What is Security, anyway?

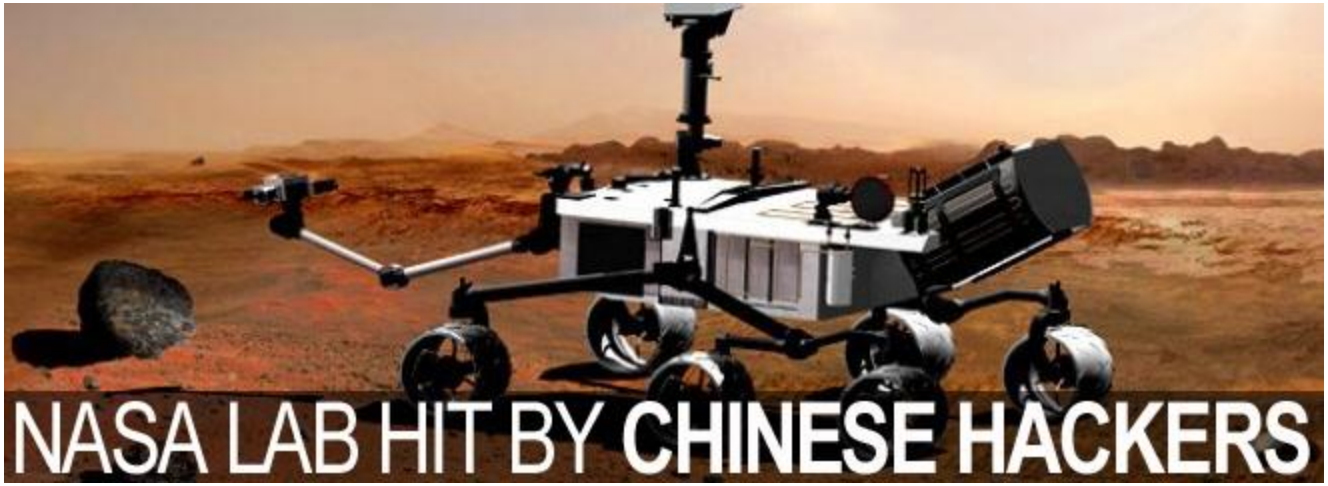
Richard Ford
Harris Professor of Assured Information
Co-Director, Harris Institute for Assured Information

Good evening… why should we listen to you?

- Prof. Richard Ford
  - University Professor
  - Associate Director, Harris Institute for Assured Information at Florida Tech., a DHS/NSA National Center of Academic Excellence in Information Assurance Research
  - Editorial Board member, Virus Bulletin, IEEE S&P, Elsevier's Computers & Security etc.
  - Been working in computers for about 20 years
  - Interdisciplinary research on disruptive technology

Florida Institute of Technology
Harris Institute for Assured Information

The State of the Nation



- "In 2010 and 2011, NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems," his report states. "These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit."

  Other incidents "may have been sponsored by foreign intelligence services seeking to further their countries' objectives," he [Paul Martin, NASA Inspector General] noted.
- Source: foxnews.com, March 2012

