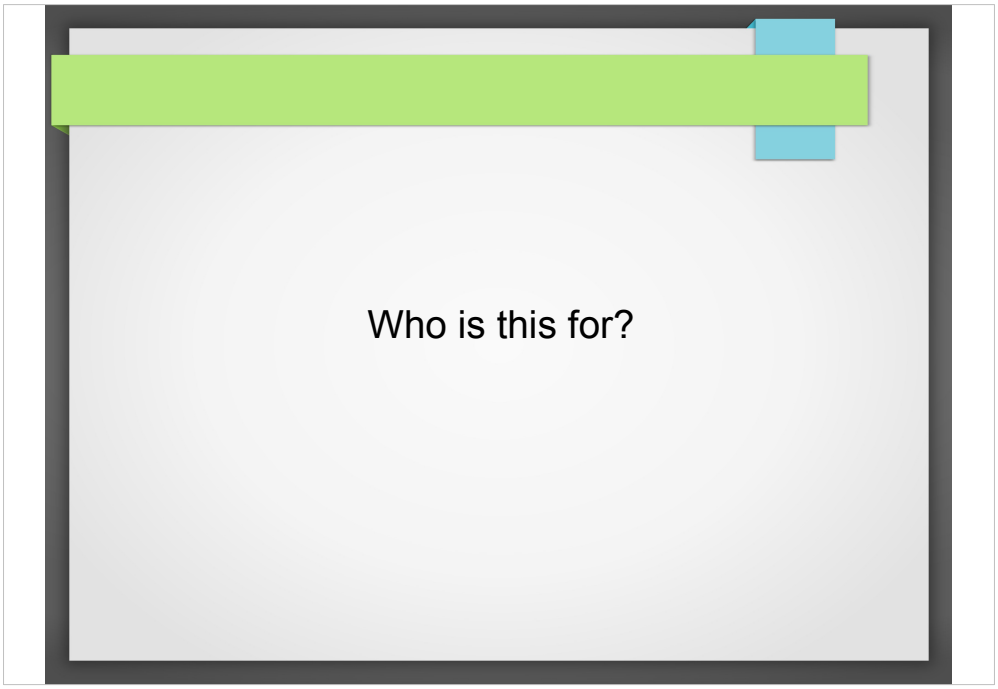
Please hold you questions until the end

*There are dozens of combinations for the tools presented in the following slides. Choose what works for you
*None of these methods should be construed as “bullet proof”

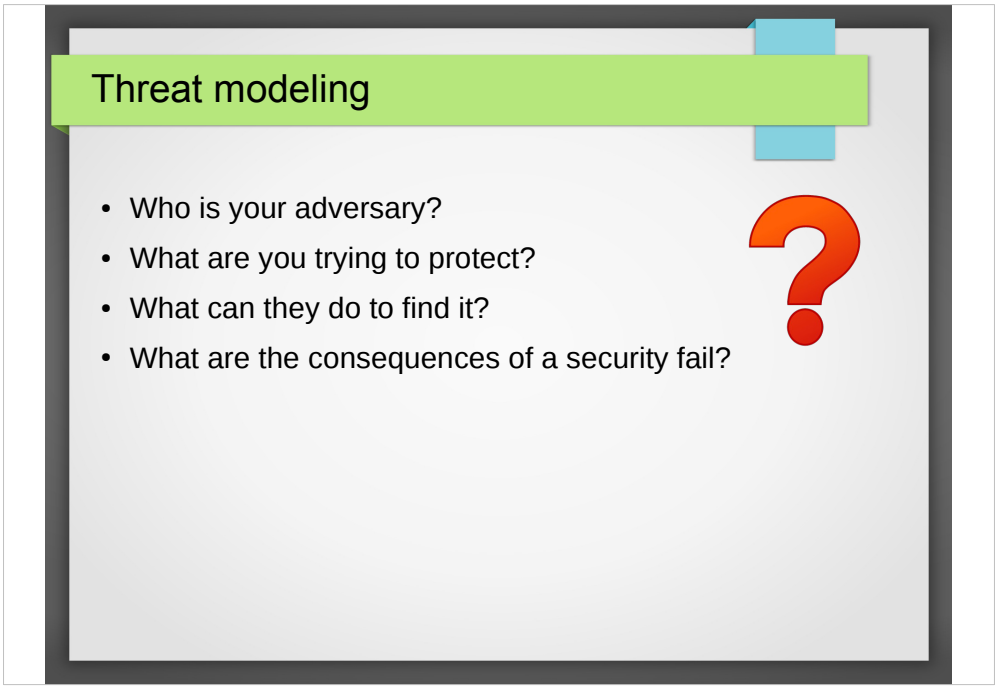
*My reference system is Ubuntu 12.04.3. Most of this stuff will work on other distributions esp. Debian based. This isn't an endorsement, just where I'm at right now

*Bullet points are stupid, I'll avoid them as much as possible

I've made an ambitious presentation subject. Thankfully I'll have time afterwards to answer questions, AND this slide deck and my resources used to build it are online

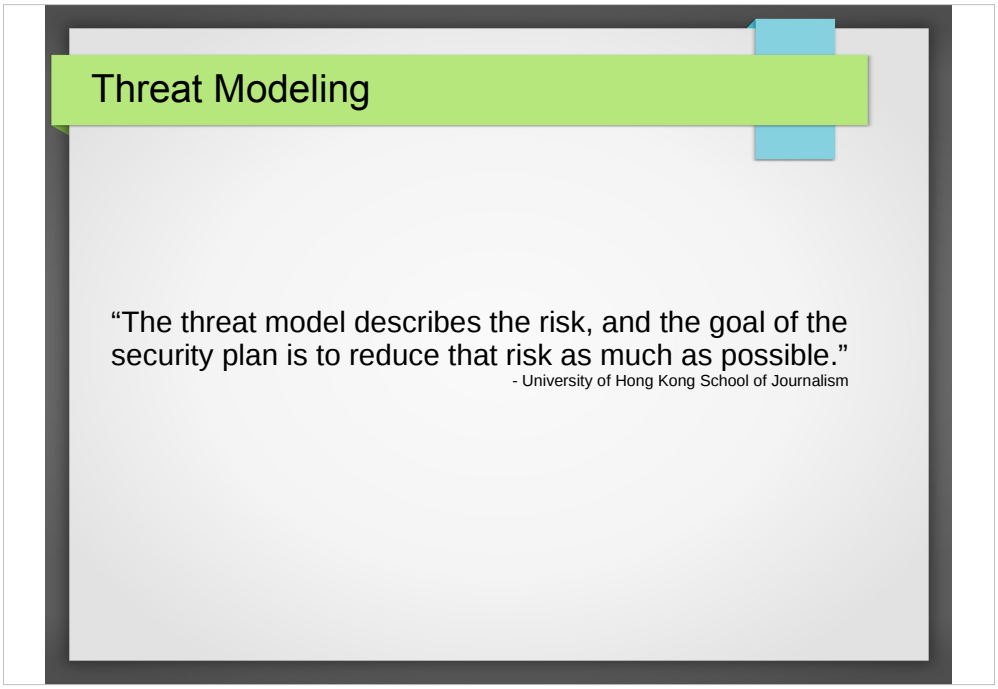


/* Next slide */

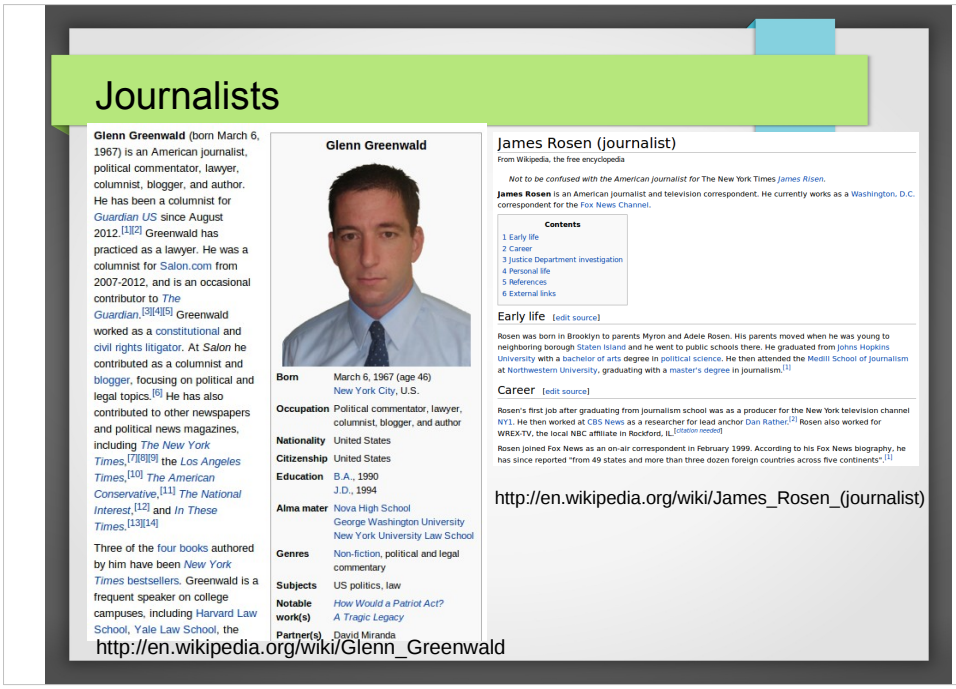


* Who is the adversary and what do they want to know? It might be a person, organization, state, or multiple entities.
* What needs to be kept private? Notes, documents, files, locations, and identities — and possibly even the fact that someone is working on a story or has a kind of information.
* What can your adversary do to find the information? including technical, legal, and social methods.
* What is the risk? What happens if an adversary succeeds in breaking your security. What are the consequences, and to /whom/? Which of these is it absolutely necessary to avoid?

http://courses.jmsc.hku.hk/jmsc6041spring2013/2013/02/08/assignment-6-threat-modeling-and-security-planning/



* The threat model describes the risk.
* The goal of the security plan is to reduce that risk as much as possible



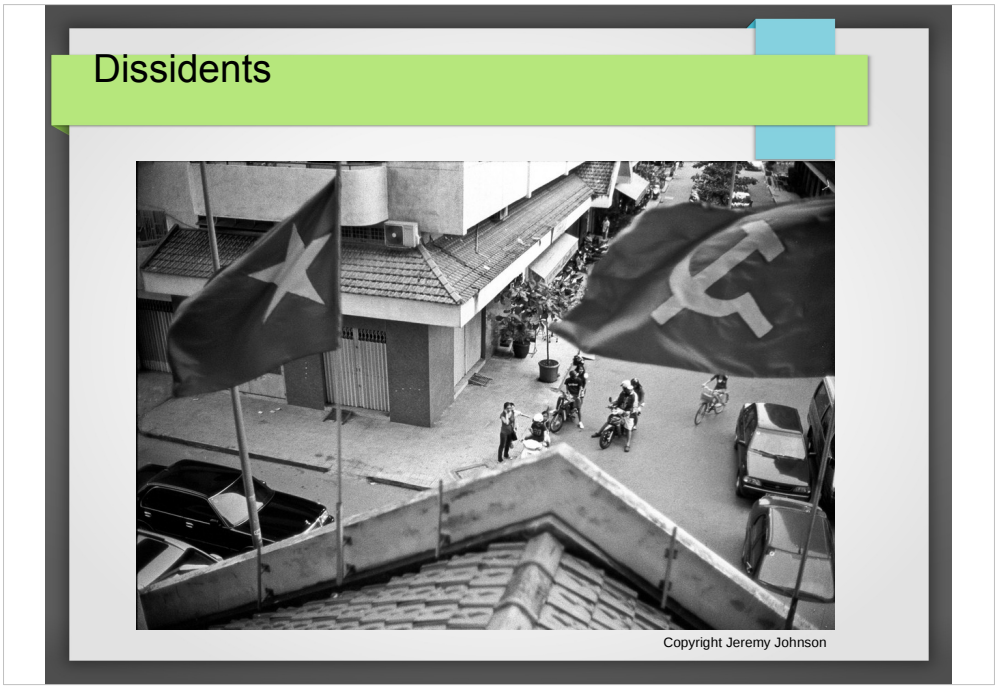
Glenn Greenwald, one of the lead reporters on the Snowden NSA leaks – His “adversaries” include people who would very much like to know what he's going to leak next so they can “get in front of it” and especially other countries wanting to know about the US intelligence apparatus

James Rosen, who the White House labeled as a “criminal co-conspirator” for receiving and reporting on classified information given to him from Stephen Jin-Woo-Kim on North Korea's plan to test a nuclear bomb.

