"[Successfully] Operating In Denied Areas Online"

Cybersecurity Symposium
Ballroom A&B, SMC Building, UMD Baltimore
10-11:15 AM, Friday April 8, 2016

Joe St Sauver, Ph.D. (stsauver@fsi.io or joe@stsauver.com)
Scientist, Farsight Security, Inc.

https://www.stsauver.com/joe/umb-cybersec/

Disclaimer: All opinions expressed are strictly my own

Thanks For The Invitation To Talk Today!

- I've known Peter Murray, University of Maryland Baltimore's CIO, for many years, back to when we both served on the Educause Higher Education Information Security Council (HEISC) together.

- I'd like to thank Peter for the invitation to talk with you today, and Ashley Cuffia for help with the logistics of my visit.

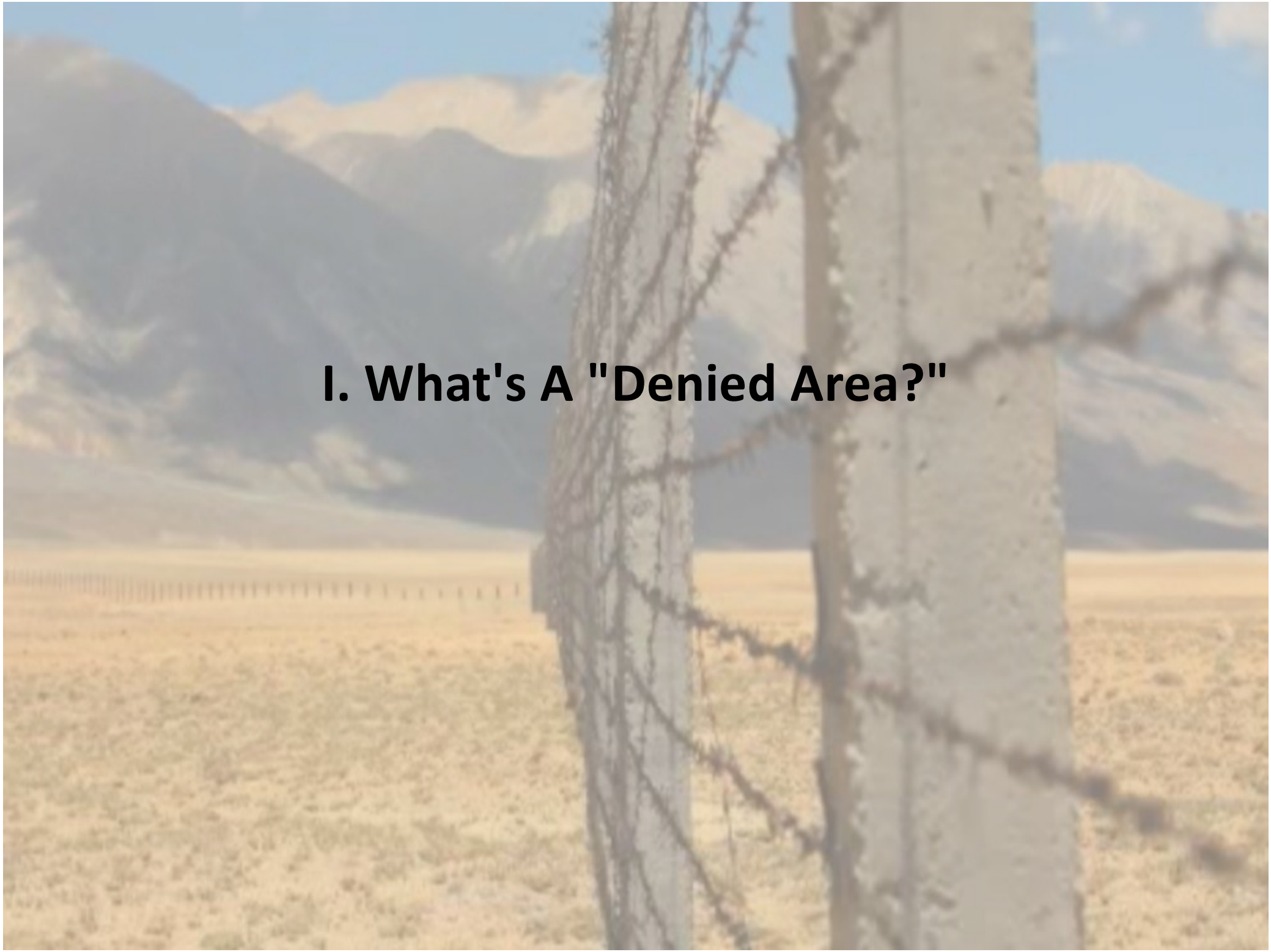
- And let me also say thank you to all of you who made time to attend today.

A Little About Me

- I worked at the University of Oregon for about 28 years, the last half a dozen or so years under contract with Internet2 and InCommon as Internet2's Nationwide Security Programs Manager, with responsibility for InCommon's SSL/TLS Certificate Program and Multifactor Program, too.
- I also advised, and continue to advise, a number of organizations including M3AAWG (the Messaging, Malware and Mobile Anti-Abuse Working Group), the REN-ISAC (the Research and Education Network Information Sharing and Analysis Center), the Online Trust Alliance, and others.
- My Ph.D. is in Production and Operations Management from the Decision Sciences Department at the University of Oregon School of Business.
- I now work as a Scientist for Paul Vixie's company Farsight Security, Inc. (https://www.farsightsecurity.com/)

The Somewhat Odd Format Of My Talks

- I'm experimenting with a new format for my slides today, striving for more graphic content. We'll see how it goes. :-) Generally, I write detailed slides to help me stay on track, and to allow me to cover more material than I otherwise could. That format also avoids the need for you to take notes, and reduces misquoting.
- It also makes my talks more accessible for the deaf or hard of hearing, and those for whom English is not their first language – my slides are like "closed captioning" for those audiences.
- Missed the actual talk? No problem, check the slides. They should make sense even if you weren't here for my remarks. Google does a great job of indexing my slides, too.
- I promise I won't read my slides to you, nor do you need to try to read them as we go through them. I make them available for you to look at afterwards, should you desire to do so.



I. What's A "Denied Area?"

"Denied Area" Defined

A denied area is an intelligence term of art describing an extremely hostile operational environment with heavy surveillance.

The United States Department of Defense defines a denied area as "an area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities."

Source: https://en.wikipedia.org/wiki/Denied_area

Real World Example: North Korea

The black hole of North Korea intelligence gathering is getting blacker. [...]

North Korea has always been the hardest target [...] The North has long been among the most brutal police states in the world, "very good at scouting human spies," says one American intelligence official, "and finishing them off fast." Thus, South Korean intelligence services have a hard time inserting agents. It is all but impossible for an outsider to travel unnoticed to the North, a land of many checkpoints, few cars and a lot of neighborhood informers.

"Intelligence on North Korea, and Its New Leader, Remains Elusive"

http://www.nytimes.com/2013/05/07/world/asia/intelligence-on-north-korea-still-out-of-reach.html

Manned Overflights of the USSR

Reconnaissance flights began in 1946 along the borders of the Soviet Union and other Socialist Bloc states. [...]

On 4 July 1956, the first U-2 flight over the Soviet Union took place. [...]

Following the [1 May] 1960 U-2 incident, Eisenhower ordered an end to American reconnaissance flights into the USSR. [...]

Source:
https://en.wikipedia.org/wiki/United_States_aerial_reconnaissance_of_the_Soviet_Union

Mogadishu Somalia ("Blackhawk Down"), 1993

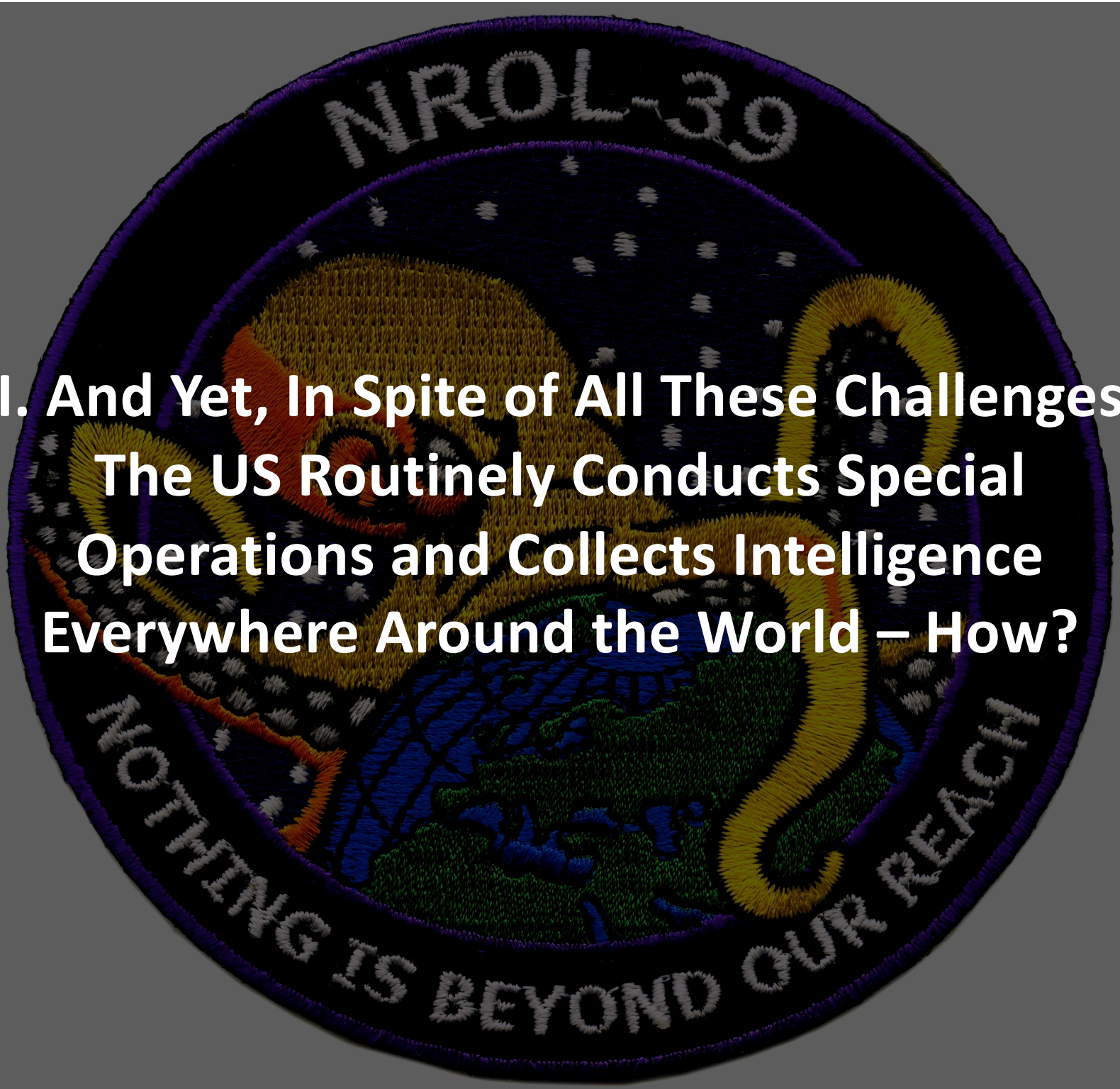
- Clan warfare lead to famine and civil war; the UN called for food relief and peacekeeping efforts (largely led by the US)
- 3 October 1993, a US operation to capture the leaders of the Habr Gidr clan, led by Mohamed Farrah Aidid, was meant to last <1 hour, including 19 aircraft, 12 vehicles, and 160 men.
- Somali militia and armed civilian fighters successfully shot down two UH-60 Black Hawk helicopters with small arms and RPGs.
- Coalition forces struggled to rescue the trapped Americans, with 18 rescuers dead, 73 wounded, and one pilot taken prisoner.
- On 6 October 1993 Bill Clinton directed a stop to all actions by U.S. forces against Aidid except those required in self-defense.