Florida Institute of Technology
Harris Institute for Assured Information

More…

Florida Institute of Technology
Harris Institute for Assured Information

And Still More…

Florida Institute of Technology
Harris Institute for Assured Information

Tell me when to stop…

Florida Institute of Technology
Harris Institute for Assured Information

And the list goes on…

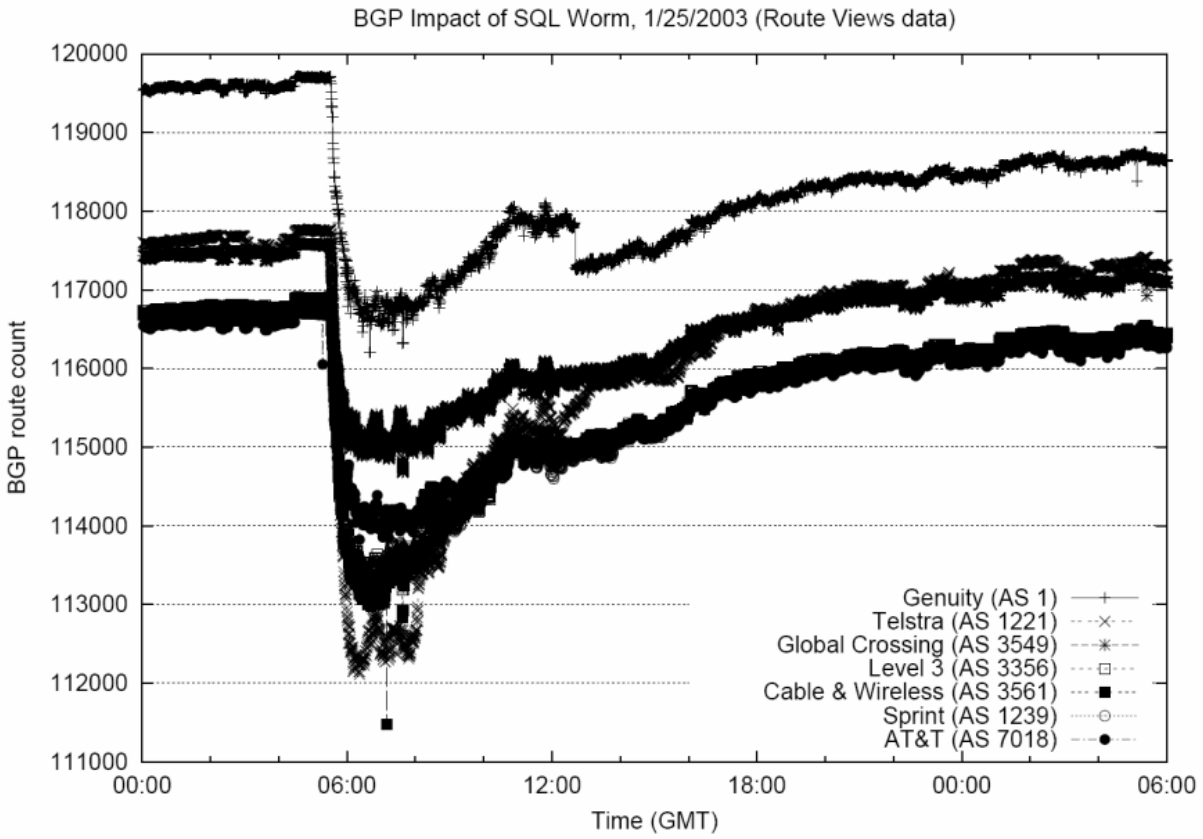
SONY

make.believe

TARGET

Florida Institute of Technology
Harris Institute for Assured Information

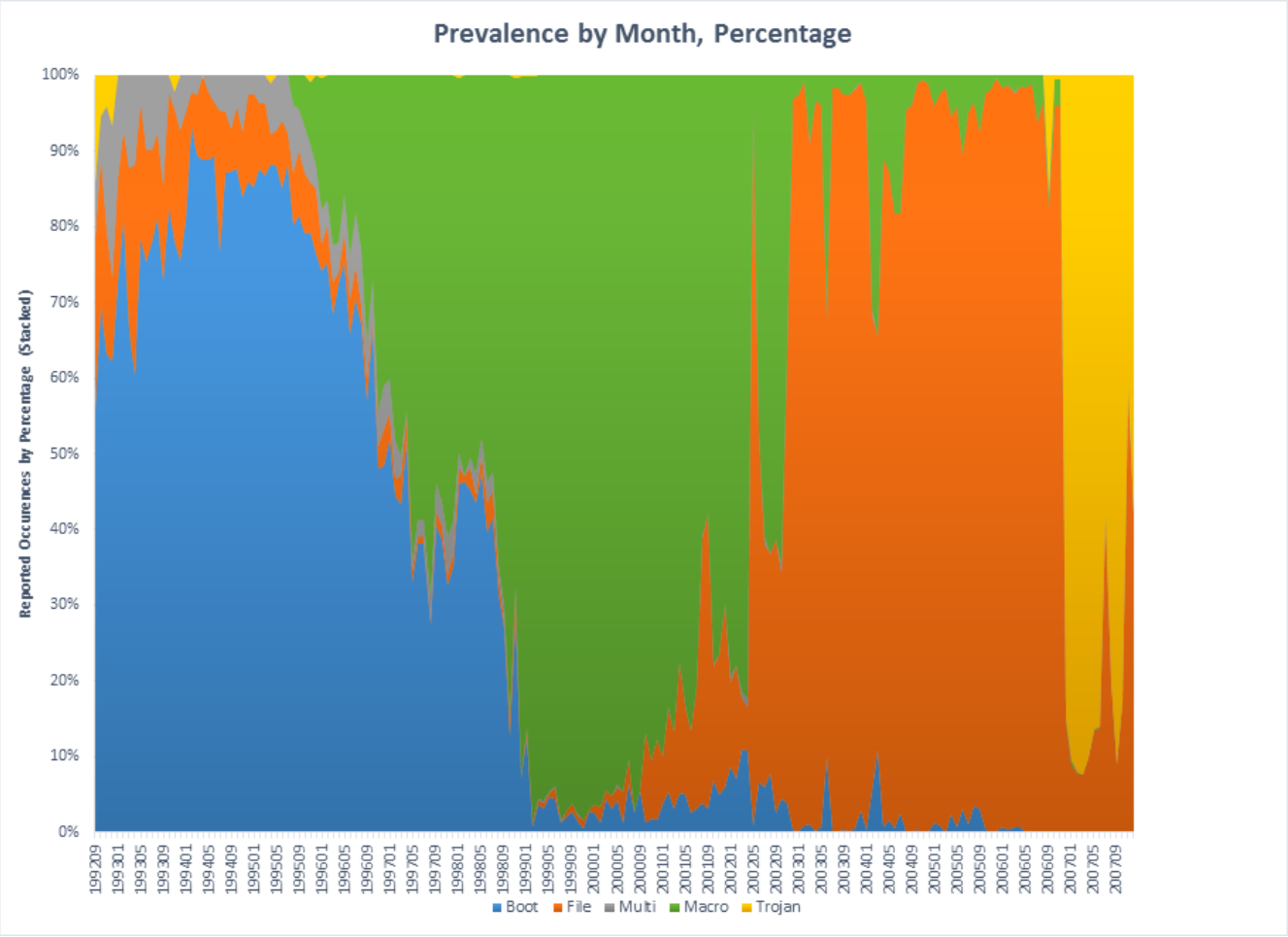
And this is actually the scary one…



Source: Griffen and Mao "Interdomain Routing Streams"

Florida Institute of Technology
Harris Institute for Assured Information

And this isn't too good either….



Florida Institute of Technology
Harris Institute for Assured Information

Today

- We lose billions in IP due to theft of data
- There can be no question we're losing the cyber security battle
  - Have you ever met someone who *hasn't* been a victim of attempted cybercrime?
- The ideas of "virtual" and "real world" are becoming very blurred
- Technology is moving so fast – the video phone kind of snuck up on us, right?
- And as if this wasn't bad enough, we have a crisis shortage of trained US personnel

Florida Institute of Technology
Harris Institute for Assured Information

One Question: Why?

- Why? Why, despite record spending on Cybersecurity, are things in such a mess
  - And for the record, I was nice about the state, based on where I'm speaking today