Several recent and historical cases of local and federal agencies tracking, monitoring, and disrupting protesters and activists

Canada Olympics: Chris Shaw, Neuroscientist, outspoken critic of 2010 Canada Winter Olympics was followed and monitored for his involvement in anti-olympics protests

WA State: an Army CID member infiltrated protest groups using the alias John Jacob he then provided information on the groups to the Army, law enforcement agencies and private security firms in an effort to thwart protests and target the protesters



Dissidents and activists in foreign countries who may experience far worse punishment than their western counterparts.

Usually in highly repressive government regimes

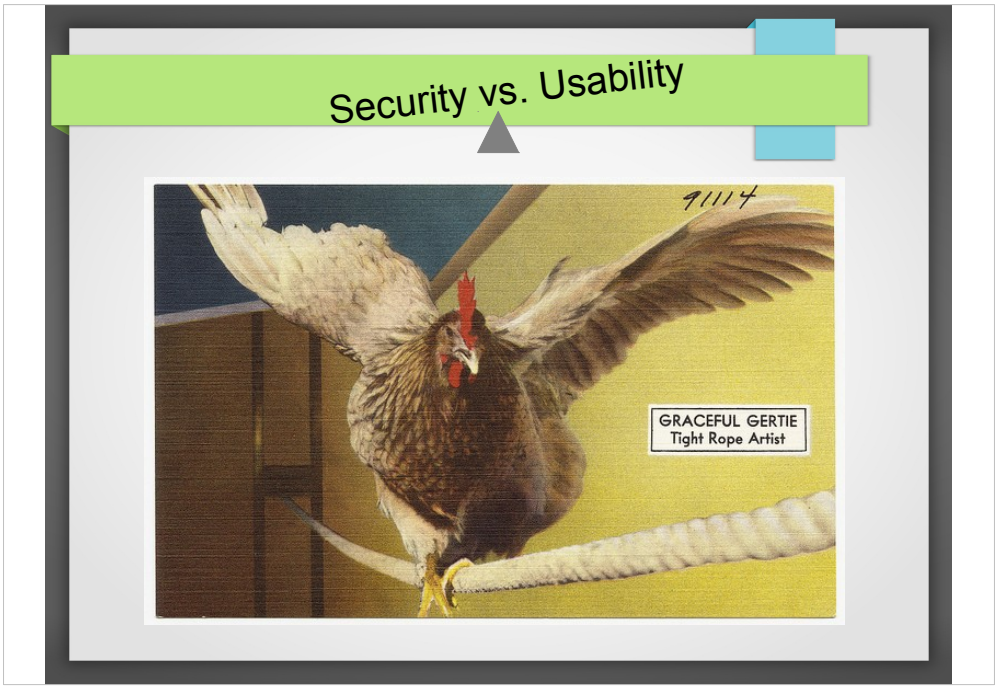
Sent malware via email, traffic is monitored or blocked. Often very serious consequences for speaking out against the government

Insurance companies, banks, retailers, and more are all looking for ways to profile and profit from you, your activities, and your data. They get to keep and profit from this data FOREVER – You may not want this, or simply want to have some control

Your social media history may someday determine a loan status, or “liking” popular junk food brands may increase insurance premiums

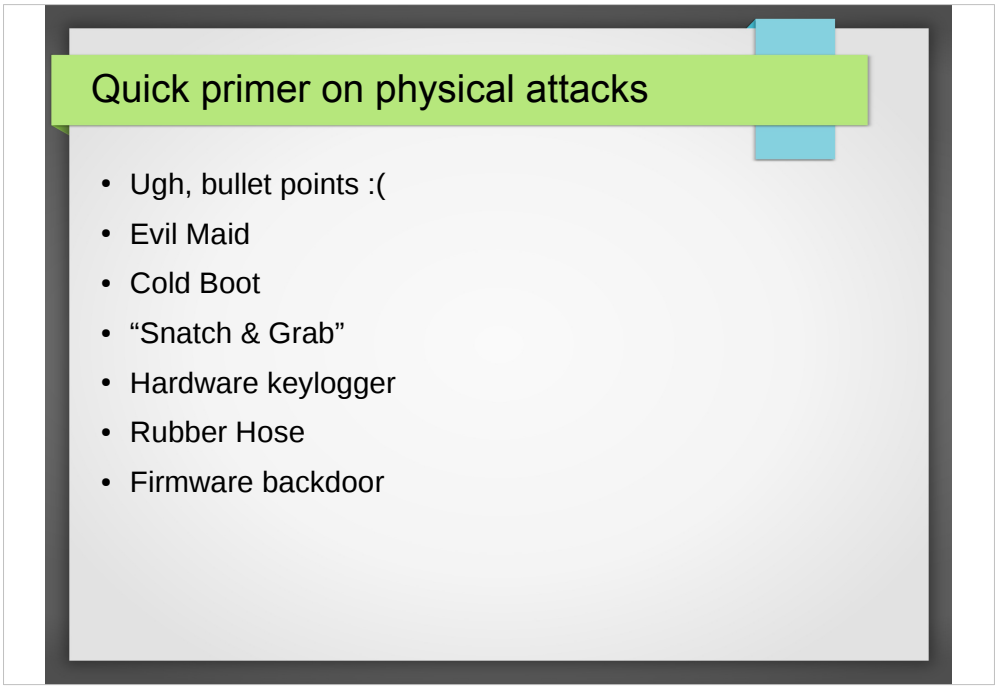
Discussing your health with family members may get you targeted in the next round of employer lay-offs (don't want sick employees who'll use sick time)

Just because you don't want something public, doesn't mean its wrong or bad or illegal.

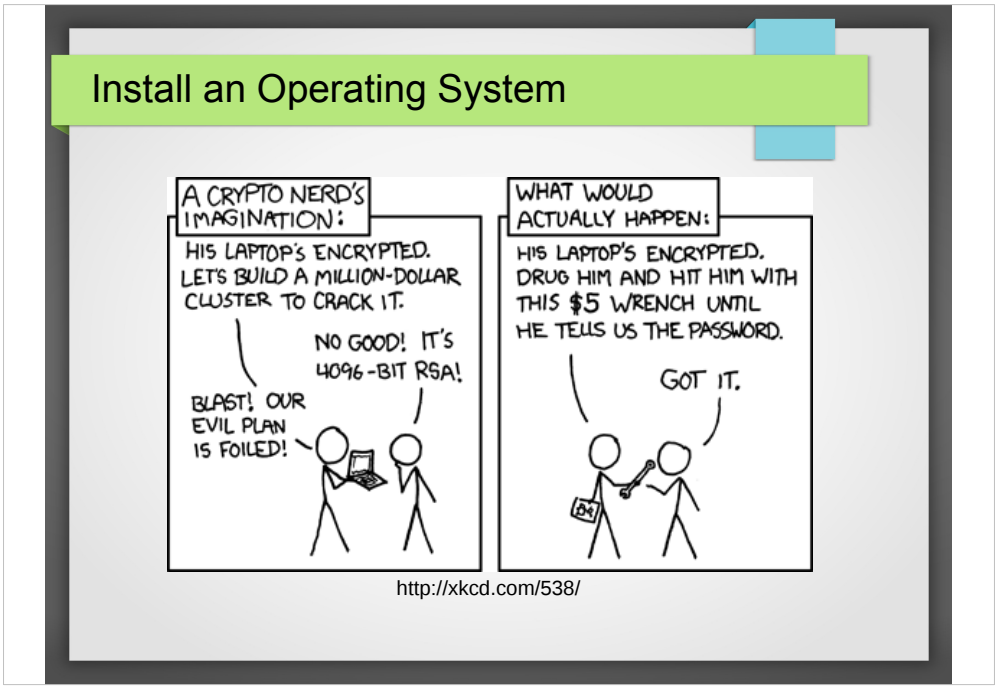


Finding the right balance between security and usability is a huge challenge. Some of the tools and techniques discussed are complicated, easy to get wrong, and not viable for everyday tasks.

Developing a threat model can help you determine what tools and methods to use in your particular scenario



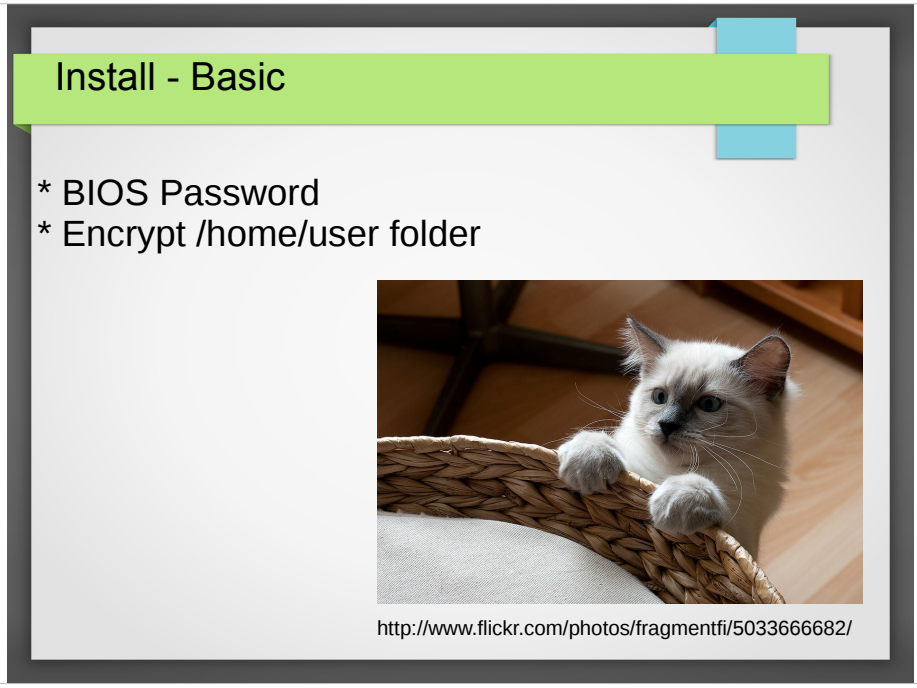
* Evil Maid: Unattended device has the kernel or hardware backdoored for later or persistent access or simply HD copied
* Cold Boot: From a running system, power down the computer violently (pull plug), freeze the RAM, remove RAM, read contents of memory including cached crypto keys (This is what convicted “Max Vision” in Kingpin)
* Snatch & Grab: Wait until the machine is decrypted, ie. Wait in coffee house, then grab machine and begin data ex-filtration – Note, compartmentalization can mitigate this
* Hardware keylogger: Self-explanatory, if you lose control of your hardware, who knows?
* Rubber hose: Ouch! Please let me give you all my passwords! PLEASE!!! D:
* Firmware Backdoor: VERY advanced, impossible to detect, perists through OS installs – Firmware over write **might** work if other firmware doesn't catch it



The math is good. The human is the weak link.