Source: https://en.wikipedia.org/wiki/Battle_of_Mogadishu_%281993%29

WMD in Saddam's Iraq

[...] the United States government asserted that Saddam Hussein had reconstituted his nuclear weapons program, had biological weapons and mobile biological weapon production facilities, and had stockpiled and was producing chemical weapons. [...] When the October 2002 [National Intelligence Estimate] was written the United States had ***little human intelligence on Iraq's nuclear, biological, and chemical weapons programs and virtually no human intelligence on leadership intentions****. [...]*

Source: Report to the President, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, March 31, 2005, http://govinfo.library.unt.edu/wmd/report/report.html [emphasis added] (but see also http://www.nytimes.com/2014/11/23/world/middleeast/thousands-of-iraq-chemical-weapons-destroyed-in-open-air-watchdog-says-.html and http://mobile.nytimes.com/2015/02/16/world/cia-is-said-to-have-bought-and-destroyed-iraqi-chemical-weapons.html)



II. And Yet, In Spite of All These Challenges, The US Routinely Conducts Special Operations and Collects Intelligence Everywhere Around the World – How?

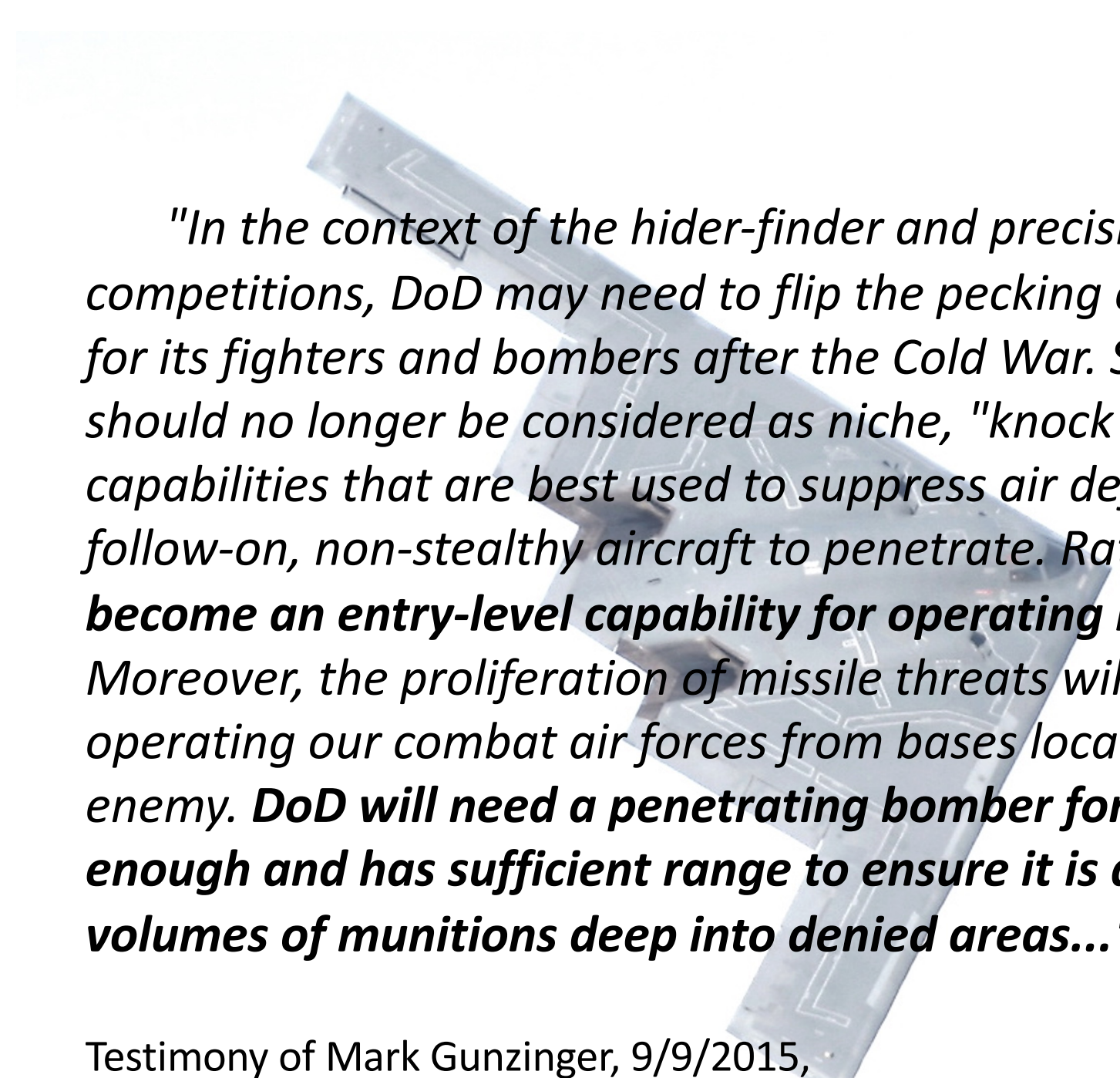
Training

- Operating undetected in hostile territories is a skill that can be taught and learned. For example, the Army offers a month-long "Reconnaissance and Surveillance Leaders" course, see http://www.benning.army.mil/armor/316thCav/content/rslc/
- More extensive training programs are offered by other government agencies. One depiction of such training (from a former CIA ops officer) can be seen in the bestselling memoir, "Blowing My Cover: My Life As a CIA Spy" by Lindsay Moran.
- Or: "[Jason Matthews] spent two years in D.C. undergoing education in so-called denied-area tradecraft, where surveillance was assumed at all times. He learned tricks like dead drops (delivering packages to agents without arousing suspicion) and the MCD, or moving-car delivery (hand brakes, no brake lights)." http://www.mensjournal.com/magazine/secrets-of-a-secret-agent-20150731

Satellite Technology

When manned surveillance overflights of denied areas became problematic, satellite imagery served as a replacement. These days, we all take access to high-res satellite imagery for granted...

Stealth



"In the context of the hider-finder and precision strike salvo competitions, DoD may need to flip the pecking order it established for its fighters and bombers after the Cold War. Stealth aircraft should no longer be considered as niche, "knock down the door" capabilities that are best used to suppress air defenses and enable follow-on, non-stealthy aircraft to penetrate. Rather, ***stealth has become an entry-level capability for operating in contested areas.*** *Moreover, the proliferation of missile threats will necessitate operating our combat air forces from bases located further from the enemy.* ***DoD will need a penetrating bomber force that is large enough and has sufficient range to ensure it is able to deliver high volumes of munitions deep into denied areas..."***

Testimony of Mark Gunzinger, 9/9/2015,
http://docs.house.gov/meetings/AS/AS28/20150909/103876/HMTG-114-AS28-Wstate-GunzingerM-20150909.pdf
[emphasis added]

Tradecraft

SPYCRAFT

During more than five years, case officers and Tolkachev met clandestinely more than twenty times. Never before had this number of personal meetings with an agent inside the Soviet Union been contemplated or securely executed. During the five years of Tolkachev's active service, the fusion of tradecraft and technology demonstrated that there were no longer permanently "denied areas" for agent operations.

Robert Wallace and H. Keith Melton

Firepower


Sometimes you may not be able to get in and get out undetected. Sometimes the only option is superior firepower, as exemplified by this Special Warfare Combatant Craft's minigun, a modern motorized "Gatling Gun" firing 2,000-6,000 rounds/minute. Video at https://www.youtube.com/watch?v=Bqoja3iWWaE
4:03 / 7:43
CC
HD

So: Successful Operations in Real World "Denied" Areas Obviously ARE Possible

Operations may require special training or technical solutions to be accomplished, but they have empirically been proven to be possible.

This is true for the intelligence community, for the military, and it can be true for you online, too.

But I know that there are at least some of you who may wonder if the Internet's really a "denied area at all?"

III. The Internet: "A Denied Area?" Really?

"You're Kidding! The Internet's Not a Denied Area!"

- Actually, I'm quite serious.

  Today's Internet may be a "denied area" just like some physical regions of the world...

  Let's check to see it really satisfies the definitions from Wikipedia, shall we?

Extremely Hostile Operational Environment?

- **Malware:** **"Nearly 1 million new malware threats released every day"** http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

- **DDoS Attacks:** **"DDoS attack on BBC may have been biggest in history,"** http://www.csoonline.com/article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-been-biggest-in-history.html [attack was estimated @**602 Gbps** (Jan. 2016)]

- **Carding:** "Over the course of eight years, a hacking group from Russia and Ukraine targeted banks and companies, including Nasdaq, 7-11, JetBlue and JC Penney. **The hackers stole 160 million credit and debit card numbers** and **breached 800,000 bank accounts**." "**The 9 Biggest Data Breaches Of All Time**," Huffington Post, August 21st, 2015

Extremely Hostile Operational Environment? (cont)

- **Phishing:** "**Phishing Attacks Grow in Volume, Complexity**: The report found **the most popular phishing attack templates with the highest click rates are items employees expected to see in their work email**," http://www.eweek.com/small-business/phishing-attacks-grow-in-volume-complexity.html (2016-02-01)

- **Ransomware:** "We are currently seeing extraordinarily huge volumes of JavaScript attachments being spammed out, which, if clicked on by users, lead to the download of a ransomware. Ransomware encrypts data on a hard drive, and then demands payment from the victim for the key to decrypt the data," **Massive Volume of Ransomware Downloaders being Spammed,** March 9, 2016, https://www.trustwave.com/Resources/SpiderLabs-Blog/Massive-Volume-of-Ransomware-Downloaders-being-

Extremely Hostile Operational Environment? (cont 2)

- **Government Censorship/Attacks on Privacy Tools:** "Freedom on the Net 2015 finds **internet freedom around the world in decline for a fifth consecutive year** as more governments censored information of public interest while also expanding surveillance and cracking down on privacy tools." https://freedomhouse.org/report/freedom-net/freedom-net-2015 [Wikipedia describes Freedom House as "a U.S.-based nonpartisan 501(c)(3) U.S. Government funded [...] (NGO)"]

- **Government Penalties:** "Two health care organizations have agreed to settle charges that they potentially violated [...] (HIPAA) [...] by failing to secure thousands of patients' electronic protected health information (ePHI) [...] The **monetary payments of $4,800,000 include the largest HIPAA settlement to date.**" http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html

[And It's Not Just "Traditional Computers," Either]

- **Mobile:** "**Kaspersky Lab Reporting: Mobile malware has grown almost 3-fold in Q2, and cyberespionage attacks target SMB companies,"** http://www.kaspersky.com/about/news/virus/2015/Kaspersky-Lab-Reporting-Mobile-malware-has-grown-almost-3-fold-in-Q2-and-cyberespionage-attacks-target-SMB-companies
- **SCADA: "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,"** http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [230,000 residents left without power as a result of infrastructure hacking]
- **Internet of Things:** "[The Chief of the NSA's Tailored Access Operations] also said that the poor security of such devices is one of his primary concerns when it comes to the safety of U.S. networks." https://www.technologyreview.com/s/546251/nsa-hacking-chief-internet-of-things-security-keeps-me-up-at-night/

OK. So What About "Heavy Surveillance?"

One domestic example, ATT:

"The cooperation involved a variety of classified programs that span decades, in one case more than 15 years before the September 11 terrorist attacks. In addition to providing the NSA with access to billions of e-mails flowing across its domestic networks, AT&T helped wiretap all Internet communications at the United Nations headquarters [...]"

Source: AT&T's "Extreme Willingness to Help" is key to NSA Internet surveillance: published report said partnership dates back to 1985, http://arstechnica.com/tech-policy/2015/08/atts-extreme-willingness-to-help-is-key-to-nsa-internet-surveillance/ [remember that telecommunication carriers require a government license to operate transoceanic cable landing stations, cellular systems, etc.]