- Is the sky falling? Is the sky *capable* of falling?
- What is the science behind insecurity?
- What is the *politics* that drives insecurity?

Florida Institute of Technology
Harris Institute for Assured Information

How Did We Get Here?

- The revolution we're in right now is so big we can't see it
- Like all massive social changes, the implications aren't obvious
- Quick history lesson: the Industrial Revolution… what can we learn from this?

Impact of The Industrial Revolution

- Unintended consequences:
  - The triumph of the middle class over nobility in the UK
  - The creation of the Luddites and the urbanization of the cities
  - Child labor (you don't need strength to operate a machine…)
  - New diseases (like the oh-so-unpleasant "phossy jaw") arise, and old ones (TB, Typhoid, Cholera) increase
  - The rise of "trade unions"
  - Population growth
- Not all of the changes were bad (far from it) *but the consequences were unpredictable*

Florida Institute of Technology
Harris Institute for Assured Information

DIGITAL REVOLUTION

274 MILLION AMERICANS HAVE INTERNET ACCESS
MORE THAN DOUBLE THE NUMBER WITH INTERNET ACCESS IN 2000

81 BILLION MINUTES SPENT ON SOCIAL NETWORKS/BLOGS

64% OF MOBILE PHONE TIME IS SPENT ON APPS

42% OF TABLET OWNERS USE THEM DAILY WHILE WATCHING TV

NUMBER OF LAPTOPS SURPASSES DESKTOPS WITHIN TV HOMES

THE LAST 10 YEARS

SOCIAL NETWORKS/BLOGS BECOME TOP ONLINE DESTINATION
Accounted for 9.2% of Internet time.
Passed former top category, Email.