The idea here is not too make the data IMPOSSIBLE for the adversary to recover, but very expensive in time, money, and risk to recover. If /YOU/ are able to recover the data, then it is at least probable that your adversary will be able to recover the data given the aforementioned time, money, risk.

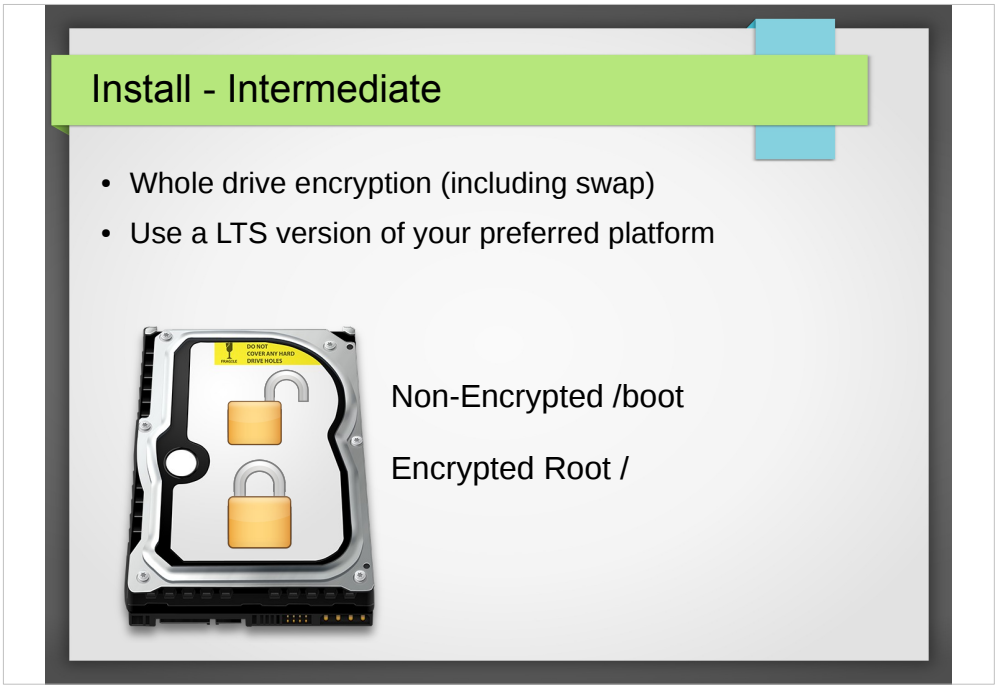
Lets make it expensive and risky for our adversaries to spy on us.



BIOS Passwords, Encrypt home folder

Simple to do, simple to manage, little overhead or learning required, often either default in newer operating systems, or easy to turn on

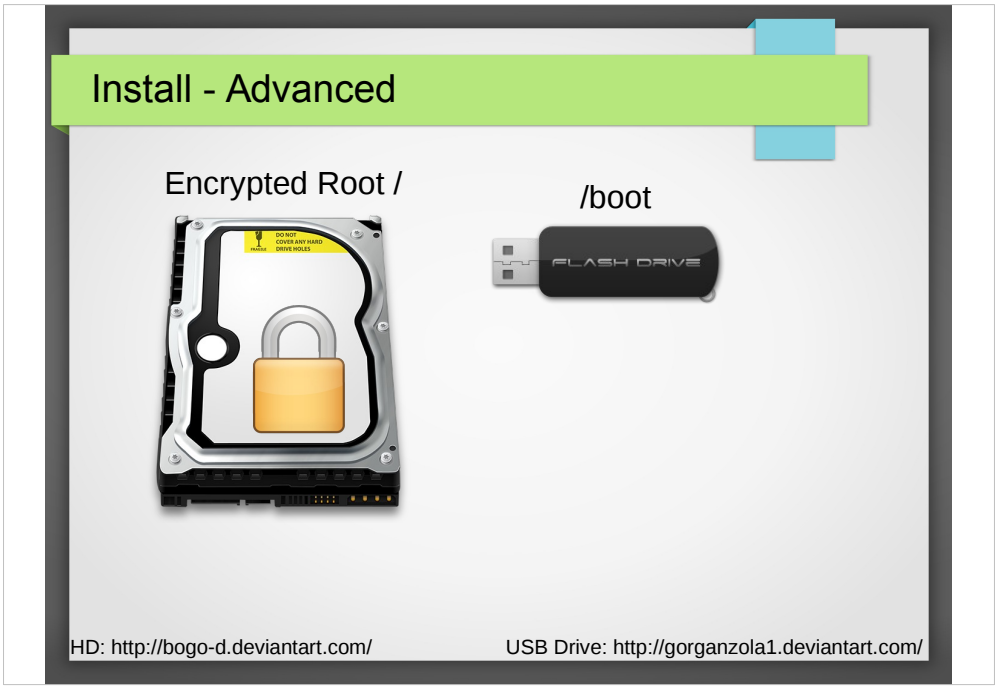
* Protects: Stolen laptop, discovery of private/personal files, gives compartmentalization from other users of the device/machine
* Vulnerable: Evil Maid attack, OS information gathering, potential evidence gathering from SWAP, Rubber Hose, cold boot, snatch & grab, password cracking



Whole drive encryption, with unencrypted. boot partition (default on some systems)

Sometimes a special install disk is needed, or advanced partition management during the install process

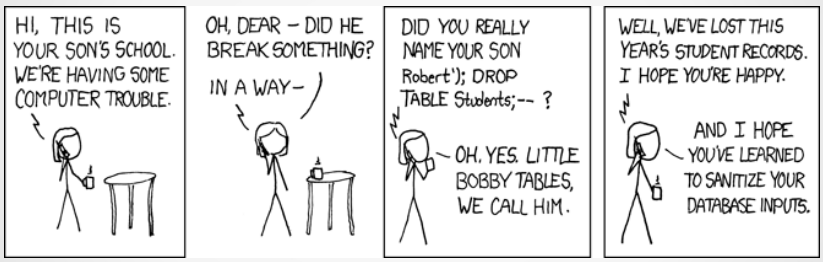
* Protects: Stolen laptop, discovery of personal files, discovery from OS and SWAP, password cracking
* Vulnerable: Evil Maid, Rubber Hose, cold boot, snatch & grab



Whole drive encryption, with boot partition on removable USB device
* Protects: Stolen laptop and discovery of files, Evil Maid (assuming USB is kept on person), Rubber Hose (assuming USB is off-person, ie. shipping it to your final destination when traveling internationally to avoid customs searches)
* Vulnerable: Loss of USB, Compromise of USB, Rubber hose (assuming USB is on-person), cold boot, snatch & grab

OS/App Hardening

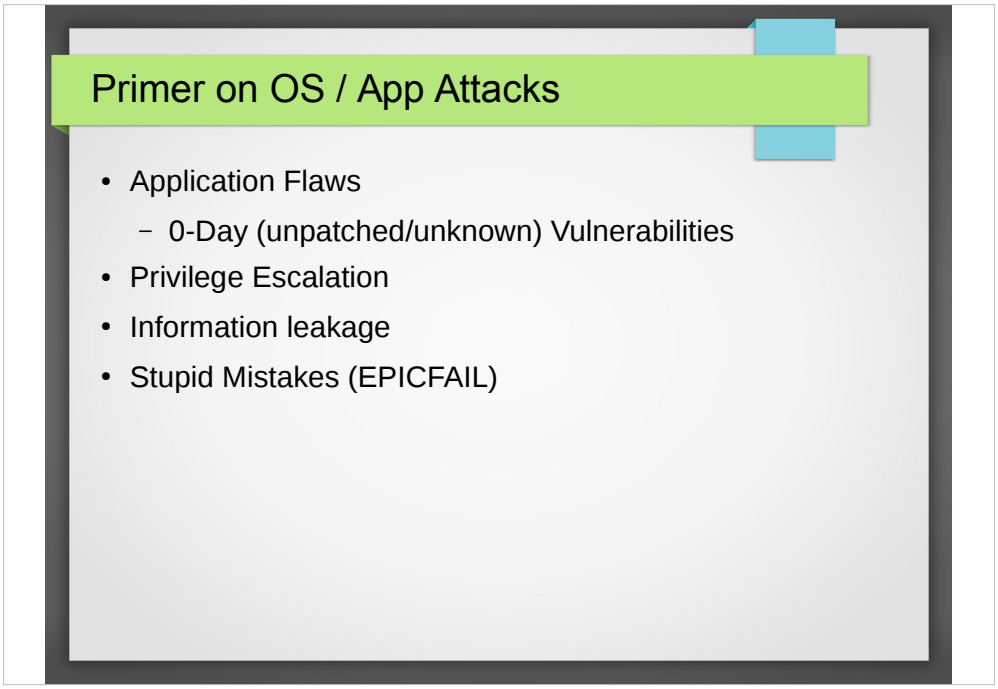
(Another) relevant XKCD



http://xkcd.com/327/

Sanitize your inputs

Flaws in applications or systems can have devastating consequences. The goal, if possible, is to minimize the impact of these flaws as much as possible.

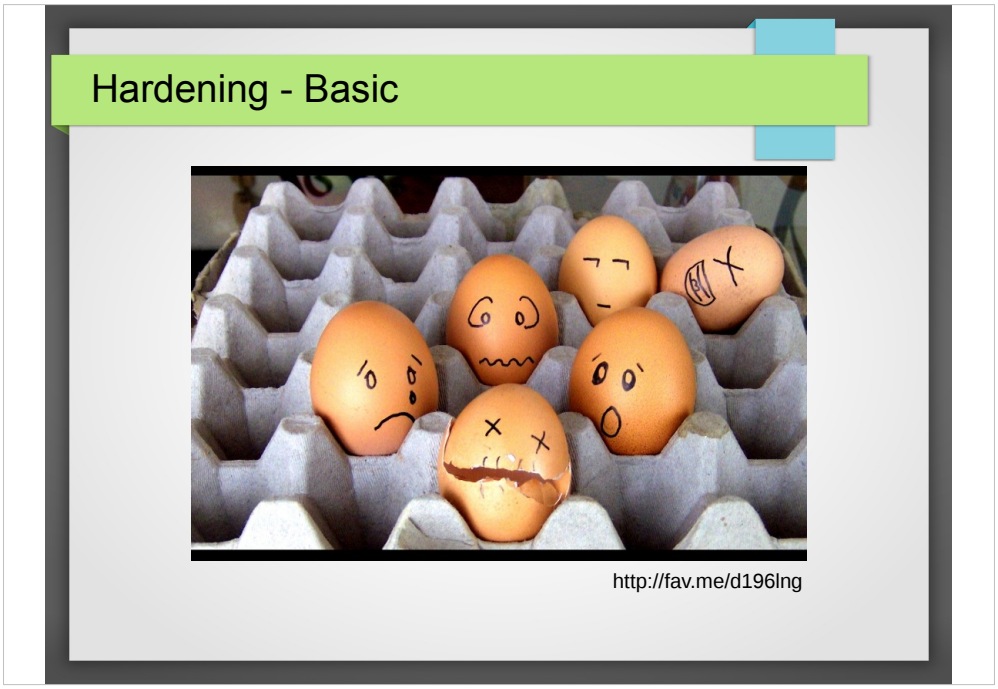


Bugs often lead to security vulnerabilities. The current state of computer security means that applications that get compromised generally have at least read access to nearly EVERYTHING