Is Heavy Surveillance Just A US Thing?

It's NOT just the US... consider the situation in Great Britain:

Communications firms - such as your broadband or mobile phone providers - will be compelled to hold a year's worth of your communications data. This new information will be details of services, websites and data sources you connect to when you go online and is called your "Internet Connection Record". For instance, it could be your visit to the BBC website from a mobile phone at breakfast and then how you used an online chat service at lunch. It does not include the detail of what you then did within each service. There is no comparable legal duty to retain these records in the rest of Europe, the USA, Canada or Australia - this appears to be a world first.

Source: "UK surveillance powers explained," November 5th, 2015, http://www.bbc.com/news/uk-34713435

"... Under Enemy Or Unfriendly Control"?

"Marrakech, Morocco… Internet Corporation for Assigned Names and Numbers (ICANN) Board Chair Dr. Stephen D. Crocker today submitted to the U.S. Government a plan developed by the international Internet community that, if approved, will lead to global stewardship of some key technical Internet functions. [...]

"The U.S. Government will now review the package to ensure that it meets NTIA's criteria. ***If approved, implementation of the plan is expected to be completed prior to the expiration of the contract between NTIA and ICANN in September 2016."***

Source: "Plan to Transition Stewardship of Key Internet Functions Sent to the U.S. Government: Culmination of a Two-Year Effort by the Global Internet Community," [emphasis added] https://www.icann.org/news/announcement-2016-03-10-en

The NTIA Says...

NTIA will now begin the process of reviewing the proposal, hopefully within 90 days, to determine whether it meets the criteria we outlined when we announced the transition:

First, the proposal must support and enhance the multistakeholder model of Internet governance [...] More specifically, we will not accept a transition proposal that replaces the NTIA role with a government-led or intergovernmental organization solution.

Second, the proposal must maintain the security, stability, and resiliency of the domain name system.

Third, it must meet the needs and expectations of the global customers and partners of the IANA services.

And finally, it must maintain the openness of the Internet.

Source: https://www.ntia.doc.gov/blog/2016/reviewing-iana-transition-proposal (March 11, 2016)

"Friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities [...]"

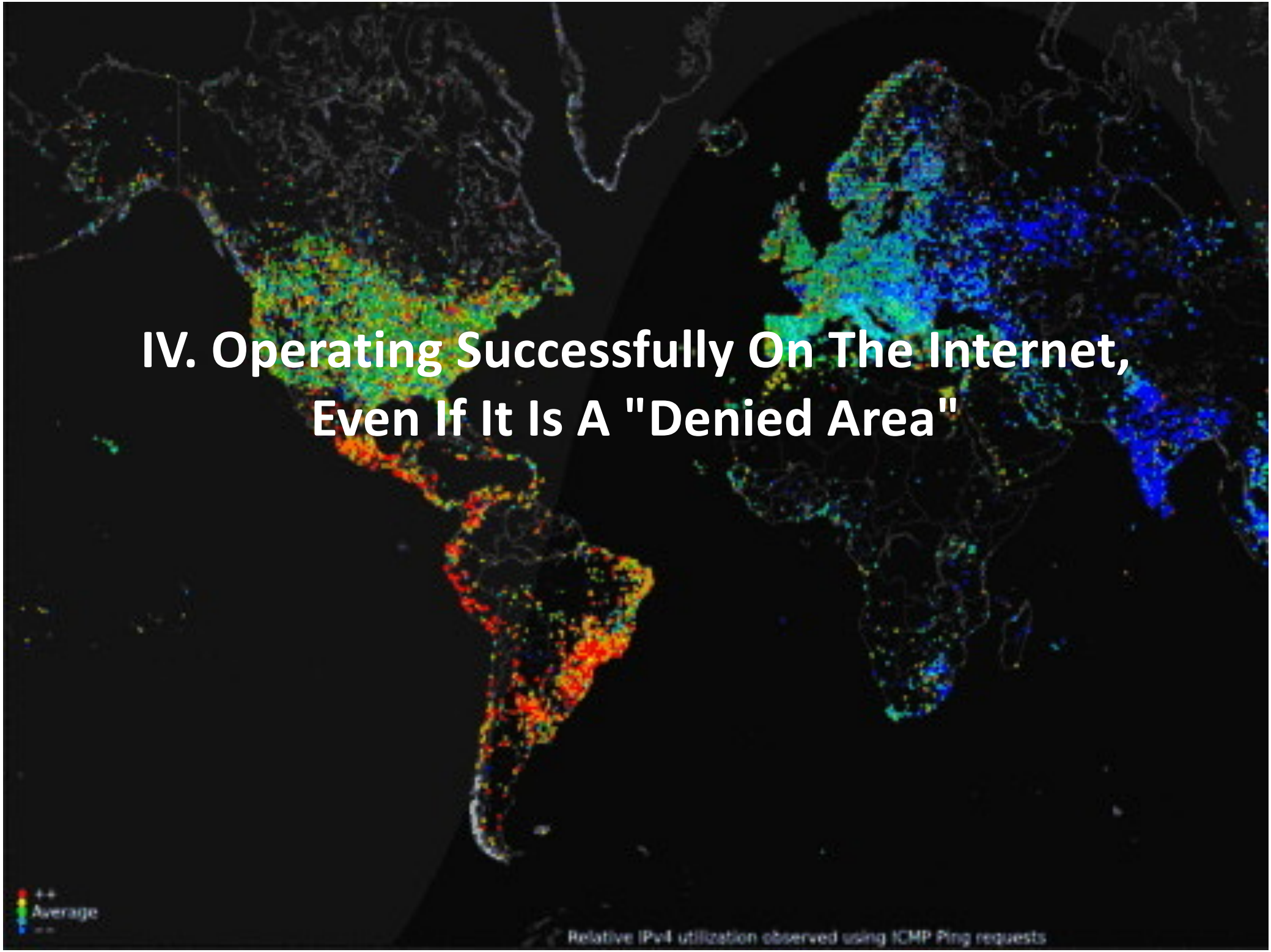
- It is very difficult to **successfully attribute** online attacks -- attacks may be indirect or conducted in intentionally misleading ways
- Even if you could identify the source of an attack, **"active response"/"counter hacking"** will almost always result in **unacceptable levels of collateral damage** to innocent 3rd parties
- Significant **asymmetries exist:** if North Korea attacked us via the Internet, they could potentially devastate the US, however, since North Korea hardly uses the Internet at all, what could we attack in kind? Would further attempts at economic isolation or a kinetic military response be America's only response options?
- Speaking of limited options, **treaties limit <u>our</u> options**, but appear to be disregarded by at least some of our foes (see www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html)

So... Today's Internet, Is It A Denied Area?

- ☑ Extremely hostile operational environment – YEP
- ☑ Heavy surveillance – YEP
- ☐ Under enemy or unfriendly control? TBD
- ☐ An environment in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities? TBD

And yet, we ALL still need to use the Internet.

So today, in just what's left of an hour, we're going to help you learn to operate (more) successfully in what's effectively a "denied online environment."

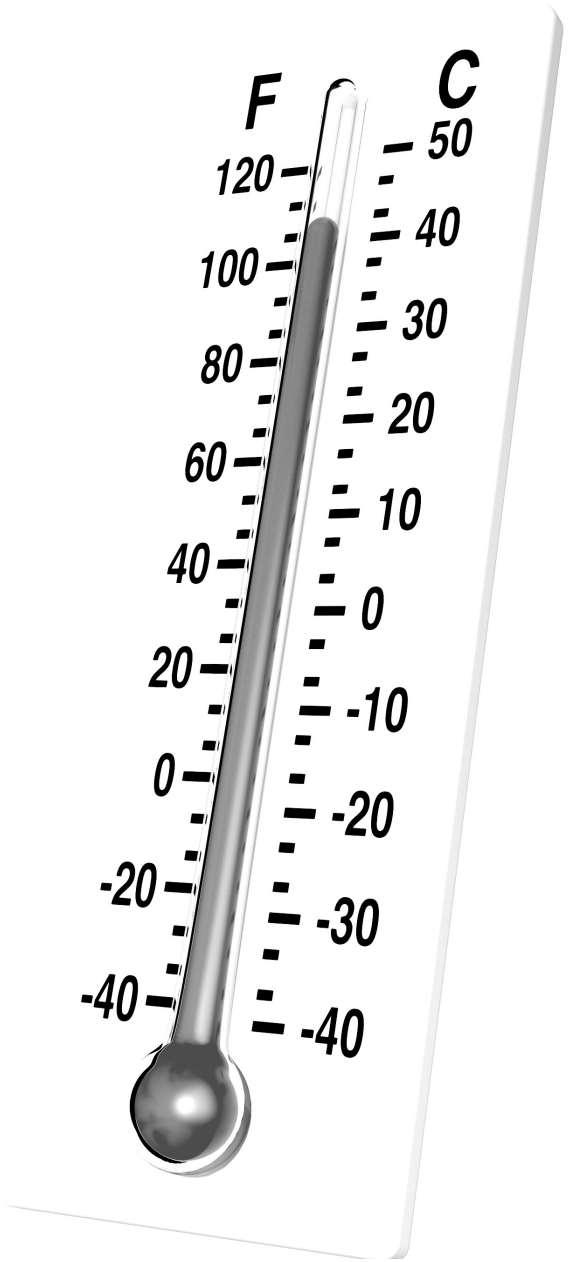

IV. Operating Successfully On The Internet,
Even If It Is A "Denied Area"
++
Average
Relative IPv4 utilization observed using ICMP Ping requests

"But Joe! I'm Not a Cyber Spy or Cyber Soldier!"

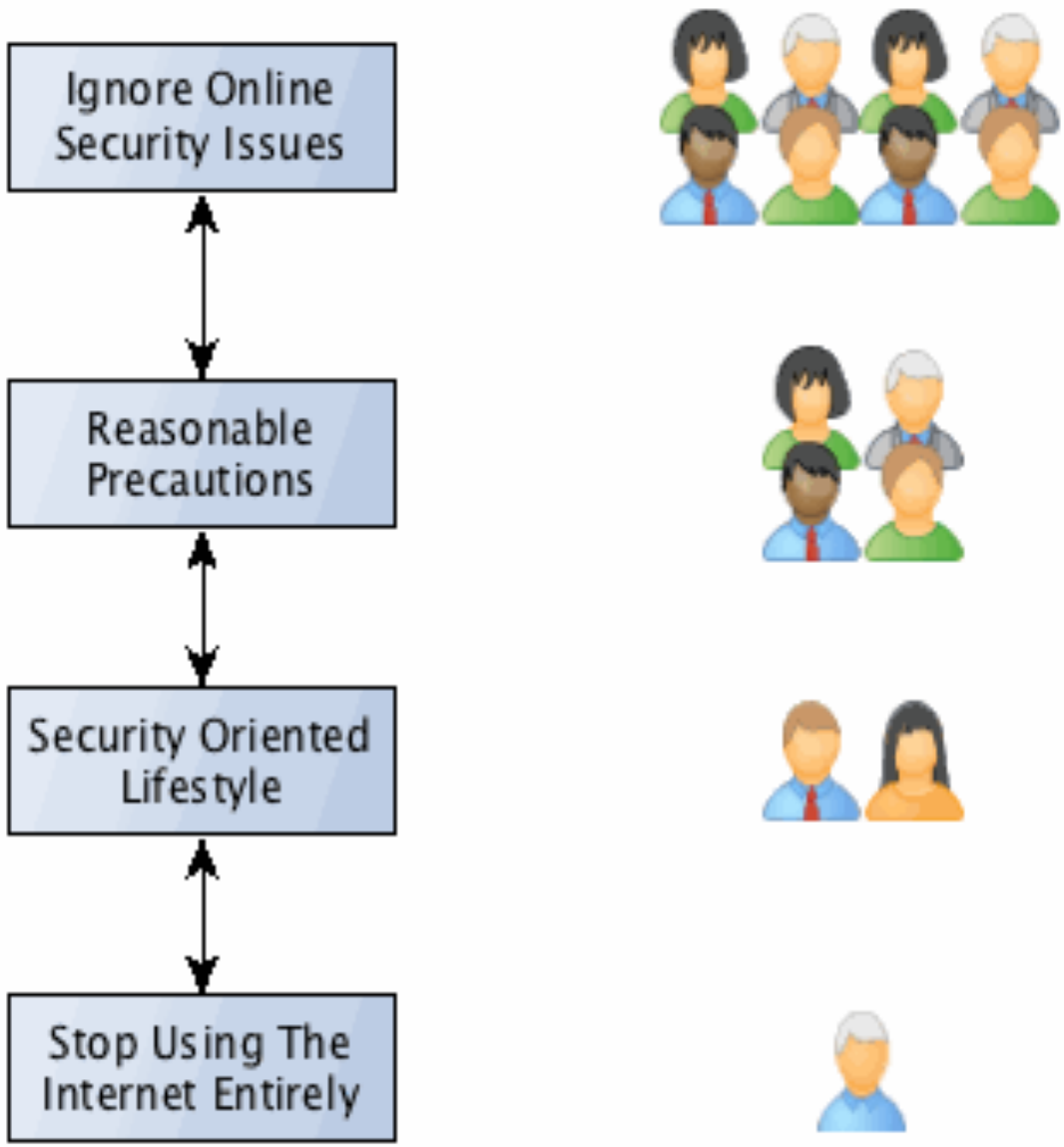
- I totally get that you don't plan to "do battle online."
- You just want to surf the web, maybe run some stuff in the cloud, use email and social media, IM with your friends, listen to some music, maybe buy a birthday gift for you spouse, file your income taxes...
- These are all very reasonable objectives, but they will only be possible if your connectivity is both **secure and reasonably private**.
- We also need to accept that **different people have different standards for what's "good enough"**