Americans averaged 1 hour, 50 minutes watching video online
11 million Americans watched video on their mobile phones

NEARLY 30 MILLION AMERICANS ACCESSED THE MOBILE WEB

3.2% OF MOBILE SUBSCRIBERS OWNED A SMARTPHONE

DEBUT OF BLU-RAY
Discs offer increased storage capacity, high definition video and audio

6.6 BILLION MINUTES SPENT ON MEMBER COMMUNITY SITES
(NOW KNOWN AS SOCIAL NETWORKS/BLOGS)
Top Member Community was MSN Spaces (2 million unique U.S. visitors)

DVD OVERTAKES VHS AS PREDOMINANT HOME VIDEO FORMAT
DVD represented 2/3 of all units sold

132.2 MILLION AMERICANS HAD INTERNET ACCESS

Source: Nielsen

Now, back to our time

- The Internet has changed our lives in ways we don't see
- Pervasive connectivity
  - Working at 1100p from the couch… what are the implications?
- Porous boundaries on the company
- Access to information has changed our *brains*
  - Very good argument that the kids I teach now simply *cannot* carry out certain tasks well because of the way their brains have been impacted by "always on" connectivity

Florida Institute of Technology
Harris Institute for Assured Information

With this as a backdrop…

- The Science
  - Computers are Turing Machines
  - Computers have no context when processing
  - Complexity
- The Politics
  - We lack the desire to address the problem
  - Geopolitical Pressures
  - People are People and the philosophical pull of general purpose computing

Turing Machines

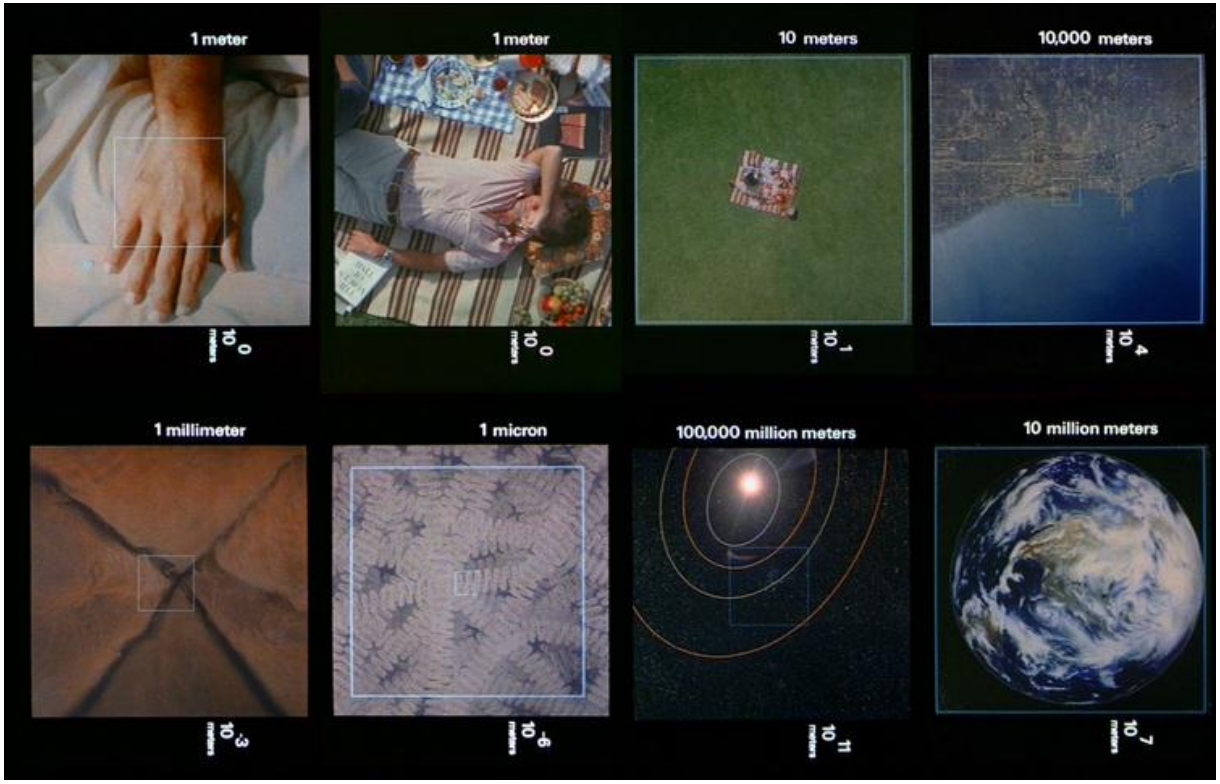
- *"Part of the inhumanity of the computer is that, once it is competently programmed and working smoothly, it is completely honest."* – Isaac Asimov

How does this relate?