Privilege escalation: an authenticated user or application elevates its privileges exploiting a weakness or weaknesses in the operating system or application

Information leakage is caused by applications that share too much about themselves to unauthorized users (log files)

Stupid mistakes, sudo rm -rf / , priviliged users misconfigure a system or perform unintended config changes



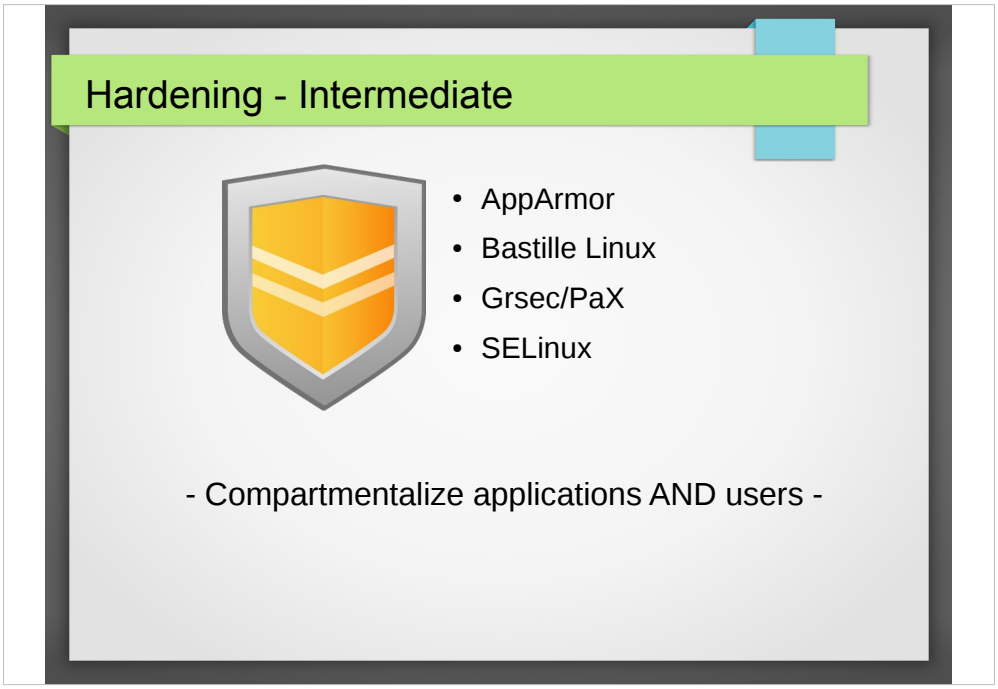
Hardening is not an easy or basic task. Find an OS that focuses on security by design or default. Ubuntu is not necessarily one of those

*Prefer LTS distributions, install only the software you REALLY need to minimize attack surface area, avoid flash & java when possible

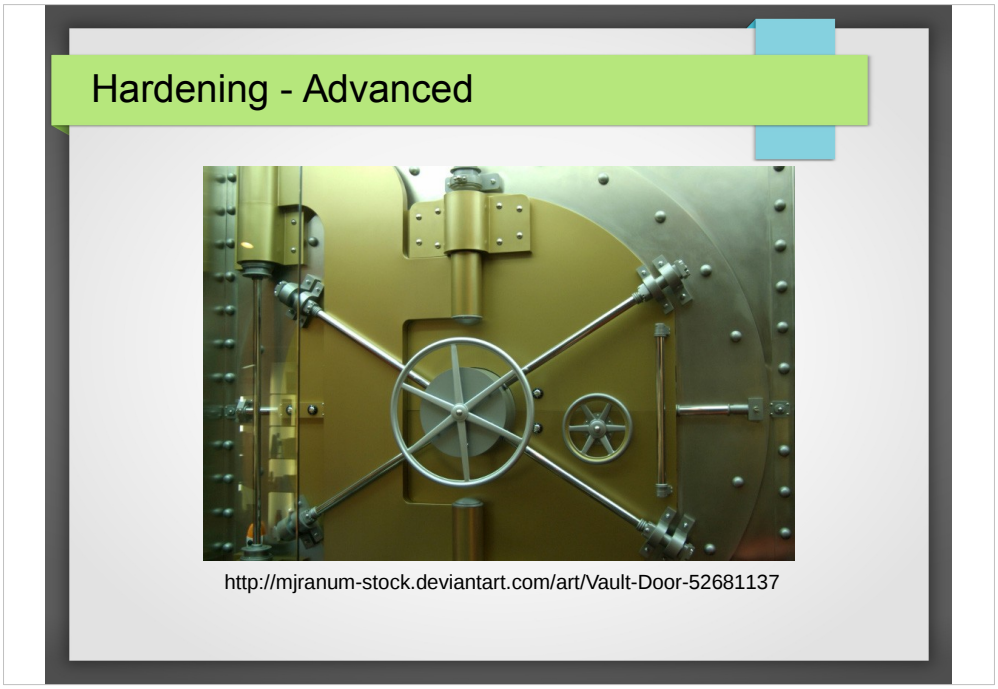
* Protects: Common vulnerabilities

* Vulnerable: 0-days, inexperienced users, poor configuration (see Ubuntu unpriv date change to allow sudo)

*BSD, Debian stable, CentOS, SSH server are examples of tried and trued software packages

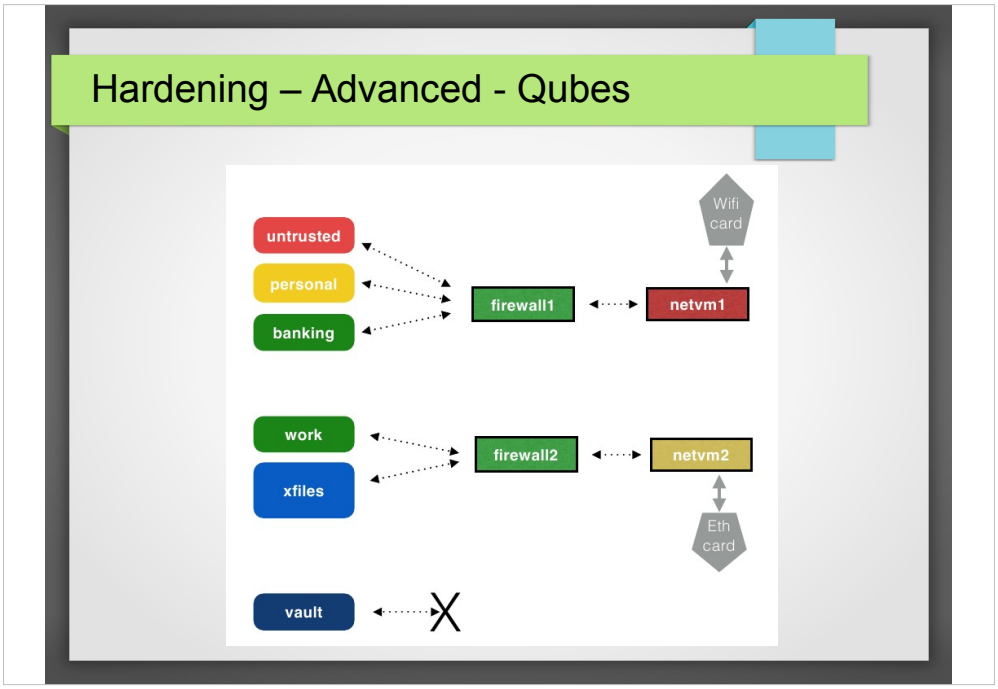


Leverage AppArmor/SE Linux/GRSecurity, encrypted containers(tomb) for compartmented storage, remove unused services, use tools like chkrootkit, Sandfox (sandboxed firefox)
* Protects: may protect from some 0-day attacks and misconfigured or vulnerable software, will likely minimize the impact of a targeted attack
* Vulnerable: 0-day (OS and Browser), not all apps are protected by AppArmor/SE Linux, poor OPSEC, stupid user (weak password gives root)



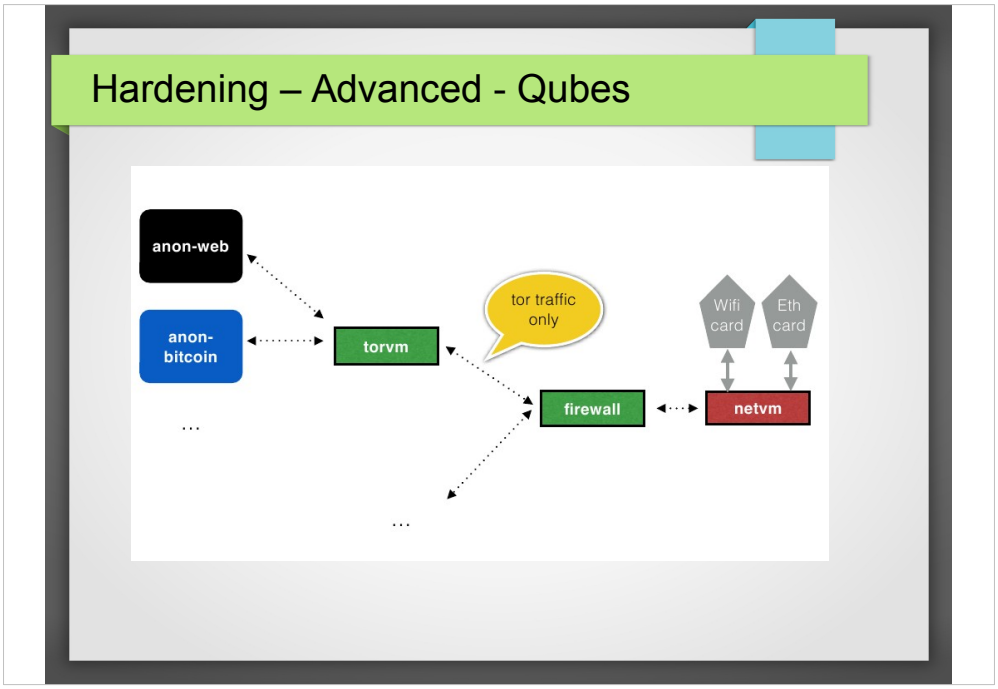
major compartmentalization, disposable VMs for different profiles, Sandbox applications

* Firewall to only allow certain apps outbound network connections, no inbound traffic if you can help it.
* SSH hardening.
* Thunderbolt, Firewire disabled (allows direct access to memory registers).
* HIDS such as TIGER, logwatch