What's The Right Amount Of Security For YOU?

- ***Totally Ignore Online Security Issues:*** Default passive approach. Often ends up victimized.
- ***Will Take "Reasonable" Precautions:*** Most common option for those who are interested in/concerned about security and privacy. Will take some security steps, if not too painful.
- ***Strict "Security-Oriented Lifestyle:"*** Means forgoing at least some Internet functionality. For example, with JavaScript disabled, much of Google won't work (or won't work very well). This is a hard/ascetic path to follow.
- ***Disconnects From the Internet Entirely:*** An extreme choice, but a choice that some people actually do make. If chosen, the Internet truly has become a "denied area" for such users. Fortunately, relatively rare.



Security Choices



What We Practically Want, WRT Online Security

- We want you to be able to use the Internet safely and securely. For example:
  - Hacker/crackers shouldn't be able to remotely scan your system and find exploitable vulnerabilities.
  - If your system gets stolen, a thief shouldn't be able to access the information contained on it.
  - You'd like to be able to freely surf the Internet without worrying that you'll get infected with malware.
  - If you want to use the Internet, it should be available, not down due to someone DDoS'ing you or someone else at your site.
- These are, IMO modest goals that most should find reasonable.

What We Practically Want, WRT Online Privacy

- Maybe you'd also like to be able to use the Internet privately, without being monitored and tracked.
- This includes:
  - Being able to search the web and visit web sites without worrying that your every move is being tracked and recorded
  - Being able to use your smart phone without have it eavesdrop on your activities via its camera, microphone or geolocation capabilities.
  - Protecting your system against those who may want to rummage through files stored on your system, if given the opportunity to potentially do so.
  - Hardening your network connectivity against eavesdropping.

The Choices You Make WILL Impact OTHERS

- If you're a faculty member and you're careless with your credentials for the student information system, someone's FERPA-covered data might get leaked or changed with disastrous consequences for the university.
- If you're careless about malware, you may download a piece of malware that may then spread to your family members or office mates, making a lot of extra work for everyone
- If you're an IT person and you think security isn't "as big a deal as some people tell you it is," all the people who rely on a system you administer might get hurt
- So remember, your security choices potentially have consequences not just for you, but for everyone around you.
- And their choices can, in turn, have an impact on you
- We need everyone to do their part.

You Need to Also Recognize That While You *Want* To Be A Noncombatant, You're Still In A War Zone Online

- The US is now officially engaged in a "cyberwar:"

> *U.S. Secretary of Defense Ashton Carter confirmed this week that the U.S. has begun waging cyberwarfare against the tech-savvy Islamic State terrorist group.*
>
> *In an interview with the Financial Times, Mr. Carter said the U.S. Cyber Command team will start launching online attacks against the terrorist group.*
>
> *"I have give Cyber Command really its first wartime assignment, and we're seeing how that works out," Mr. Carter said.*

Source: http://www.washingtontimes.com/news/2016/apr/6/us-begins-cyber-war-against-islamic-state/

Our Agenda: Help You Take Prudent Steps

Some of the changes we need you to make are **behavioral** (we need you to change how you think about some things and how you do some things). Other changes are largely **technical**, involving how you configure your:

1) Computer
2) Web browser
3) Phone
4) Networks, and
5) Third Party ("Cloud") Network Providers

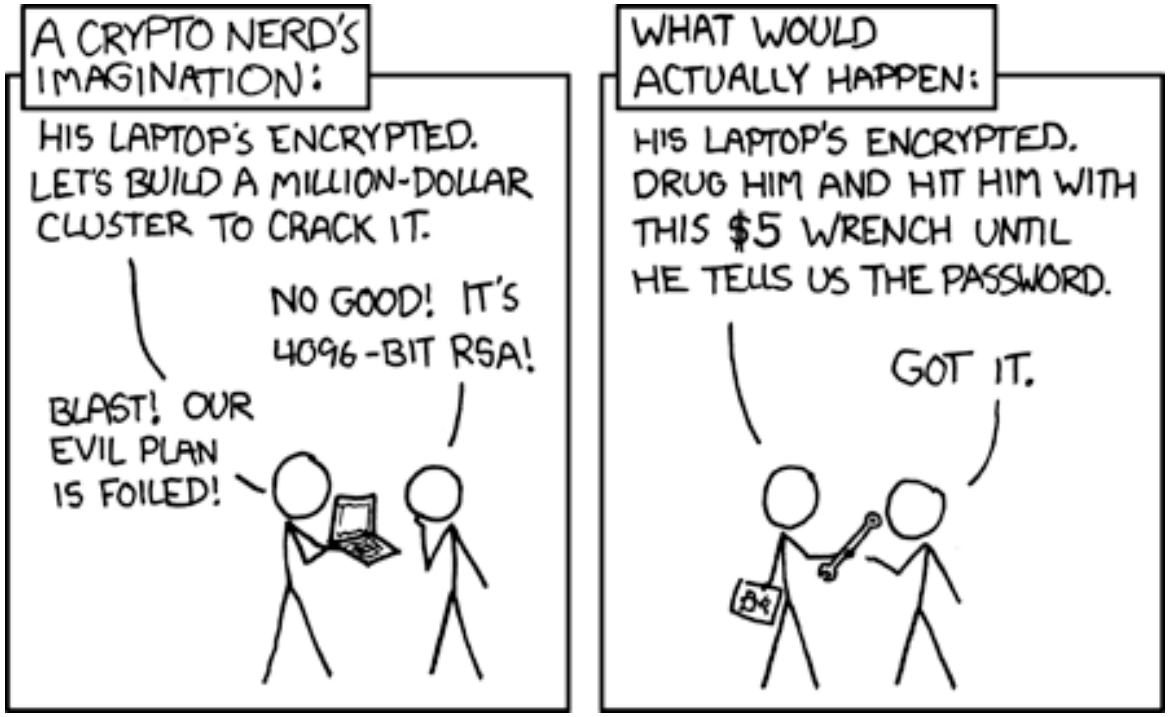
V. Security Begins With You (And May End With You, Too)

"Only amateurs attack machines; professionals target people. "

Bruce Schneier, Cryptographer and Cybersecurity Expert
https://www.schneier.com/crypto-gram/archives/2000/1015.html

You're Part of A System, and Unfortunately, Often Its Weakest Link

- The classic XKCD cartoon:



https://xkcd.com/538/

Attacking Highly Classified Defense Networks via Thumb Drives

- "The malicious software, or malware, caught a ride on an everyday **thumb drive** that allowed it to enter the secret system and begin looking for documents to steal. [...] Pentagon officials consider the incident, discovered in October 2008, to be the **most serious breach of the U.S. military's classified computer systems.** [...] What is clear is that [the infection] revealed weaknesses in crucial U.S. government computer networks — vulnerabilities based on the **weakest link in the security chain: human beings."**

  https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html [emphasis added] [incident referred to was "Buckshot Yankee"]

Hacking a Tech Journalist: Thanks, Tech Support

- "At 4:33 p.m., according to Apple's tech support records, someone called AppleCare claiming to be me. Apple says the caller reported that he couldn't get into his Me.com e-mail — which, of course was my Me.com e-mail.

  "In response, Apple issued a temporary password. It did this despite the caller's inability to answer security questions I had set up. And it did this after the hacker supplied only two pieces of information that anyone with an internet connection and a phone can discover."

  "**How Apple and Amazon Security Flaws Led to My Epic Hacking",** http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

ID Cards, ID Badges, etc.

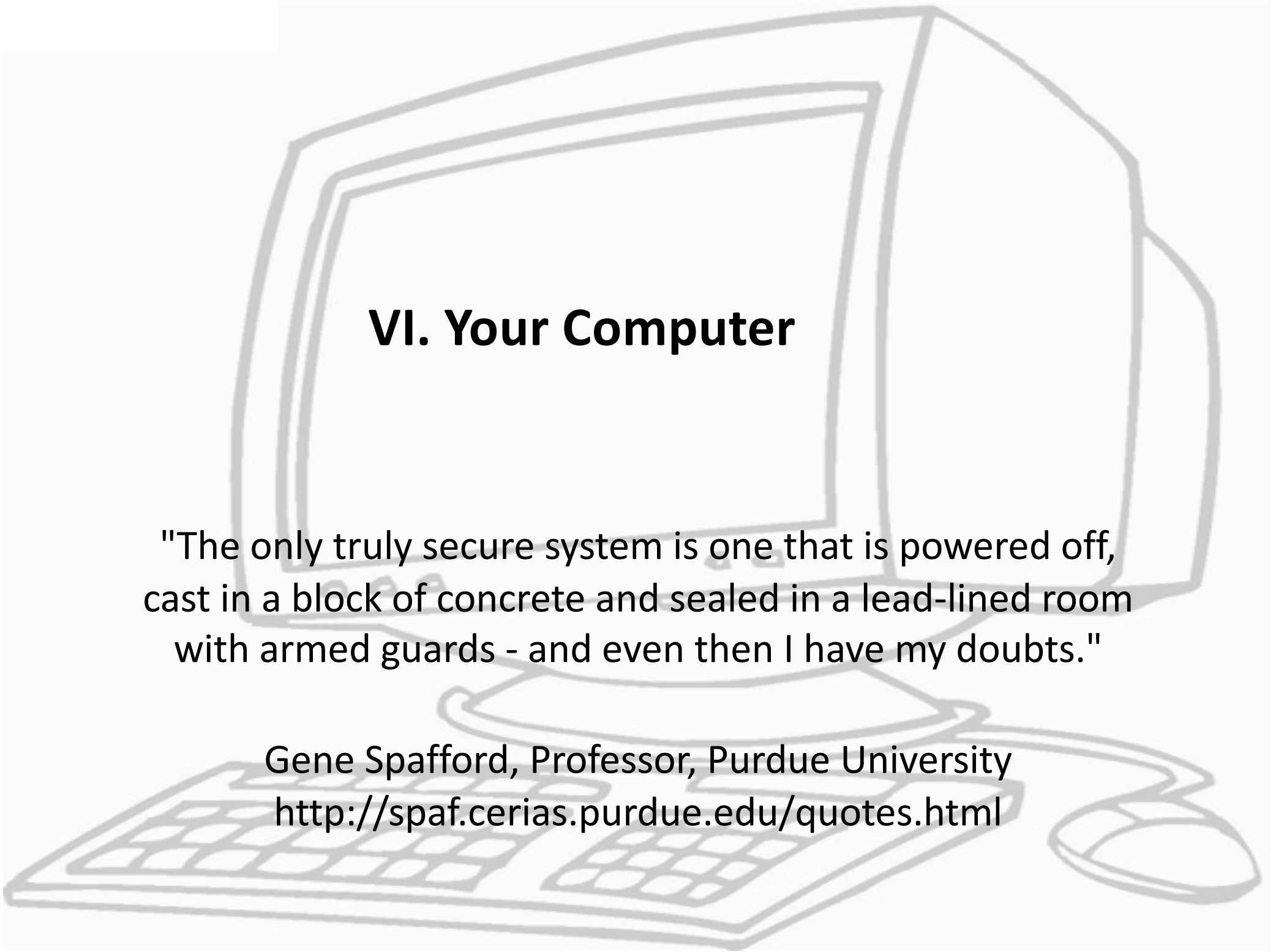
- If you're Norm Peterson from the classic TV show "Cheers," everybody knows your name.
- If you're an employee at a growing number of colleges or universities, most folks likely rely on your **ID card** or **ID badge.**
- **Machine-readable ID cards** can help **improve** security, e.g., when they're used as part of a building's access control system (scan your card, enter your secret code, get in to the facility).
- Prominently relying on the appearance of IDs badges can **reduce** security. (Remember sneaking into bars when you were under age?) Some badges may be easily forged, and without a database backing it up, you may end up trusting someone you shouldn't.
- Challenge **anyone** you don't recognize in a secured area, badged or not. If you're not comfortable doing so yourself, **immediately** tell your manager or whomever's in charge.