- Most of the computers we use every day can be modeled by (or, to pretend I'm a scientist, are Isomorphic to) a Turing Machine
- Turing Machines execute a calculus – a mathematical function
- A Turing Machine has NO WAY of detecting changes to its tape, and there is no way to recover from an error
- The very nature of computing means that it is brittle with respect to an attack
  - There are lots of examples of other computing paradigms, but they are not really mainstream

Context

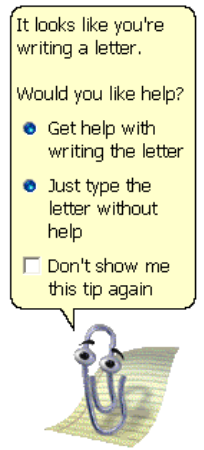
- *"il n'y a pas de hors-texte"* – Jacques Derrida



Florida Institute of Technology
Harris Institute for Assured Information

Computers seldom (never?) have context

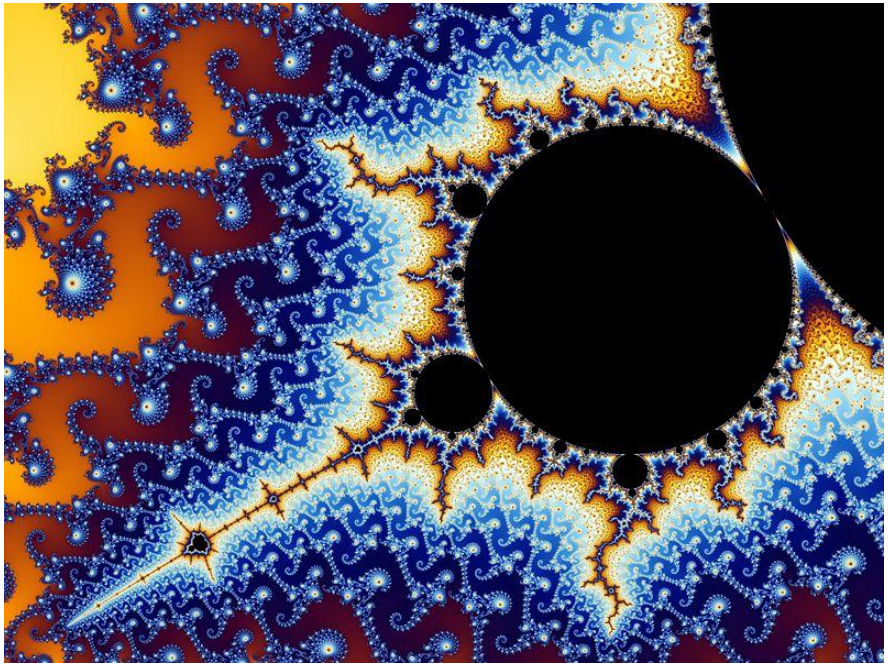
- We have our model of computation from our Turing Machine
- But our minds are wonderful, because we can engage in meta-cognition
- Example: Spreadsheet with 10.000.00 instead of 10,000.00
- Our examples of context are painful…
- The challenge is that this is a VERY hard problem
  - Remember the whole Turing Machine thing?