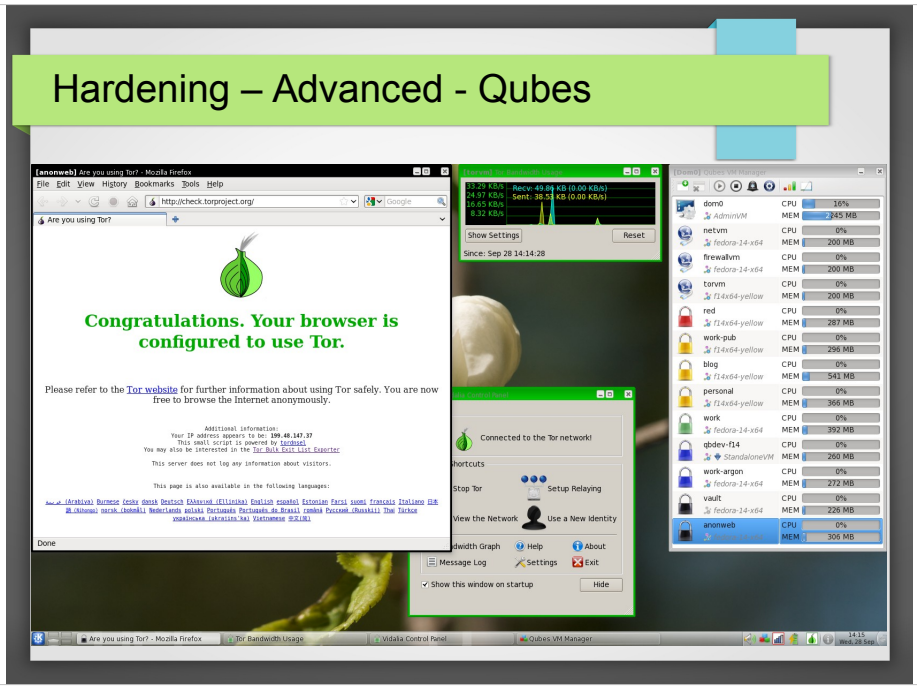
Special Mention: Qubes OS

Compartmentalization built-in using Xen and virtualization to separate contexts for information and activity classification levels.
* Network contexts, firewall, tor
* AppVM's: Disposable, Untrusted, Marginal Trust, Trusted, Vault (no network)

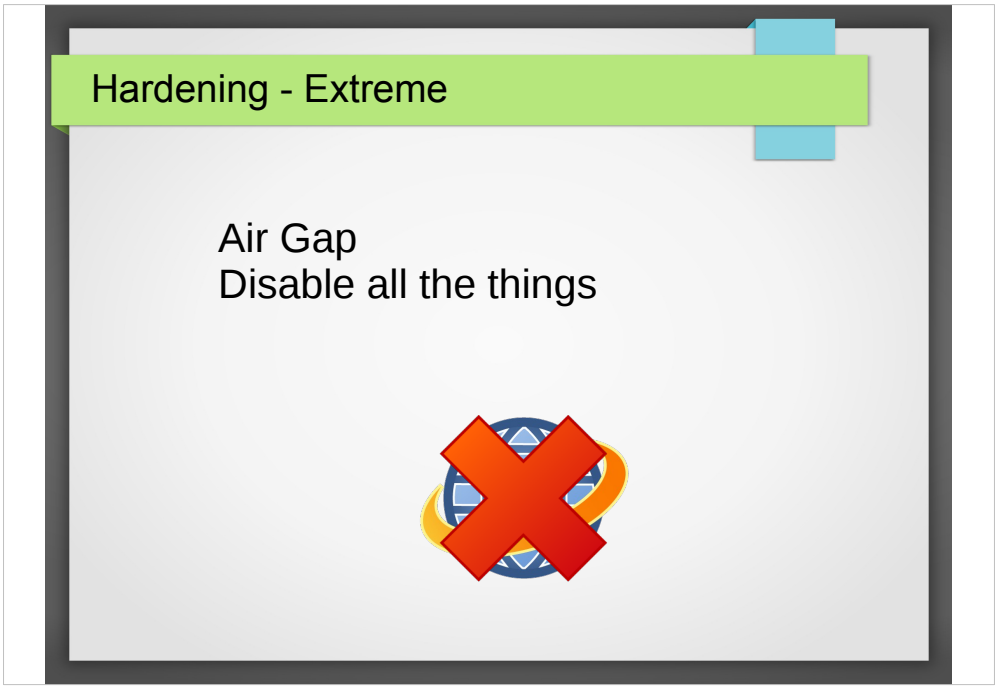


The anon-web AppVM is traversing through torproxy. All applications, tor-ified or not will ALWAYS go through tor proxy, similar to Whonix, or PORTAL but built-in

* Awesome: Built from ground-up w/ security in mind, Secure compartments to the extreme, read-only dom0, encrypted containers for each context
* Not Awesome: Xen 0-day, User error, Still in-progress, NOT easy-mode

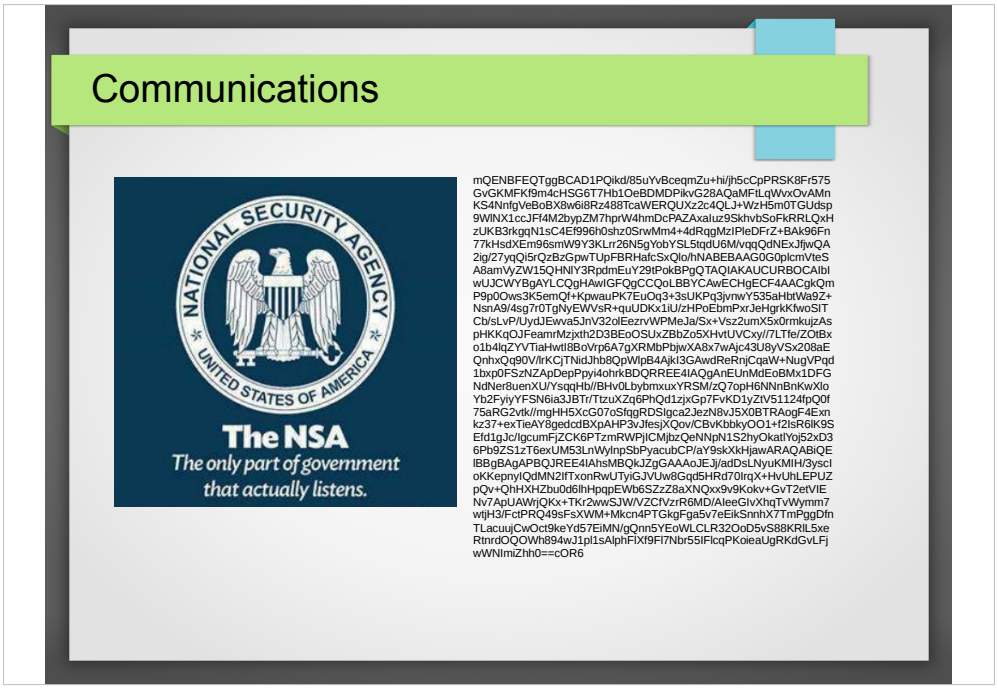


The window decorations are used to display the AppVM context (ie. “red” for untrusted, “yellow” for personal, and “green” for trusted, “black” for no network access ie. Vault AppVM)



Air gapped, Wireless card removed, Network card disabled in BIOS/Modprobe, Thunderbolt, Firewire disabled in BIOS/modprobe (linux ignores BIOS and probes for devices anyway) if possible.

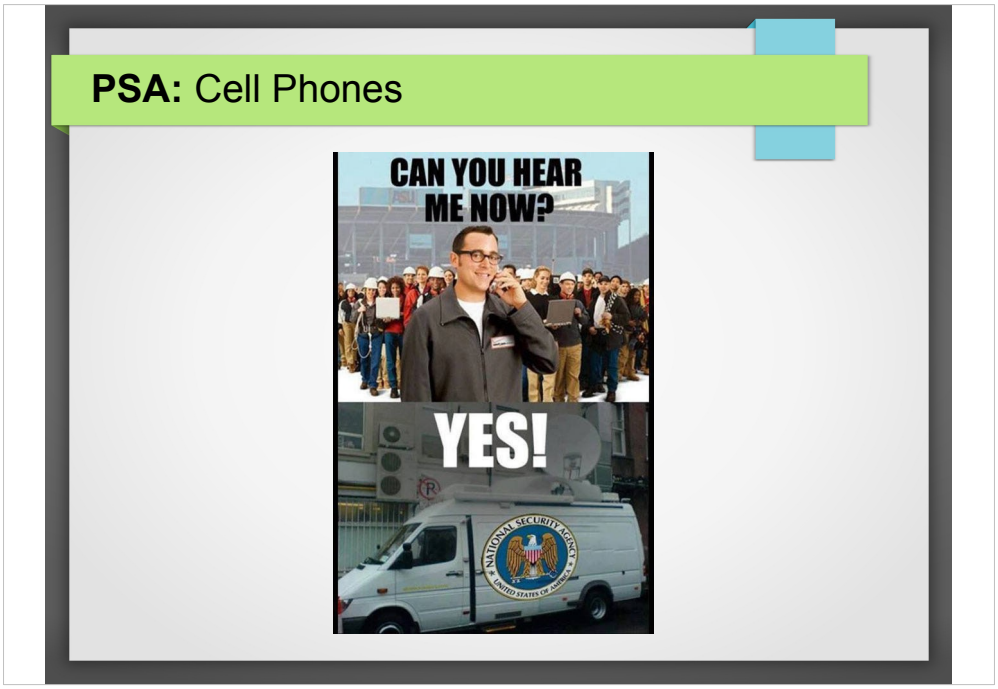
* Protects: 0-day (no way to load files on/off)
* Vulnerable: Evil Agency installs HW keylogger, Rubber hose, sneaker-net (see stuxnet)


Communications
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
The NSA
The only part of government
that actually listens.
mQENBFEQTggBCAD1PQikd/85uYvBceqmZu+hi/jh5cCpPRSK8Fr575
GvGKMFKf9m4cHSG6T7Hb1OeBDMDPikvG28AQaMFtLqWvxOvAMn
KS4NnfgVeBoBX8w6i8Rz488TcaWERQUXz2c4QLJ+WzH5m0TGUdsp
9WlNX1ccJFf4M2bypZM7hprW4hmDcPAZAxaIuz9SkhvbSoFkRRLQxH
zUKB3rkgqN1sC4Ef996h0shz0SrwMm4+4dRqgMzIPleDFrZ+BAk96Fn
77kHsdXEm96smW9Y3KLrr26N5gYobYSL5tqdU6M/vqqQdNExJfjwQA
2ig/27yqQi5rQzBzGpwTUpFBRHafcSxQlo/hNABEBAAG0G0plcmVteS
A8amVyZW15QHNlY3RpdmEuY29tPokBPgQTAQIAKAUCURBOCAIbI
wUJCWYBgAYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQm
P9p0Ows3K5emQf+KpwauPK7EuOq3+3sUKPq3jvnwY535aHbtWa9Z+
NsnA9/4sg7r0TgNyEWVsR+quUDKx1iU/zHPoEbmPxrJeHgrkKfwoSIT
Cb/sLvP/UydJEwva5JnV32olEezrvWPMeJa/Sx+Vsz2umX5x0rmkujzAs
pHKKqOJFeamrMzjxth2D3BEoOSUxZBbZo5XHvtUVCxy//7LTfe/ZOtBx
o1b4lqZYVTiaHwtI8BoVrp6A7gXRMbPbjwXA8x7wAjc43U8yVSx208aE
QnhxQq90V/lrKCjTNidJhb8QpWlpB4AjkI3GAwdReRnjCqaW+NugVPqd
1bxp0FSzNZApDepPpyi4ohrkBDQRREE4IAQgAnEUnMdEoBMx1DFG
NdNer8uenXUYsqqHb/BHv0LbybmxuxYRSM/zQ7opH6NNnBnKwXo
Yb2FyiyYFSN6ia3JBTr/TtzuXZq6PhQd1zjxGp7FvKD1yZtV51124fpQ0f
75aRG2vtk//mgHH5XcG07oSfqgRDSIgca2JezN8vJ5X0BTRAogF4Exn
kz37+exTieAY8gedcdBXpAHP3vJfesjXQov/CBvKbbkyOO1+f2lsR6lK9S
Efd1gJc/IgcumFjZCK6PTzmRWPjICMjbzQeNNpN1S2hyOkatlYoj52xD3
6Pb9ZS1zT6exUM53LnWylnpSbPyacubCP/aY9skXkHjawARAQABiQE
lBBgBAgAPBQJREE4IAhsMBQkJZgGAAAoJEJi/adDsLNyuKMIH/3yscl
oKKepnyIQdMN2IfTxonRwUTyiGJVUw8Gqd5HRd70IrqX+HvUhLEPUZ
pQv+QhHXHZbu0d6IhHpqpEWb6SZzZ8aXNQxx9v9Kokv+GvT2etVIE
Nv7ApUAWrjQKx+TKr2wwSJW/VZCfVzrR6MD/AIeeGlvXhqTvWymm7
wtjH3/FctPRQ49sFsXWM+Mkcn4PTGkgFga5v7eEikSnnhX7TmPggDfn
TLacuujCwOct9keYd57EiMN/gQnn5YEoWLCLR32OoD5vS88KRIL5xe
RtnrdOQOWh894wJ1pI1sAlphFlXf9FI7Nbr55IFlcqPKoieaUgRKdGvLFj
wWNlmiZhh0==cOR6