Your Trash; The Bad Guy's Toe Hold Into Your Site

- What you throw away isn't necessarily gone. Stuff that's been thrown away may easily be retrieved by an adversary who's simply willing to rummage around a little through your trash.
- When a hacker d00d does this, it's often called dumpster diving (when Federal agents do it, it's called running a 'trash cover')
- You should routinely shred ALL documents you discard (and be sure to use a good quality microcut shredder, not a shredder that makes relatively wide continuous strips).
- Burning discarded documents can be an ever better solution.
- We'll discuss securely discarding surplus hardware later.

The Behavioral Changes We Need

- **You've been trained to "do as you're told**." Unthinking obedience is **very** bad. "Do as you're told" and you may end up getting phished. Ask questions. Double check. Be skeptical.
- **You've been trained to "help," even when you have no obligation to do so:** "Gosh! Someone lost this 128GB thumb drive marked 'final dissertation draft' in the parking lot – if I check it on my computer, I bet I can see who lost it..."
- **You've be trained to be "polite."** Example #1: As you approach the door where you work, you see a person with an armful of boxes also approaching that secure door. They call out, "Hold the door, please!" Do you do so? Example #2: "My computer's dead. Could I briefly borrow *your* computer to show my slides?"
- **You may have been taught to act and not "think too much" in an emergency.** Never rush! Be cautious! It's like the joke about pilots: there are old Internet users, and bold Internet users, but...



VI. Your Computer

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Gene Spafford, Professor, Purdue University
http://spaf.cerias.purdue.edu/quotes.html

Choice of Hardware

- Let's assume (whether it's true or not) that you can buy any sort of computer you want: a system running Microsoft Windows, a Mac, or a Linux or BSD system, for example. What should you buy?

- This is obviously a deeply emotional question, rivaling religion, politics, sex and salaries as topics that are best avoided when visiting friends or family for drinks and dinner.

- I'll merely offer two observations:

  1) If you go to any meeting attended by cyber security professionals, **you'll see an awful lot of Macs** (including mine)
  2) Of the hundreds of millions of pieces of malware out there, almost all of it does **NOT** run on Macs.

Operating Systems

- Stay current. Whatever hardware you end up running, run the most recent (production) version of it's operating system
- For example, if you're on a Mac, you should run OS X El Capitan
- If you're a Windows user, run Windows 10, not some earlier version of Windows (and remember, at least at the time this was written you can upgrade to Windows 10 from at least some earlier versions of MS Windows for free!)

  If your MS Windows computer isn't "powerful enough"/compatible with Windows 10, it's *way* past time for you to upgrade your computer.

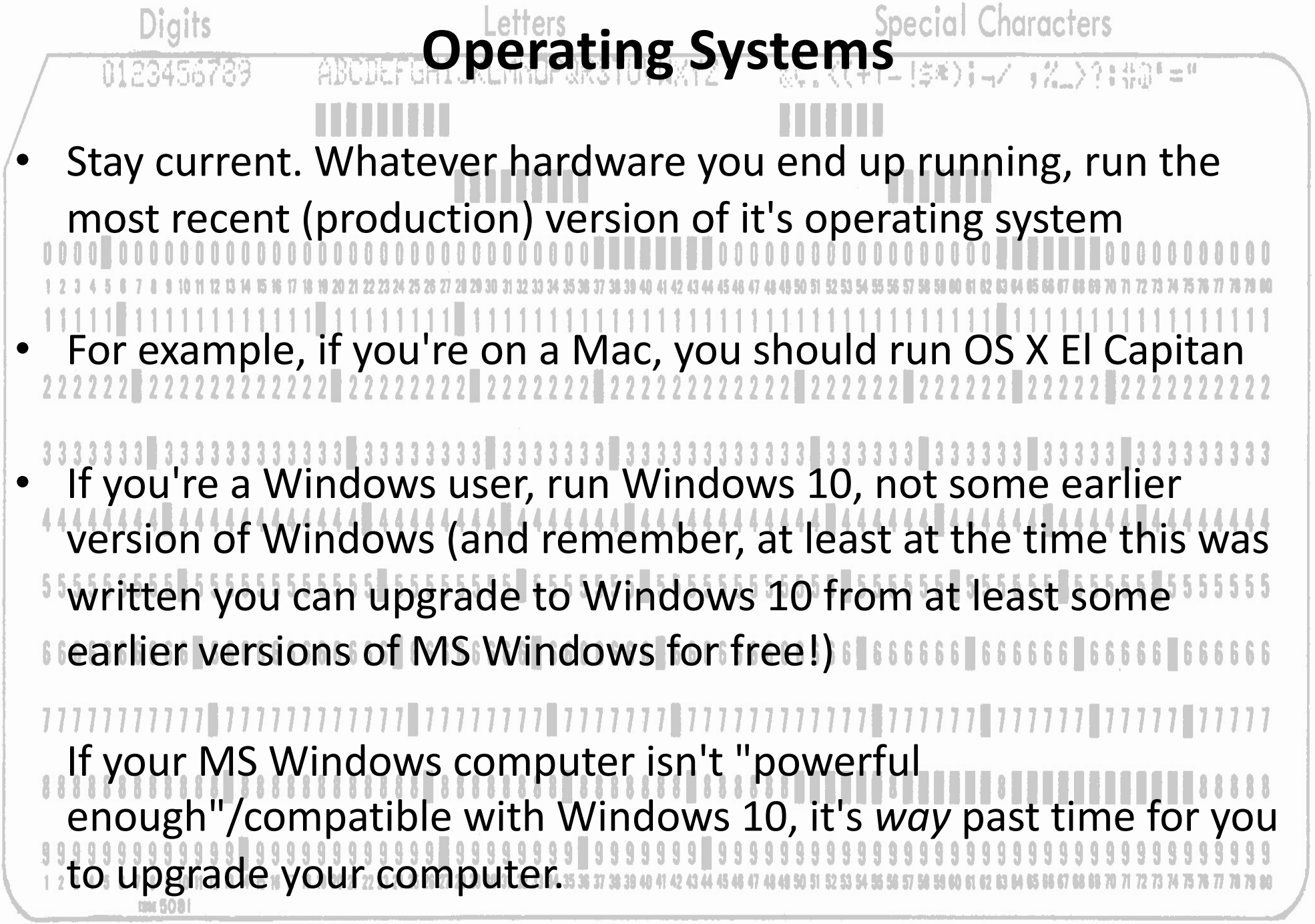


Figure 4. Card Codes and Graphics for 64-Character Set

Patch, Patch, Patch

- **The single most important thing you can do to secure your computer is to patch it, and all the applications running on it.**
- In general -- unless you receive specific instructions to the contrary from your manager or from your local security people -- **set your computer and all software running on it to self-update whenever updates become available.**
- Yes, there's a vanishingly small risk that you might get bitten by a bad patch, but you face a MUCH, MUCH, MUCH BIGGER risk of getting 0wn3d if you leave your system unpatched.
- Fascinating paper:
  "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices,"
  https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf And what was the #1 recommendation of the experts? **"Update Your System"**

WHAT To Patch/Update? *Everything*, Of Course!

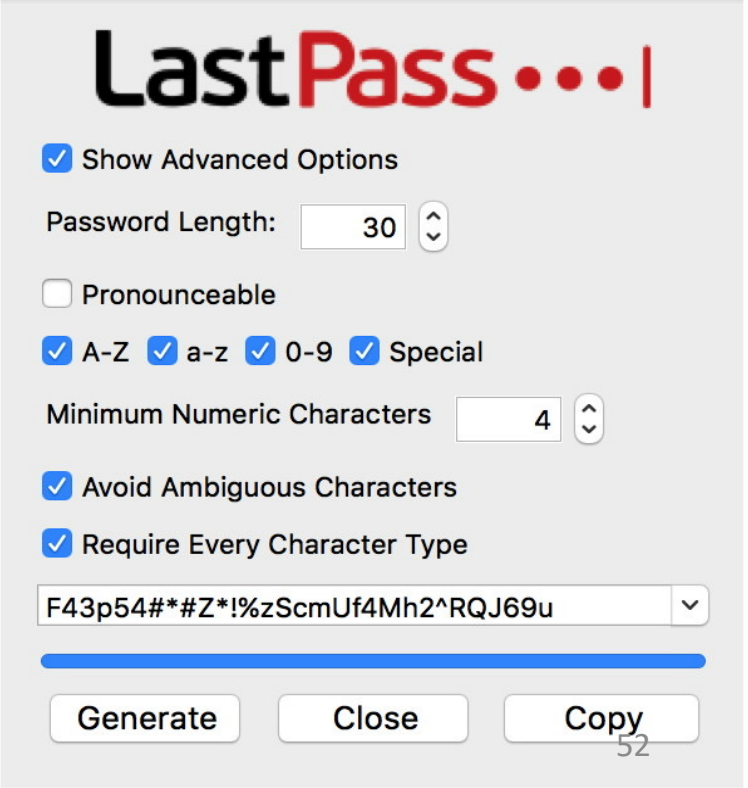
- The **operating system** (most people now tend to be pretty good about doing this, except when they're on a slow connection)
- **Vendor-specific updates** (HP is very fond of this sort of thing)... these vendor updates are in *addition to* regular OS updates!
- **Security software** (antivirus, software firewall, etc.): they may fail to update if you were running "trial ware," and you haven't purchased a license (note: there are some terrific free options)
- **Office software suite** (may get handled with the OS, or may not – periodically check your office software's update status manually)
- Your **web browser** (your most-used app needs to be up-to-date)
- Any **helper applications** or extensions used by your web browser
- Any other software you may have purchased or downloaded
- **Secunia PSI** can really help manage this in the Windows world
- Mac? Check out **AppFresh** (14 day free trial of a for-fee product)