Florida Institute of Technology
Harris Institute for Assured Information

Complexity

- *"Simplicity is a great virtue but it requires hard work to achieve it and education to appreciate it. And to make matters worse: complexity sells better."* – E.W. Dijkstra



Florida Institute of Technology
Harris Institute for Assured Information

Complexity

- We ignore (at our peril) the incredible complexity of computing
  - Ivy Bridge is up around 1.40 ***BILLION*** transistors
  - So complex, we cannot exhaustively test it (not even close)
- Furthermore, nature loves complexity… and in that complexity we get to play our games as an attacker
- When we view our systems through the lens of complexity, their weaknesses become obvious

All Complex Systems have Parasites

- Talk by Cory Doctorow – very well given with a lot of insight
- Doctorow says:
  - You could stop spam by simplifying email: centralize functions like identity verification, limit the number of authorized mail agents and refuse service to unauthorized agents, even set up tollbooths where small sums of money are collected for every email, ensuring that sending ten million messages was too expensive to contemplate without a damned high expectation of return on investment. If you did all these things, you'd solve spam.

    By breaking email.

    Small server processes that mail a logfile to five sysadmins every hour just in case would be prohibitively expensive. Convincing the soviet that your bulk-mailer was only useful to legit mailing lists and not spammers could take months, and there's no guarantee that it would get their stamp of approval at all. With verified identity, the NYTimes couldn't impersonate you when it forwarded stories on your behalf -- and Chinese dissidents couldn't send out their samizdata via disposable gmail accounts.

    An email system that can be controlled is an email system without complexity. Complex ecosystems are influenced, not controlled.

Florida Institute of Technology
Harris Institute for Assured Information

The Politics: No Desire!

- Solving the insecurity issues won't be cheap, and will require a *fundamental* redesign of our view of computing
- There's no appetite among any group of politicians for this unpleasant business, and it partly goes back to human nature…
  - Short term v. Long term, Risk v. Reward
- No feedback about weaknesses/errors until much later – if at all
- Put off problems until later

Florida Institute of Technology
Harris Institute for Assured Information

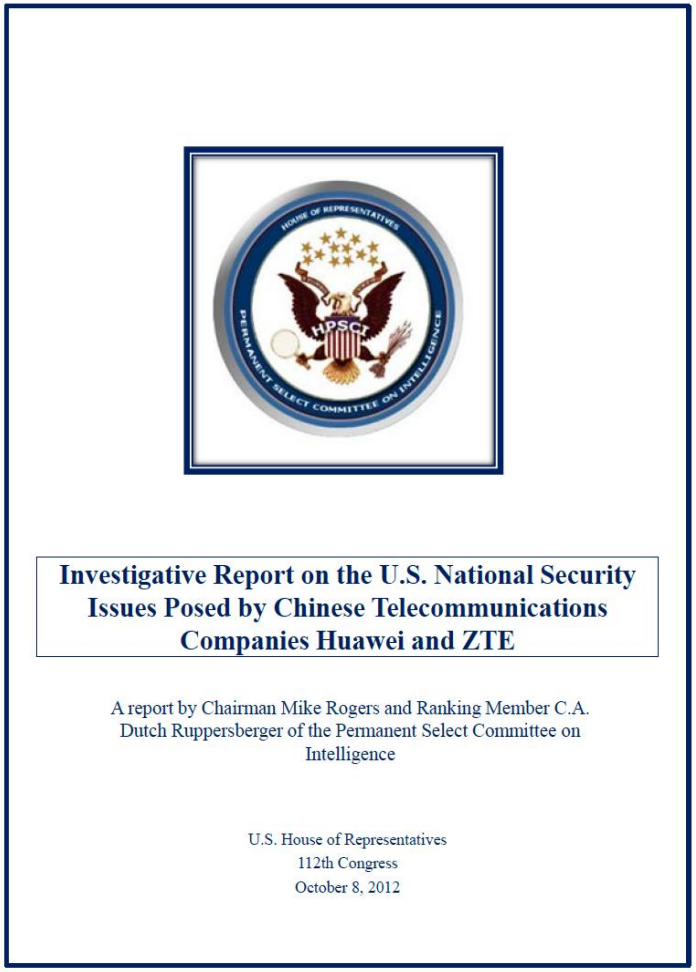
Can We *Legislate* The problem away?

- Probably not…
- We have to have realistic views of our laws – let's look at history
- First Road Traffic Act
- A more modern example: SOPA
  - We laugh at the "Red Flag" law when we hear about it… but that's where we're at now
  - Conflate two issues: copyright and legislation

Florida Institute of Technology
Harris Institute for Assured Information

Geopolitics & Asymmetry

- Quoting the report:
  - The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.
  - Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services.