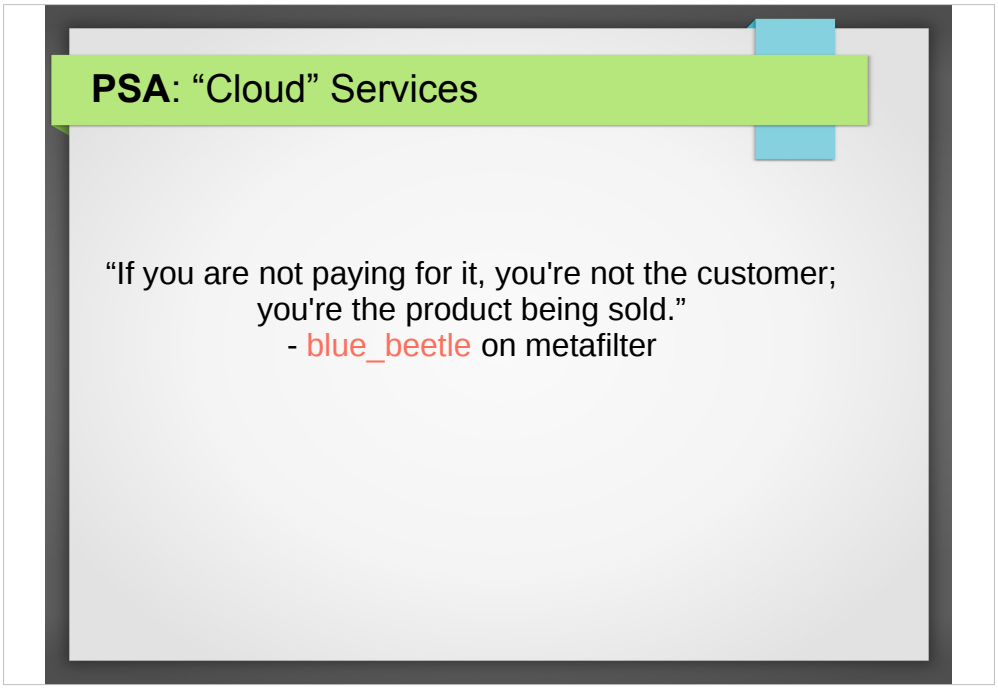
/* Next Slide */

Let's break down communications into three sections:

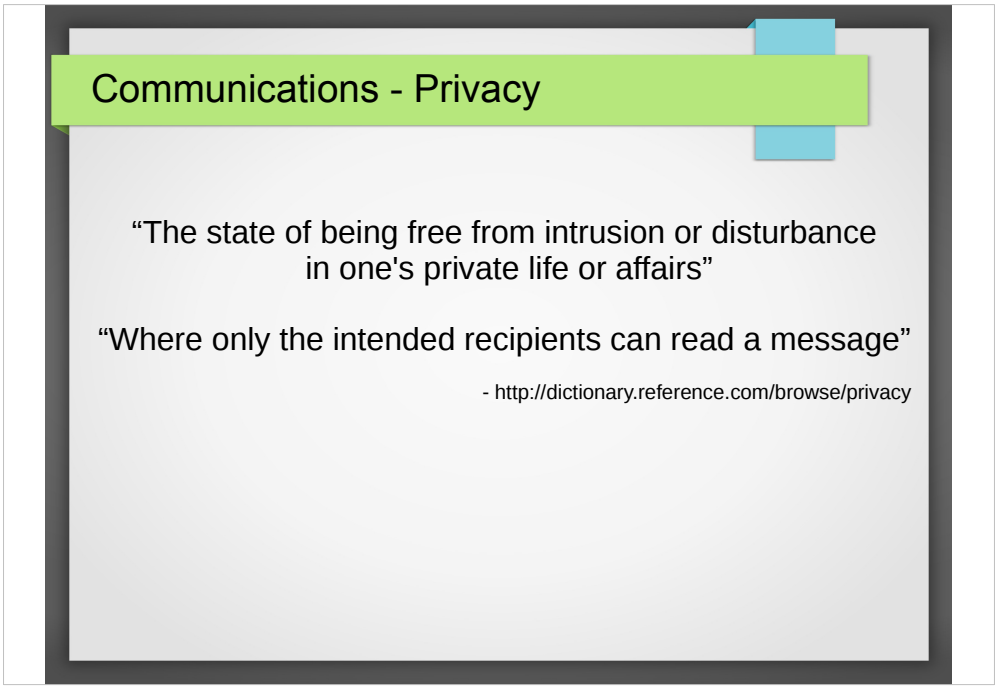
* Privacy
* Anonymity
* Security



*** Public Service Announcement
Cell phones are glorified tracking, bugging devices. Especially if you are a target, the phone should be considered untrustworthy and completely backdoored depending your your threat model or adversary
*** /Disclaimer

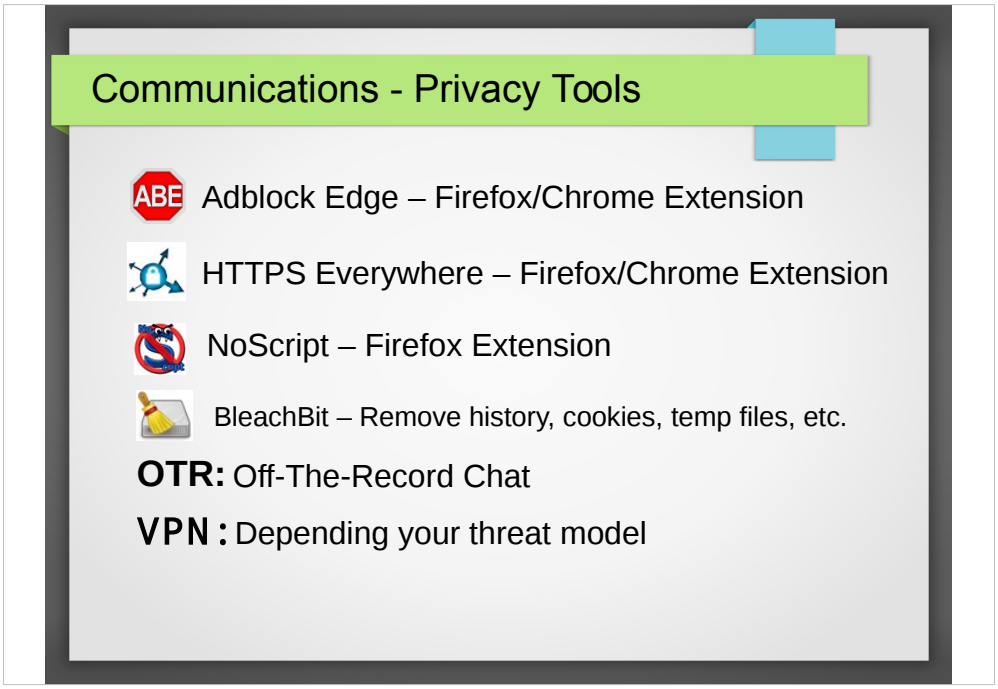


Cloud Services/Social Media: If you are not paying for the product, you are the product. The current state of private, secure, and anonymous communications kinda sucks. Yes, solutions exist. However, the process for setting up, and more importantly, using safely can be cumbersome and confusing.

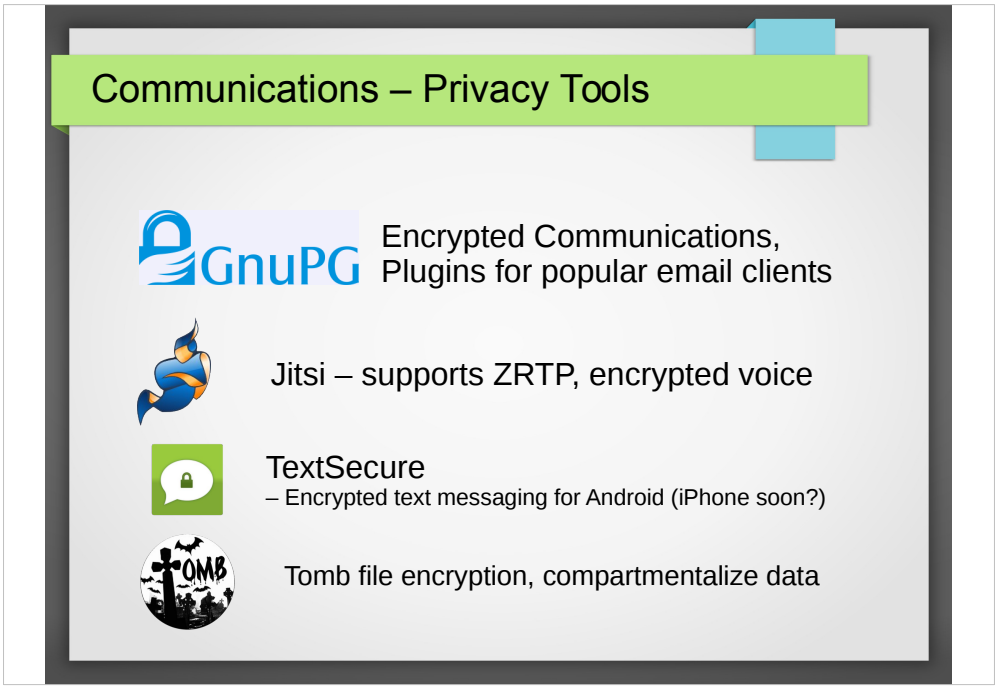


Lets start with Privacy:
Dictionary.com definition:
“the state of being free from intrusion or disturbance in one's private life or affairs”
“Where only the intended recipients can read a message”

Your browsing history, and the cookies sharing it can say ALOT about you. Who you are, where you are, what you like/dislike. Cookies have been one of the most relied upon methods for tracking browsing history, up to and including the NSA for targeting Tor users. We'll get into Tor in the anonymity section.