Backups

- Backups tend to be like the old comedian Rodney Dangerfield: they "just don't get no respect."
- These days, however, with Cryptolocker and comparable ransomware threats in broad circulation, backups have taken on a new and critically pivotal role...
- With backups, if you get hit by a file encryptor, wipe the machine, restore from backups, and drive on – minor annoyance.
- Without backups, you'll often be faced with two pretty bad choices: pay the ransom, or live without your sometimes irreplaceable files
- Ouch
- Please take backups of your system, and keep more than one generation of backups in multiple locations (just in case your most recent one is corrupted or becomes inaccessible)

Password Manager

- Passwords play a crucial role in securing many services. Let me emphasize the word **MANY** in the preceding line. That's the problem. We all have far too many passwords to sanely manage.
- One solution is to write your passwords down in a little black book, but that's sort of "old school." The best solution to this is probably to use a password manager. Doing so makes it realistically practical for you to use very **strong passwords**, and DIFFERENT strong passwords for each site where you need to login.
- Once you try one, you'll never believe you lived without one.
- Tempting as the sample password over there may be, please choose another. :-)



Multifactor

- Many of the services you use continue to just rely on plain old passwords to control access.
- Use of just plain old passwords is as wrongheaded as a belief in a Ptolemaic ("geocentric") universe. You really want to get with the modern era! Augment your plain old password (something you know) with something you have (such a cryptographic hard token or your smart phone), or something you are (such as your fingerprint, a photo of your eye, or a sample of your speech – but when it comes to biometric, beware of coerced "cooperation").
- Many sites, including the University of Maryland Baltimore, use Duo Security, a multifactor product that's offered as part of a special academic deal through InCommon. It works great, and I recommend it highly (ObDisclaimer: I used to run the InCommon Multifactor Program when I worked for Internet2)

Anti Virus

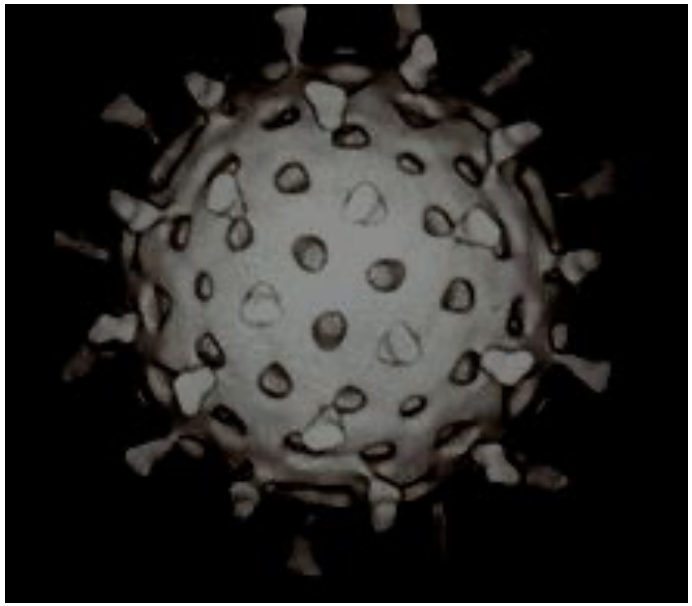
- Anti virus software won't *always* work, but it *may* work *sometimes*, and since people expect it, you should still use it.
- Doing so is not without risk, however. Every piece of software you run may have it's own problems, including security software:

"A bug in its software meant that Trend Micro accidentally left a remote debugging server running on customer machines. ***The flaw****, discovered by Google's Project Zero researcher Tavis Ormandy,* ***opened the door to command execution on vulnerable systems (running either Trend Micro Maximum Security, Trend Micro Premium Security or Trend Micro Password Manager)."***

"Patch out for 'ridiculous' Trend Micro command execution vuln" http://www.theregister.co.uk/2016/03/31/trend_micro_patches_command_execution_flaw/ [emphasis added]

"Which Anti Virus Software Should I Run?"

- Interesting/tricky question. We know bad guys test and tweak their malware to avoid the most popular antivirus products. This may imply that the most popular antivirus products may miss some of the more aggressive malware (since the malware may have been specifically tailored to avoid being detected by it)
- Less popular antivirus products, on the other hand, may be less popular for good reasons. Less popular antivirus products may also not be able to afford to maintain the analysis team and facilities needed to keep up with today's flood of malware.
- The best thing to do may be to run an operating system that's less-targeted by malware, **plus** an antivirus product of your choice.



Firewalls

- Firewalls are much like anti virus software: they're not perfect, but still, they're a staple recommendation of most security pundits.
- If you **don't** have one running, you'll be crucified if something goes wrong that could have been stopped by one.
- Check to see what you've got open with GRC's Shield's Up https://www.grc.com/x/ne.dll?bh0bkyd2 (select "All Service Ports" after agreeing to the sites terms and conditions). Ideally, as results, you should see a matrix of only little green squares (if you're running a firewall).

Some of the Problems With Firewalls

- The firewall "medicine" can be nearly as bad (or worse) than the insecurity "disease."

  Firewalls...

  -- provide an illusion of "total security," and that can lead to complacency ("crunchy on the outside, gooey in the middle")
  -- they break end-to-end transparency (RFC2775 and RFC4924)
  -- they can make it hard to go fast
  -- they can complicate provisioning and debugging services particularly if non-1:1 network address translation/PAT is used
  -- they can result in the de facto creation of a "two-port Internet" (everything over http/https)
  -- ....

If You Do Firewall, Firewall At the Host (or at the Subnet), NOT At the Institutional Border

- Perimeter firewalls are a lot like traditional medieval castles: you want to carefully limit who/what is inside the walls with you.

- Putting a firewall at the institutional border means that you may have 20,000 of your "closest friends" inside the firewall with you and your sensitive systems. Are you sure that you trust each and every one of those users, and each and every one of their devices?

- Beware of attacks that specifically target firewalls, too (e.g. state exhaustion attacks). Simple router ACLs (access control lists) may be preferable in some cases.

System Login / Idle System Screen Lock

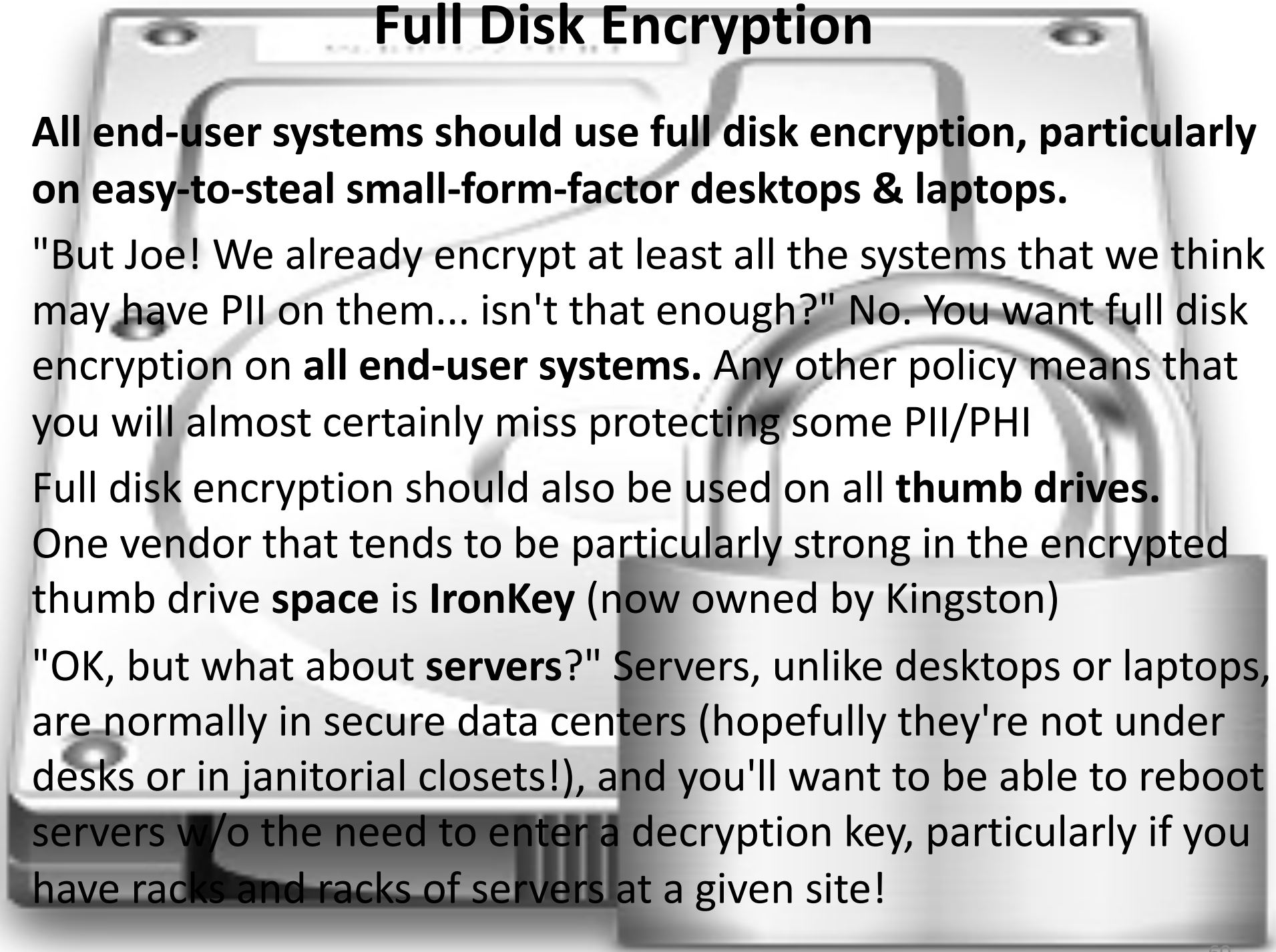
- Very basic, but you'd be surprised how often people don't bother: all end-user systems should require a physically present user to login before granting access at boot time.

- All end-user systems should also have an idle system screen lock that activates after some reasonable period of inactivity.

- Some might also be interested in trying a hardware proximity-based lock such as Gatekeeper from https://gkchain.com/

  That token-based product locks your screen when you walk away, and unlocks it automatically when you return.