Florida Institute of Technology
Harris Institute for Assured Information

The Geopolitical makes things hard

- Diplomacy is a Good Thing, but it makes management of security-related things very hard
  - Multiple and complex tensions that pull us in seemingly strange directions; the answers are *way* above my pay grade
  - In the Huawei case, the answer is very complex; it's not like we can build many of these artifacts ourselves… and it's not like we don't do this kind of thing to others…
- New media requires new paradigms
  - Google Image Redaction/Censorship problem
  - ITAR applied to algorithms
- Once again, this speaks to the "long game"

Florida Institute of Technology
Harris Institute for Assured Information

Human Nature

- *"Two things are infinite: the universe and human stupidity; and I'm not sure about the universe."* – Albert Einstein

We Want it All (and we want it now!)

- There is a drive for us to want everything to be "right"
  - Look at the philosophical arguments for "general purpose" computing, when many are better served by something more limited
  - We can have security but instead we want Java™
- The nature of a human is to be asymmetric with respect to risk – many experiments demonstrate this
  - Solutions need to understand the *person*: example from smoking campaigns
- At some level, people think we just need to "do things better" – this ignores the attacker in the equation

Florida Institute of Technology
Harris Institute for Assured Information

Who attacks us?

- Well, mostly, us
  - Also known as the "insider threat"
  - Yes, hackers may steal your data… but perhaps the most likely person to really get at it is someone who works for you
  - Good statistics are hard to come by, but we often spend so much time looking outward that we forget to look inward
- This is a hard problem
  - We want workplaces that are fun, efficient, safe and secure, and that is a tough balance
  - Perhaps the biggest takeaway is don't be so busy looking outward that you forget to look in

How the Attacker Thinks

- First, remember the attacker doesn't play by the same rules as you…
  - What's the shortest distance between two points?
  - We play by what we think the rules are; the attacker plays by the *actual* rules
- Attackers will come at your sideways
  - Often not through your firewall, but through your phone
  - "Social engineering" involves getting your target to compromise himself by basically asking them… you just pick up the phone

What the Attacker Wants…

- … isn't always obvious
- I had a friend carry out a penetration test on a bank: his mission, break in!
- He discovered that each individual account was pretty well protected
  - Three tries with an invalid PIN and he was locked out
  - But he could get into random accounts quite easily: try the two most common PINs on every account number and voila… sooner or later he was through the first layer of security
  - The lesson: the bank focused on protecting each account one at a time… not defending all accounts from attack
  - The moral: see your system as it is, not how you use it lest you leave it vulnerable

We Have to Use Common Sense

- Alas, it's not exciting, and it's certainly not rocket science
- Security is about seeing your system as it is
- Security is about seeing the big picture *and* the details
- Security is about doing the simple things reliably, every time (patches, firewalls…)
- Security is not going to get better – we need to encourage people to enter the discipline and contribute
- The insecurity of one person can impact us all...

Florida Institute of Technology
Harris Institute for Assured Information

Security and Contract Management

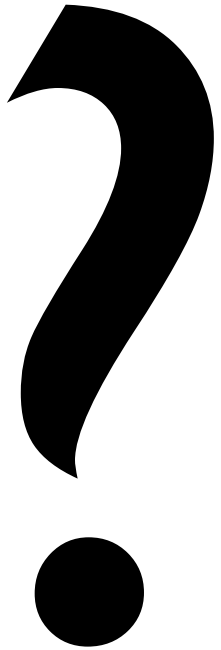
- First, most large contracts talk about security, and it's critical you understand that *security is not about risk removal, it is about risk mitigation*
  - BEST PRACTICE is your friend (although defining best practice is another matter altogether)
- Second, there are rapid technology changes that may make your past knowledge actively harmful to evaluating an opportunity and/or risk
  - Cloud based issues are complicated and change the game a bit
  - Data redaction (anonymization) *always* goes wrong
  - PII is a nightmare to handle and is a lawsuit just waiting to happen

Florida Institute of Technology
Harris Institute for Assured Information

Security matters at ALL phases

- The number one mistake I see at a business level in security is thinking that this is a "bolt on"
  - NEVER leave security to the end or add it on as an afterthought
  - This is a disaster, and can add millions (or billions) to the cost of a deliverable (I have stories… I kid you not)
  - Just like a heading correction when flying a plane, 5 degrees error is EASY to correct at departure, and a massive error after 2 hours in flight…

Questions



Florida Institute of Technology
Harris Institute for Assured Information