Popular privacy tools:
* Adblock Edge: Block advertisements and trackers across the web
* HTTPS Everywhere: Force SSL when the web server is capable (encrypted traffic from browser to server, no MiTM listening)
* NoScript – Block javascript/flash from all but approved sources
* BleachBit – delete cache, cookies, history, temp files
* OTR: Added layer of encryption, can be used with Google chat, Yahoo!, etc. to provide an extra layer of encryption – Plugins provided for popular chat clients like Pidgin
* VPN Protects from immediate vicinity on the wire, ISP, Coffee Shop, Shared WiFi. NOT an anonymity tool – Requires trust of provider



* GnuPG, implements PGP (pretty good privacy) encryption on most platforms. Encrypts file and messages using public/private key encryption. VERY secure, cumbersome to use
* Jitsi – Supports encrypted voice calls
* textsecure, encrypted txt
* Tomb – File encryption, uses keyfiles protected by passwords. IOW, separates the encrypted content from the key

Communications - Anonymity

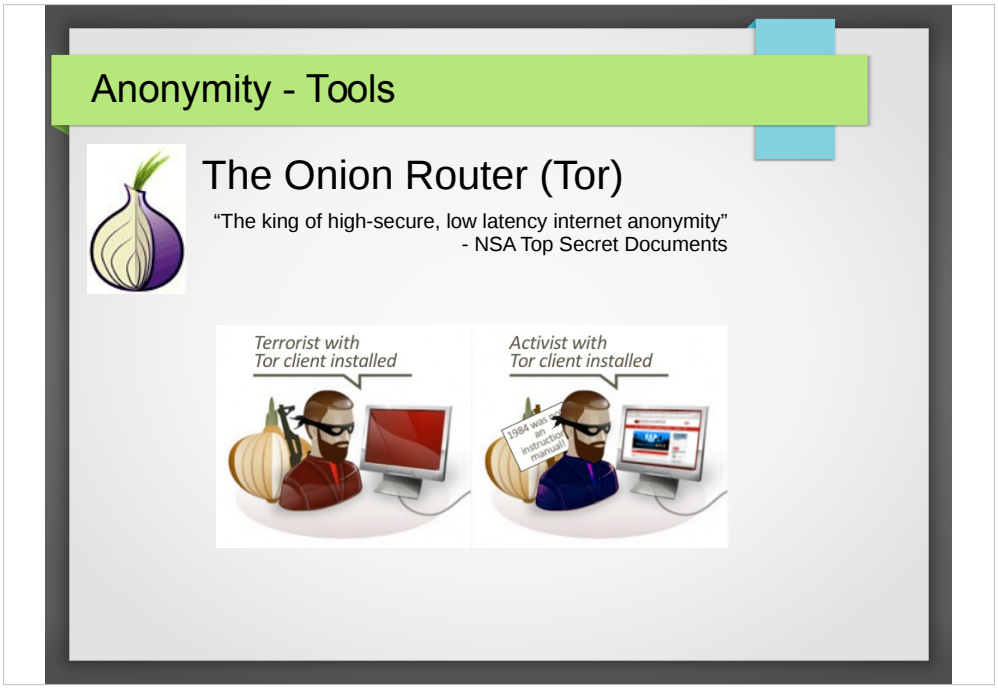
“without any name acknowledged, as that of author, contributor, or the like”

- http://dictionary.reference.com/browse/anonymous

http://www.flickr.com/photos/dfectuoso17/

Anonymity is the inability to provide attribution.

Remove the “who” from communications



NSA gave it a great endorsement

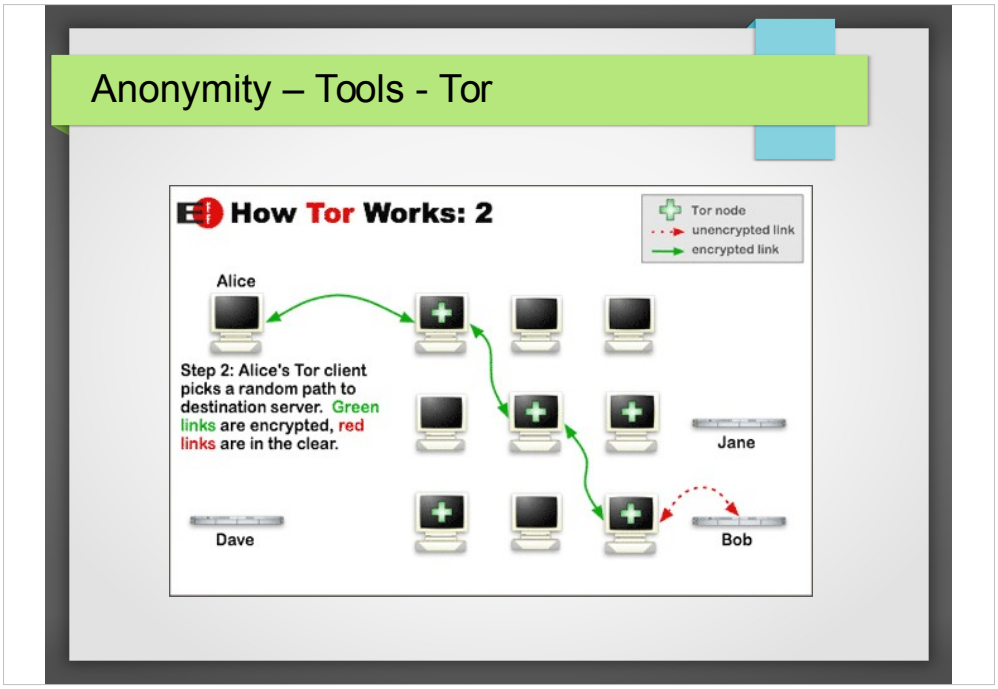
Advantages: Strong anonymity, very difficult to identify who the initiator of the traffic is

Disadvantages: Exit node can monitor (read: keep it all) and inject traffic into unencrypted streams. Possible attempts to MiTM encrypted streams (successful for users not paying attention)

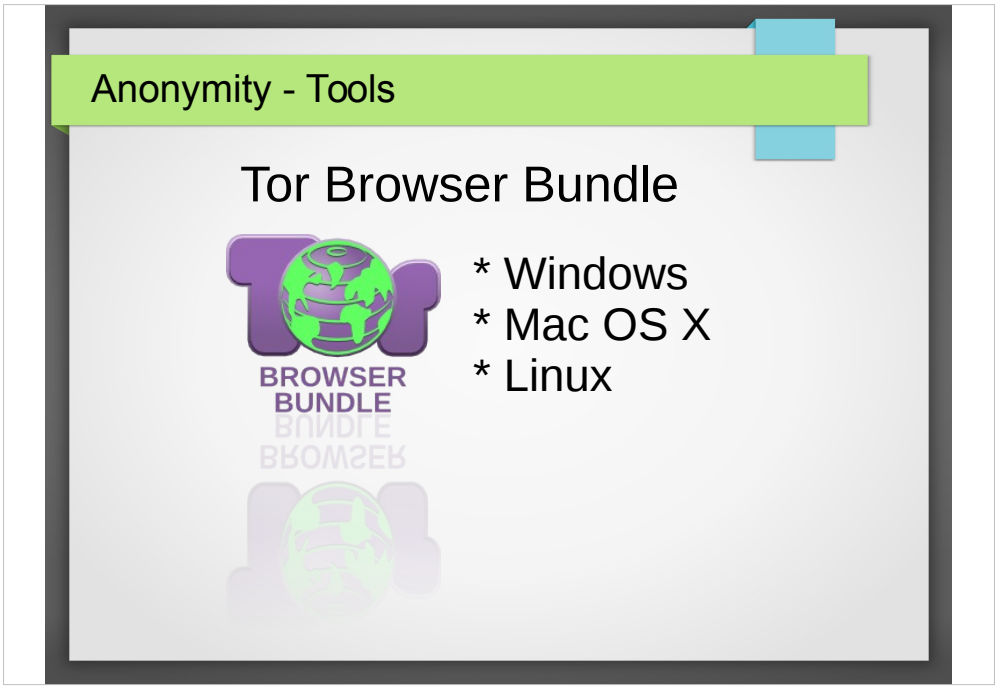
IOW, The exit node should be considered hostile. Use encrypted protocols like TLS/SSL to safeguard your communications from exit nodes

Very expensive, risky for nation-states to identify users.

OPSEC Tip: Don't login to your non-anon stuff while using TOR (at least, not in the same session).



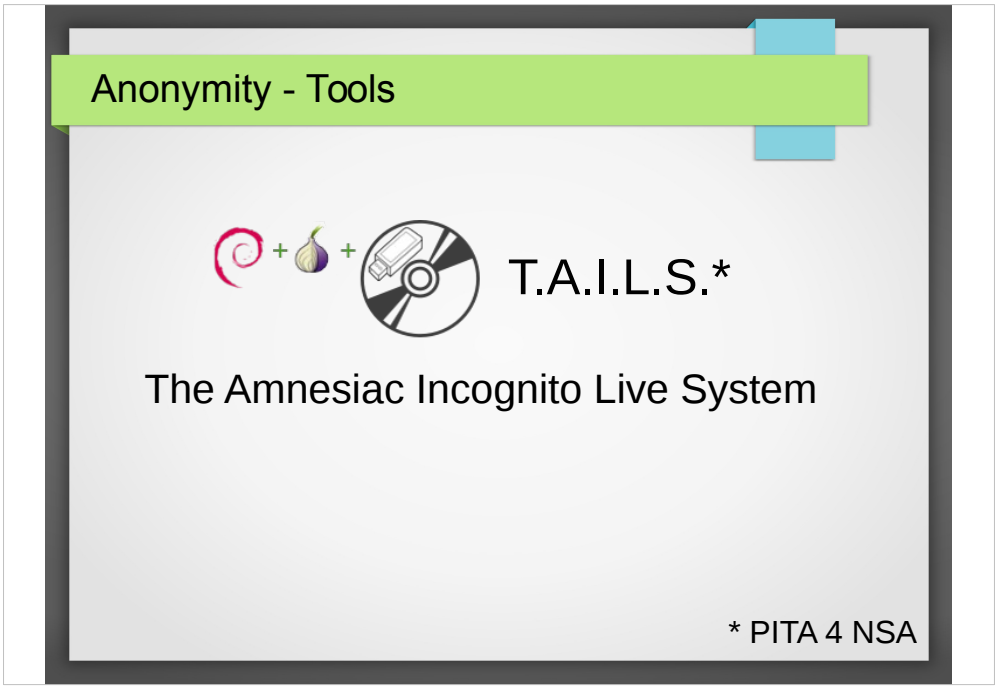
How it works: Tor routes your traffic through several hosts, each connection wrapped in a new layer of encryption until it gets to the exit node where the request is sent to the destination. Tor Gateway sends the response back through the relay and eventually reaches the Tor client.