Full Disk Encryption



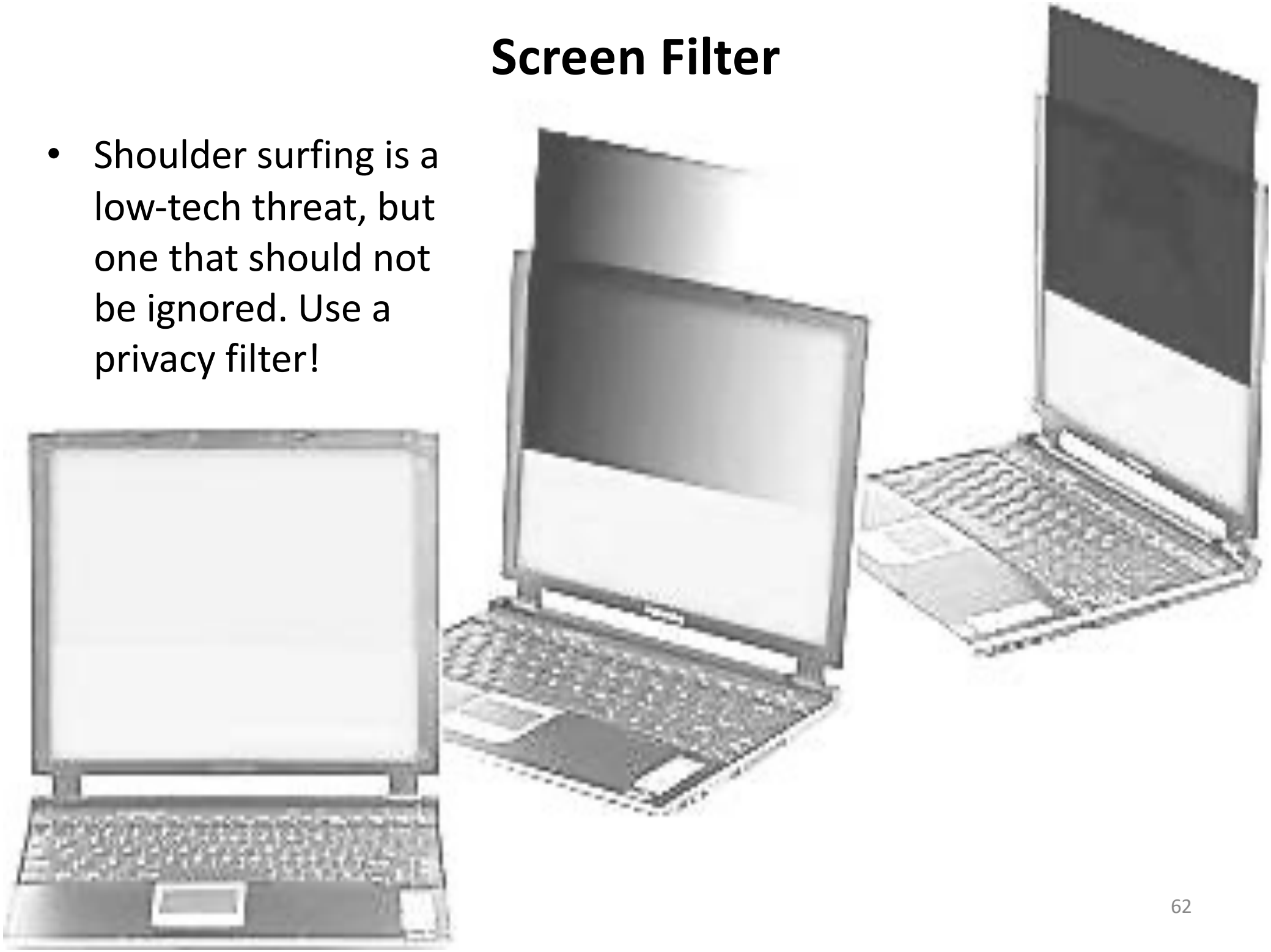
- **All end-user systems should use full disk encryption, particularly on easy-to-steal small-form-factor desktops & laptops.**
- "But Joe! We already encrypt at least all the systems that we think may have PII on them... isn't that enough?" No. You want full disk encryption on **all end-user systems.** Any other policy means that you will almost certainly miss protecting some PII/PHI
- Full disk encryption should also be used on all **thumb drives.** One vendor that tends to be particularly strong in the encrypted thumb drive **space** is **IronKey** (now owned by Kingston)
- "OK, but what about **servers**?" Servers, unlike desktops or laptops, are normally in secure data centers (hopefully they're not under desks or in janitorial closets!), and you'll want to be able to reboot servers w/o the need to enter a decryption key, particularly if you have racks and racks of servers at a given site!

Physical Security

- Some of your greatest computer-related risks are associated with real world **physical security** phenomena such as:
  - Having your unencrypted laptop **stolen** from your unlocked office, or having your unencrypted laptop stolen from your car trunk or hotel room while traveling. Use full disk encryption, then lock up your laptop or keep it with you!
    You may find a device locator service such as FindMyMac or LoJack for Laptops to be helpful if laptop theft is a material risk for you (note: obvious tracking-related tensions here...)
  - Dropping your laptop, or having it **accidentally damaged** (spilled liquids, knocked off a table at a conference, crushed by a fellow passenger while you have it in an overhead bin on a plane, etc.). Insurance, a hard case, care with power cords, and a silicone keyboard membrane can all help to reduce your exposure.

Screen Filter

- Shoulder surfing is a low-tech threat, but one that should not be ignored. Use a privacy filter!



Discarding Hardware

- Maybe you had to replace your old MS Windows laptop in order to be able to run Windows 10. After you're sure you've transferred all the files you need from your old system, but **before** that hardware gets surplused or otherwise disposed of, it needs to be sanitized. One popular tool for wiping drives is DBAN, see http://www.dban.org/
- When it is not possible to run a software disk sanitizer, or if you have a large number of disks to process, or if you need extra assurance, consider obtaining a hard disk destroyer that can crush/shred no-longer-needed hard drives, smartphones, etc.
- Special note: you may get push back from your property control office if you seek to destroy "serviceable" but unneeded property. In the case of security-sensitive hardware, institutional security (should) trump relatively minor cost recovery opportunities. Recycle desks, not disks.

VII. Your Web Browser

Use An Alternative Browser

- If you're like most people your web browser is one of your most-used applications. Most operating systems come with a bundled web browser such as Microsoft's Edge, or Apple's Safari. Because it comes pre-installed, many people just use those bundled web browsers by default.

- I recommend that you consider installing and using an alternative browser, instead. Three choices worth considering are:

  -- Firefox
  -- Chrome
  -- Opera

Helper Apps: Don't Install Them If At All Possible

"*According to the country report for the fourth quarter of 2014 regarding the vulnerability state of machines in the United States,* ***Java is at the top of the list of software that exposes users' machines to unnecessary risks.***

The data in the report from Secunia shows that on almost half (48%) of the US systems with ***Java*** *installed, a vulnerable version was found. Apple* ***QuickTime*** *was detected to be outdated in 44% of the cases.*

Adobe Reader *10.x appears as unpatched on 49% of the computers that have the product on the list of installed programs."*

Source: "Java, QuickTime and Adobe Reader Present Highest Exposure Risk in US and UK," [emphasis added]

http://news.softpedia.com/news/Java-QuickTime-and-Adobe-Reader-Present-Highest-Exposure-Risk-In-US-and-UK-470616.shtml

DO Use AdBlock Plus

- None of us need to view online ads, yet we many of us routinely accept them as part of the web pages we visit.
- In doing so, we unnecessarily expose ourselves to a great deal of potential "malvertising" (malicious advertising). Note that you may get hit with malvertising even when you're visiting perfect reasonable/legitimate sites (e.g., this is not just something you only encounter on "iffy" or out-and-out "bad" web sites).
- Give strong consideration to **blocking all advertising** using Adblock Plus. Doing so will remove an avoidable risk, and will often speed up your surfing, too.
- Note: a few sites may block your access if you refuse online ads (this currently includes Forbes and Wired, among others you may run into)

Use Ghostery to Defeat Trackers

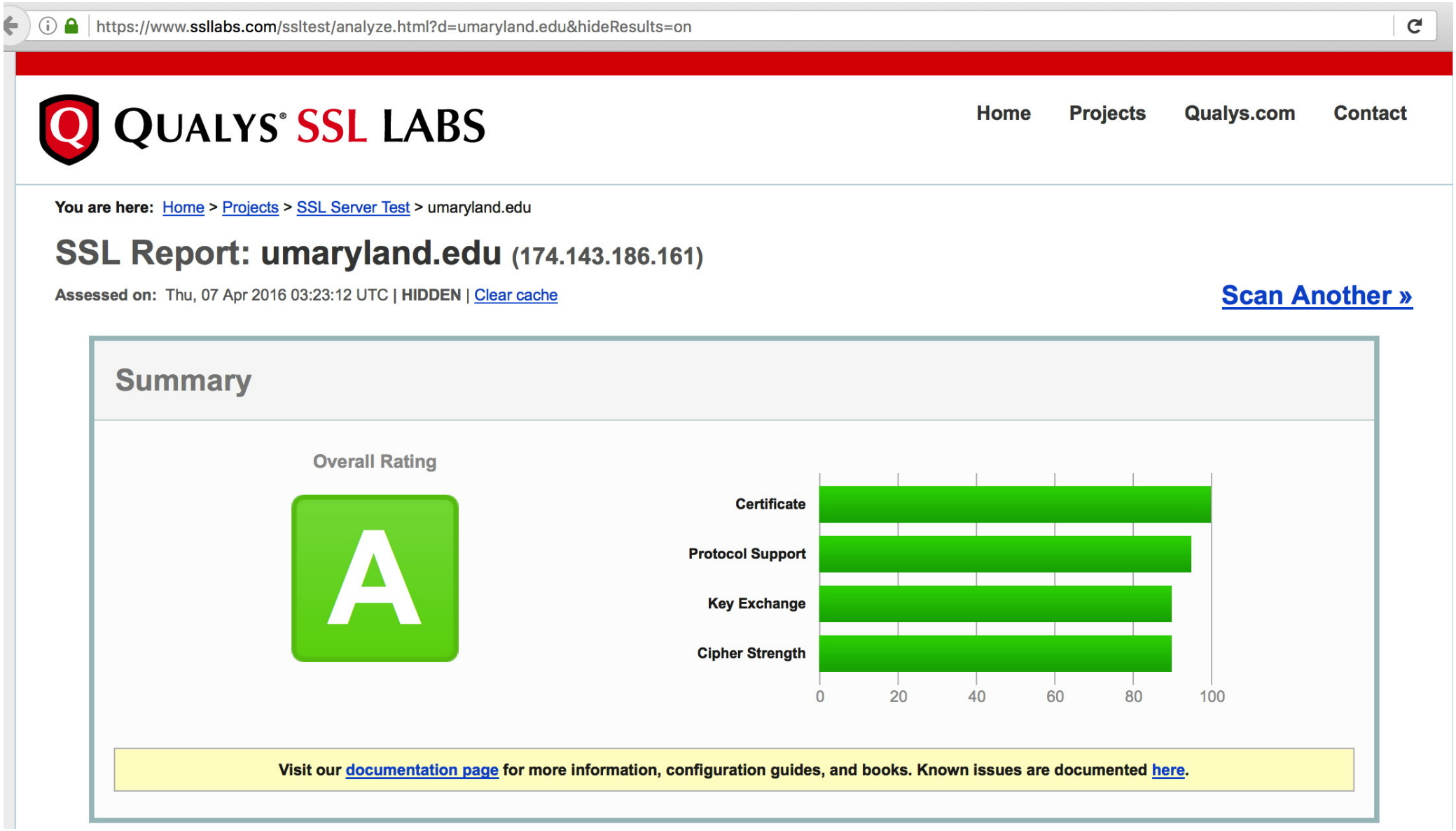
- Ad blocking tools help control what you're shown on screen, and that's great. However, if you value your privacy, you also want to control "trackers."

- Blocking trackers, in addition to helping to preserve your privacy, also reduces the number of unnecessary visits to potentially dangerous third party sites (sorry about sounding like a broken record).

- To block trackers, you may want to run an anti-tracker add-on such as Ghostery.

  When you first try it or a comparable product, you may be surprised at the number of trackers present on some web pages.

SSL/TLS: Check The Quality of Your Sites' Web Crypto



VIII. Your Smart Phone

This is one "denied area"
I don't think we can fix.

DON'T USE A MOBILE PHONE?

- Everyone has a smart phone, I know, I know. Some people would sooner have one of their legs amputated then live without one. And yes, I do know that they're cool and useful and hard to live without. However, at the same time, they're:
  -- Widely targeted for intrusive monitoring
  -- A terrific data collection device that makes it trivial to obtain a social graph of all your family, friends and associates
  -- Continually tracking your location (even when "turned off")
  -- Able to be surreptitiously turned into a bug and surveillance device (see for example https://media.blackhat.com/us-13/US-13-McNamee-How-To-Build-a-SpyPhone-Slides.pdf)
- There's a reason why phones aren't even permitted at most sensitive installations
- Weird stuff is happening with cell phones, even here in Baltimore

www.theguardian.com/us-news/2016/apr/05/maryland-stingray-ruling-baltimore-convictions-privacy

Baltimore

Stingray ruling could challenge hundreds of Baltimore convictions

Maryland could appeal to supreme court to reverse ruling that found police use of device to track cellphones without warrant in violation of fourth amendment

Baynard Woods in Baltimore

@baynardwoods

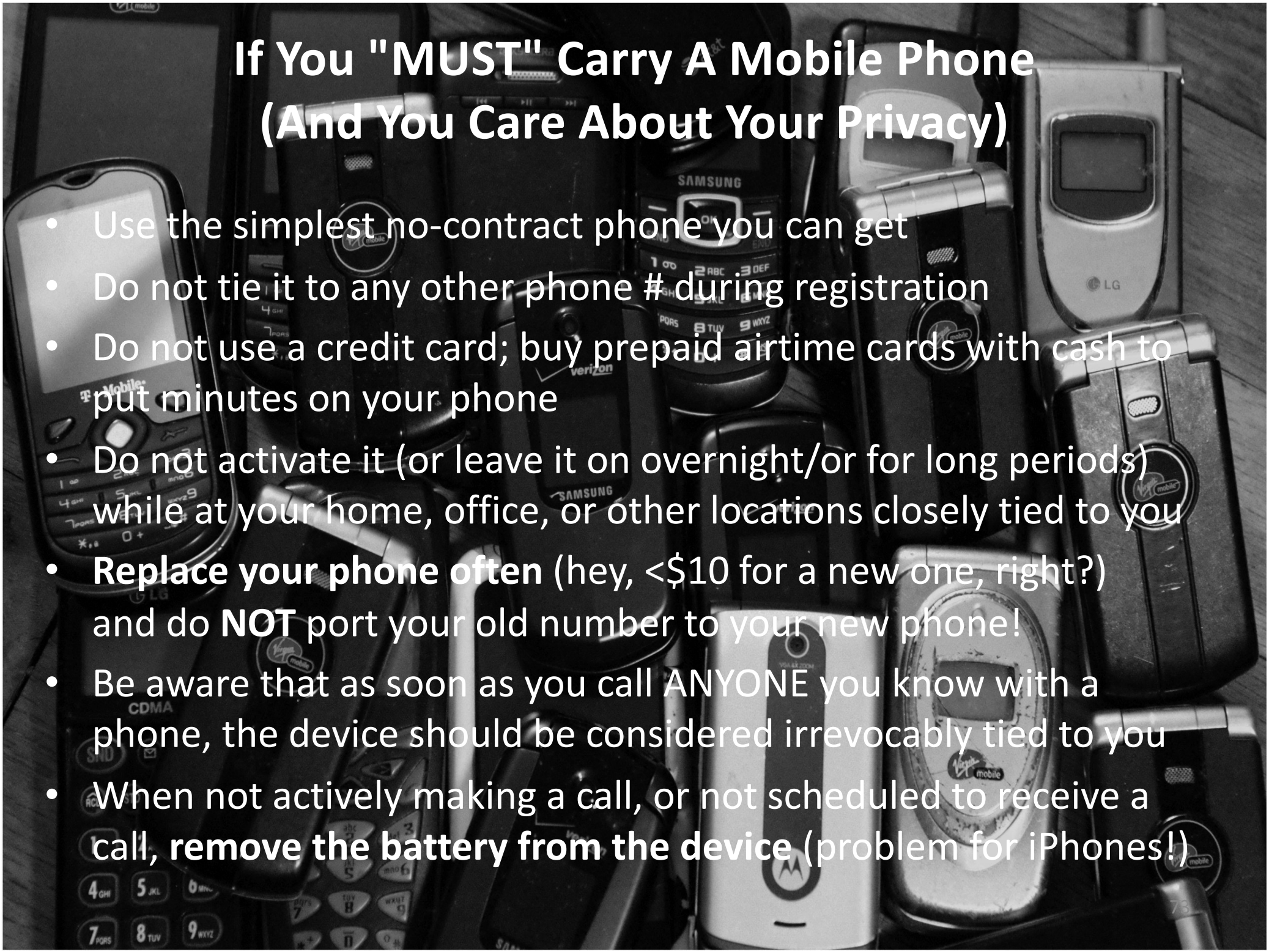
Tuesday 5 April 2016
14.17 EDT

Comments
47

Save for later

Stingray ruling was the first by an appeals court to hold that using cell site simulator technology without warrant violates a person's right against illegal search and seizure. Photograph: Electronic Frontier Foundation via Flickr / Creative Commons

A major Maryland court ruling that found police cannot use cellphones as a "real-time tracking device" without a warrant could call into question hundreds, if not thousands, of convictions in Baltimore - and set a precedent for similar



If You "MUST" Carry A Mobile Phone (And You Care About Your Privacy)

- Use the simplest no-contract phone you can get
- Do not tie it to any other phone # during registration
- Do not use a credit card; buy prepaid airtime cards with cash to put minutes on your phone
- Do not activate it (or leave it on overnight/or for long periods) while at your home, office, or other locations closely tied to you
- **Replace your phone often** (hey, <$10 for a new one, right?) and do **NOT** port your old number to your new phone!
- Be aware that as soon as you call ANYONE you know with a phone, the device should be considered irrevocably tied to you
- When not actively making a call, or not scheduled to receive a call, **remove the battery from the device** (problem for iPhones!)

Use A Long and Complex Password To Lock Your Phone

- Rather than just leaving your phone unlocked or relying on a four digit all numeric pin, most phones will allow you to enable a longer complex password. You should do so. See for example:

  "Use a passcode with your iPhone, iPad, or iPod touch https://support.apple.com/en-us/HT204060

- "What about integrated fingerprint readers?"

  They're certainly convenient, but do you think someone could get a court order to force you to unlock your phone? Sure...

Use Application Layer Crypto, If Your Phone Supports It

Rather than just relying on the phone itself to provide secure messaging, use a security-enhanced messaging application such as Bleep, Signal, or Wickr, instead.

	Bleep	Signal	Wickr*
E2E Encrypted 1:1 Voice	Yes	Yes	Voice Messages
E2E Encrypted 1:1 Text	Yes	Yes	Yes
iPhone	Yes	Yes	Yes
Android	Yes	Yes	Yes
Mac OS X	Yes	Beta	Yes
MS Windows	Yes	No	Yes
Linux	No	No	Yes
Peer to Peer	Yes	No	No
Open Source	No	Yes	No
Linked to Email	Optional	No	Optional
Linked to Tel #	Optional	Yes	Optional
Cost	Free	Free	Free

IX. Your Networks

All Networks Are Equally Trustworthy, Right?

- All networks should be assumed to be equally **untrustworthy.** For what it may be worth, Google agrees with me, see "Google reveals own security regime policy trusts no network, anywhere, ever," http://www.theregister.co.uk/2016/04/06/googles_beyondcorp_security_policy/
- What could happen on an untrusted network?
  - Unencrypted traffic may be eavesdropped upon, including usernames and passwords, credit card numbers, or other PII.
  - Unencrypted traffic may be modified (or selectively dropped). For example, malware might be injected.
  - The network might point you at an untrustworthy DNS servers, which might result in you being misdirected to an untrustworthy site.
- So what should you do? **ENCRYPT ALL NETWORK TRAFFIC.**

Application Crypto vs. VPNs

- There are basically two different approaches to handling encryption of network traffic.
- Individual applications, such as SSH, can encrypt traffic all the way from your client all the way to the server, **"end-to-end."** We like that, a lot. However, that's application-by-application.
- Virtual private networks, or VPNs, on the other hand, can encrypt all the traffic from your workstation, but NOT end-to-end, just up to the VPN concentrator.
- Neither approach is perfect on its own. In the ideal world, you want layered protection, so use BOTH approaches: nest SSH (or some other end-to-end encrypted application) within a VPN.
- An added "free" benefit of using a VPN: you will normally end up using trusted domain name servers provided by your VPN provider rather than random local network name servers.

Speaking of DNS, Let's Talk About DNS "Firewalls"

- DNS is a tremendous convenience. It's a lot easier to remember www.umaryland.edu than 174.143.186.161
- However, there's nothing that says you have to cooperate with bad guys when it comes to providing THEM with DNS. In fact, you should use your DNS as another way to *interfere* with the bad guys. Block DNS names that are used solely for no good!
- Multiple providers offer this sort of blocking service for free:
  -- https://www.opendns.com/home-internet-security/
  -- http://dyn.com/labs/dyn-internet-guide/
  -- http://dns.yandex.com
  -- https://dns.norton.com/
- Why do these companies offer this free service? Answer: your DNS queries represent a potentially valuable sources of telemetry about what's happening on the Internet.

An Aside: 3rd Party VPNs

- When I talk about using a VPN, by the way, I'm talking about your local institutional VPN, not a VPN run by a random third party as a commercial service.

- In general, I do NOT recommend trusting third party VPNs. Third party VPNs may subject you to additional risks you otherwise might not face, including:

  -- dubious co-users,
  -- untrustworthy VPN administrators, and
  -- laws of other jurisdictions associated with the VPN concentrator's location (and the apparent "origination" point for your VPN tunneled traffic)

While We're Talking Networks: Instrument Your OWN Network (IF You're The Person Running It)

- You need to know what's happening on any network you administer. That means running an intrusion detection system such as Snort or Bro on it, or a commercial network monitoring product such as Fireeye. You may also want to consider collecting Netflow/Jflow/Sflow (be sure your flow collection project collects both IPv4 AND IPv6 traffic).

- Be sure to let people know what you're doing as part of your privacy policy disclosures, too.

- Do NOT sniff or otherwise collect network traffic if you're not legally authorized to do so!

X. Third Party ("Cloud") Providers

"The Cloud"

- The cloud is very seductive.
- It lets you "avoid doing your chores" by letting someone else do them for you, sometimes for "free."
- "Cloud" solutions can take on many different forms, including:
  -- Cloud-based email solutions (such as Google for Education)
  -- Cloud-based compute platforms (such as AWS)
  -- Cloud-based application providers (such as Salesforce or RingCentral)
  -- etc., etc.
- What's common to all cloud providers is that you're no longer running the service, they are. Since that's the case, you need to trust those who do. But what's the basis for doing so? How can you tell which ones are worth relying on and which ones may not be?

Cloud Security Alliance Cloud Controls Matrix

- If you're an individual, you don't have much choice. You can use a cloud provider, or not. Take it or leave it. Your choice. :-)
- However, if you're a major institution, like a university, you may have at least some negotiating or detective powers.
- When you get right down to it, if you like the product under consideration, the one other critical thing you need to know is, "Is the service secure?"
- One of the best systematic reviews of that sort of thing is the list of controls available as the CSA Cloud Controls Matrix. If your provider has already written a document describing how they satisfy the controls outlined in that document, ask for a copy. If they haven't produced/won't create such a document... Hmm.
- When you look at the response you receive (if you receive one at all), you'll know an awful lot about the maturity of that program.

Federated Authentication With Shibboleth

- If you're using the cloud, you need to think about how you'll authenticate. In general, institutions should insist on Shibboleth, as offered through InCommon. You can see who currently participates: http://www.incommonfederation.org/participants/
- Federated authentication separates authentication (who you are) from authorization (what you're allowed to do), and allows you to safely use your home institution's credentials for cloud services in a privacy preserving sort of way.
- For example, if you're accessing an online chemistry database licensed for use by University of Maryland Baltimore faculty, the database provider doesn't need to know your name or your faculty ID number, they just need to know if you're a faculty member with the right school. Shibboleth provides that sort of fine-grained attribute release control, without the need for kludgy authentication "solutions."

X. Conclusion

Nothing ever comes for free

This world is watching me

* * *

Now all that's left is all I need,

This world is watching me

Armin van Buuren, "This World Is Watching Me"

Wrapping It All Up

- We're living in an unprecedented time for the Internet.
- Never have we relied on it more... and yet, average users face daunting threats to using it securely and with reasonable privacy.
- Some may give up and do nothing. Others may be overwhelmed and cease using the Internet altogether. Both of those are "fails."
- You now know enough to keep using the Internet, but hopefully at least a little more securely.
- I hope you will do **your part** to keep yourself and the University of Maryland Baltimore secure online.

Thanks For The Chance To Talk!

- If everything stayed on track, we should have time for a few questions, if there are any...

- Remember, the slides for this talk are available online at:

  https://www.stsauver.com/joe/umb-cybersec/