Easy to use and install, great for casual use

Doesn't fail closed, if an attacker compromises Firefox. Default allows javascript for usability

Specifically targeted by NSA for browser exploits (javascript, flash, other)

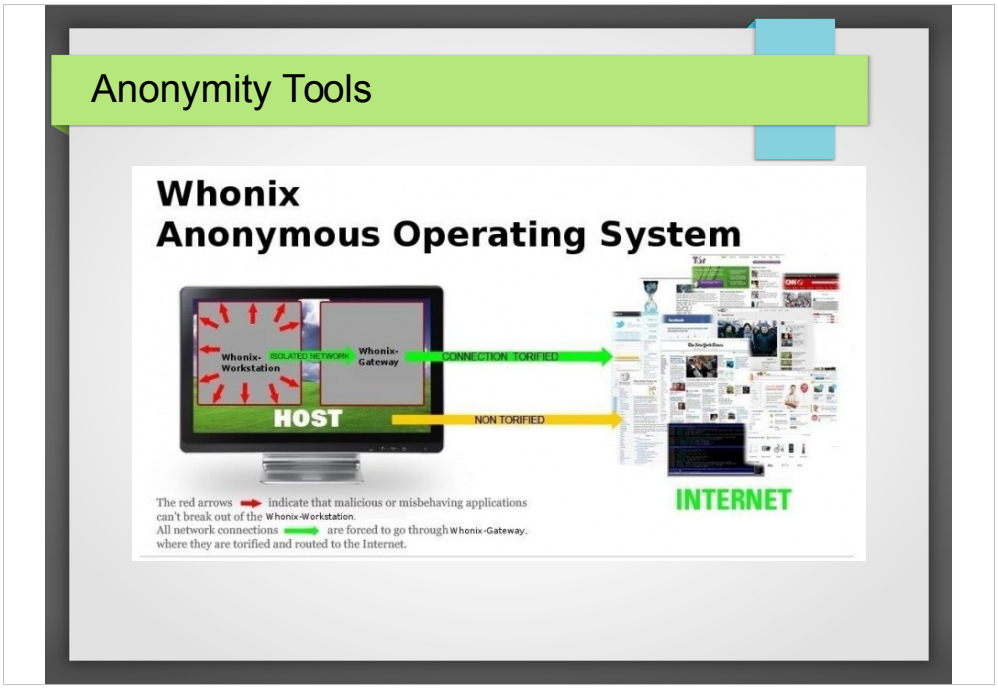


LiveCD Desktop environment routes all traffic through Tor

Bundled with several Tor aware applications and tools. LiveCD can be run in eCafe, School, Laptop, etc.

As a LiveCD, it does not leave traces on a computer of previous activity

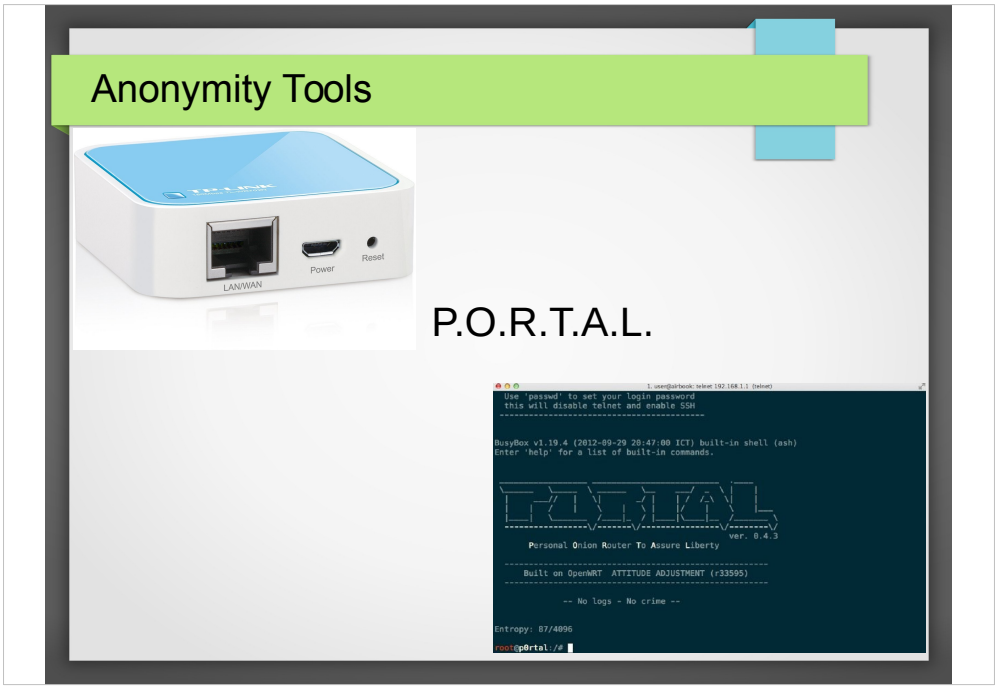
Mentioned in NSA ppt that it provides problems for them, esp. their persistent attacks – PITA for NSA



Fails closed, mostly

Host virtual machine routes ALL traffic through Tor. Runs on VirtualBox, VM Ware, probably Xen. Easy(er) to deploy and use, more EPICFAIL proof as long as good OPSEC is followed

Host is vulnerable to attack, and VM /may/ be vulnerable



Personal Onion Router To Assure Liberty by The Grugq
Hardware Tor router/gateway

Fails closed. Closed even in event of complete OS/VM compromise

Once its setup, pretty easy to use and mostly technical fail proof. Not safe against stupidity

Compartmentalization (I keep saying this...)
  Encrypted Containers – This alone can mitigate a number of attacks

“Boring” Long Term Support, look for reliability, reputation, and community tested

Test the SHA-1/MD5 Sums
Don't include (untrusted) ubuntu ppa's or other pre-compiled binaries from unknown and untrusted sources – You are granting an unknown, unverified author to run code on your system

Air-Gap if you need extreme information security

Should be 'nuff said

The math is good. Utilize encryption where-ever it makes sense, and compartmentalize your information. A Qubes model (disposable, untrusted, trusted, vault) of compartmentalization using encrypted containers may make sense. Containers should use different key files or password. Encrypt communications. The more often you use encryption, the less “outlier” it will look. If only using it to talk to confidential sources, it will be easier to profile your activity and information

If your threat model indicates the need to use an air gap. Don't EVER connect it to a network. In extreme cases, use write only media to transfer files to the air-gapped machine. Malware may transfer over, but it won't be able to escape. **Note, Iran nuke plant was air-gapped, stuxnet was still successful

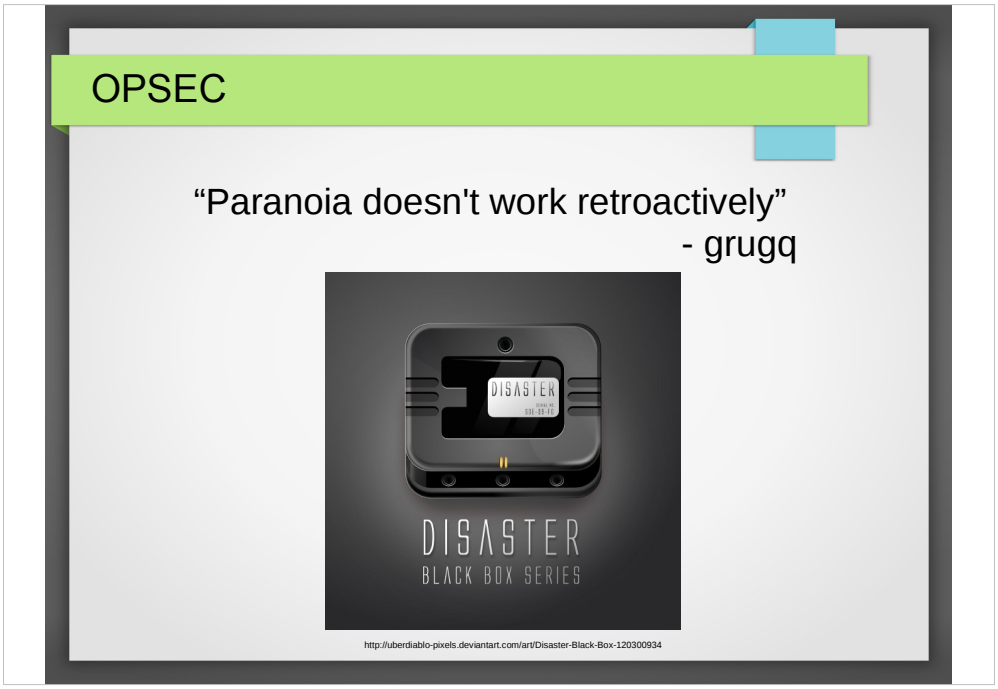
#1 Rule of OPSEC
“@thegrugq: dont reveal information that'll help the adversary. STFU”

Don't mix family and business. One WILL infect the other

Keep your mouth shut. Seriously, stop talking about your story/research/political affiliations, etc with untrusted parties – And really, keep the trusted parties down to an absolute minimum.

Buy burner phones, burner laptops. Be prepared and ready to dump them. Don't use burner phones in places where your primary identity would be.

TNO: Trust No One, they are not your friends, they are your co-defendants

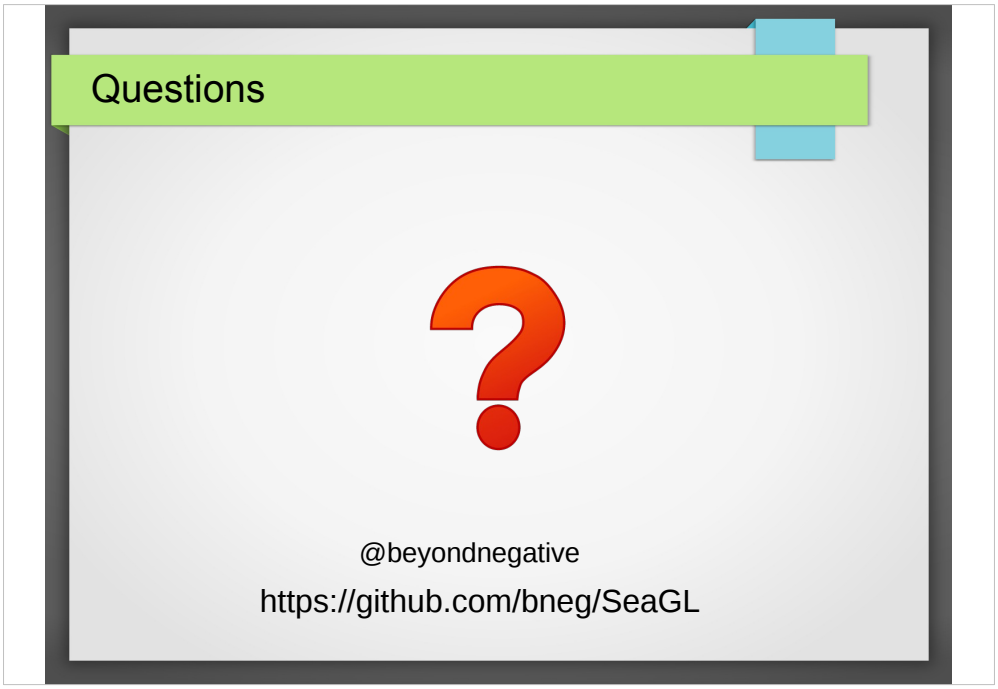


If you have to work securely in a public space, keep your back to the wall with an eye on the door. Take mental note of your surroundings.

Better yet, don't be predictable. Going to the same place, every day, at the same time is bad

Your mindset should be that “they” are in fact after you. The black helicopters exist, and that suspicious van across the street broadcasting “FBI Surveillance Van 42” is a sting op ready to bust down the door the moment you fuck it up

OPSEC is hard, really hard, but if you think that your activities might make you a target or a huge target in the future, remember: paranoia doesn't work retroactively



Depressing final note – None of this matters if your hardware can't be trusted. Upside, extremely risky to implement H/W backdoors. Company stock would get eviscerated if ever found out – Also, H/W backdoors would only work with physical access on air-gapped machines