Cybersecurity:
How did we get here and
How do we get out of here?

University of Maryland
CyberCenter Symposium
May 16, 2012

Carl Landwehr
Carl.Landwehr@gmail.com
www.landwehr.org

0. Where are we, in computing and communications?

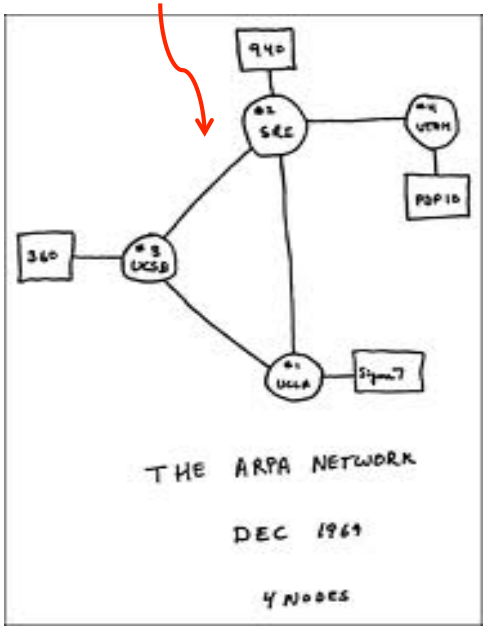
1969: IBM 360/67:	2009: iPhone 3GS:
2 CPUs	CPU + GPU
16MB RAM	256MB DRAM
4MB paging drum	64KB L1 Cache / 256KB L2 cache
230 MB per 8 2314 drives	32GB Flash memory
Occupies entire basement	Fits in pocket
Serves entire campus	2 Cameras and makes phone calls
Costs $M's	Cost $Hs

It's an amazing network out there

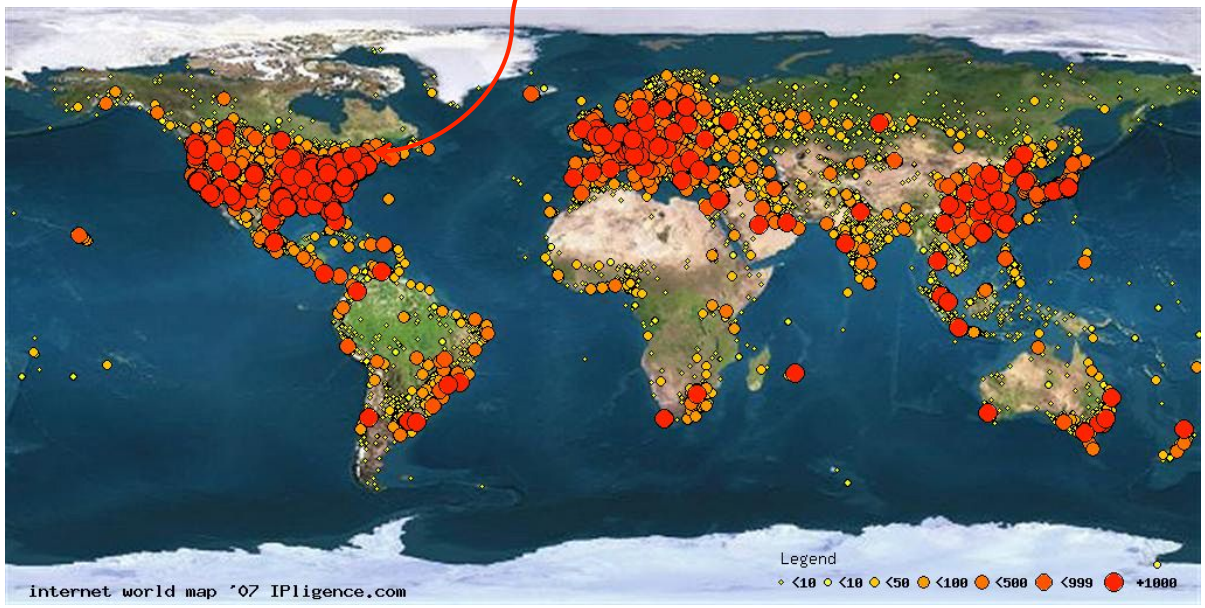
1969

2009

50KB/sec backbone



10 GB/sec backbone



1. Where are we in cybersecurity and privacy?

WSJ 9/27/2011

"Users are the biggest risk"

Should we count on every employee to lock the front door on the way out?

Leadership: Information Security

THE JOURNAL REPORT

THE WALL STREET JOURNAL. Monday, September 26, 2011 R1

What's a Company's Biggest Security Risk? YOU.

Opening an unexpected email attachment from a colleague
HOW YOU SEE IT
Being a good co-worker
HOW HACKERS SEE IT
An opportunity to inject a virus inside the corporate network, bypassing the firewall

Bringing a new personal gadget to the work network
HOW YOU SEE IT
An opportunity to keep up with the latest technology
HOW HACKERS SEE IT
A new route for viruses and spyware to make their way into corporate systems

Posting job details on LinkedIn
HOW YOU SEE IT
Creating a professional presence and finding another potential job
HOW HACKERS SEE IT
Reconnaissance data to map out company hierarchies and target specific users with spear-phishing attacks

Using personal Web email for work
HOW YOU SEE IT
Making it easier to work from home or to move files between computers
HOW HACKERS SEE IT
A path to access critical data from relatively unprotected services

EMPLOYEES DON'T MEAN TO BE THE PRIMARY ENTRY POINT FOR HACKERS. BUT THEY ARE.

BY GEOFFREY A. FOWLER

ILLUSTRATION BY BRIAN STAUFFER

We are the weakest link.

Hacking attacks against companies are growing bigger and bolder—witness a string of high-profile breaches this year at Sony Corp., Citigroup Inc. and others. But gone are the days when hackers would simply find holes in corporate networks to steal valuable data. Large companies have grown wise to the threat of hacking, and have spent the past 30 years hardening the perimeters of their networks with upgraded technology.

These days, criminals aren't just hacking networks. They're hacking us, the employees.

"The security gap is end users," says Kevin Mandia, chief executive of security firm Mandiant Corp. The majority of corporate security breaches his firm is currently investigating involve hackers who gained access to company networks by exploiting well-intentioned employees.

Consider what happened in March at EMC Corp.'s RSA security unit, the maker of computer login devices used by thousands of other companies. A hacker sent emails to two small groups of employees that looked innocent enough, including a spreadsheet titled "2011 Recruitment plan." The message was so convincing that one employee retrieved it from the "junk mail" folder and then opened the attachment. Doing so introduced a virus inside RSA's network that eventually gave the hacker access to sensitive company data and enabled later attacks against RSA's customers.

Employees have more opportunities than ever to compromise company information. We not only screw up by clicking on emails from hackers that download viruses, letting them bypass corporate firewalls. We also open a Pandora's Box of security problems by circumventing company tech-support rules and doing work with personal gadgets and consumer-grade online services like Web email and cloud storage services.

Closing these holes is proving very difficult, security experts say. But companies that employee habits, they're testing new tools to keep track of what's happening on their networks and rolling out employee education programs.

Here's a look at what employees are doing wrong and how companies are trying to fight our bad habits.

We Help Hackers Target Us

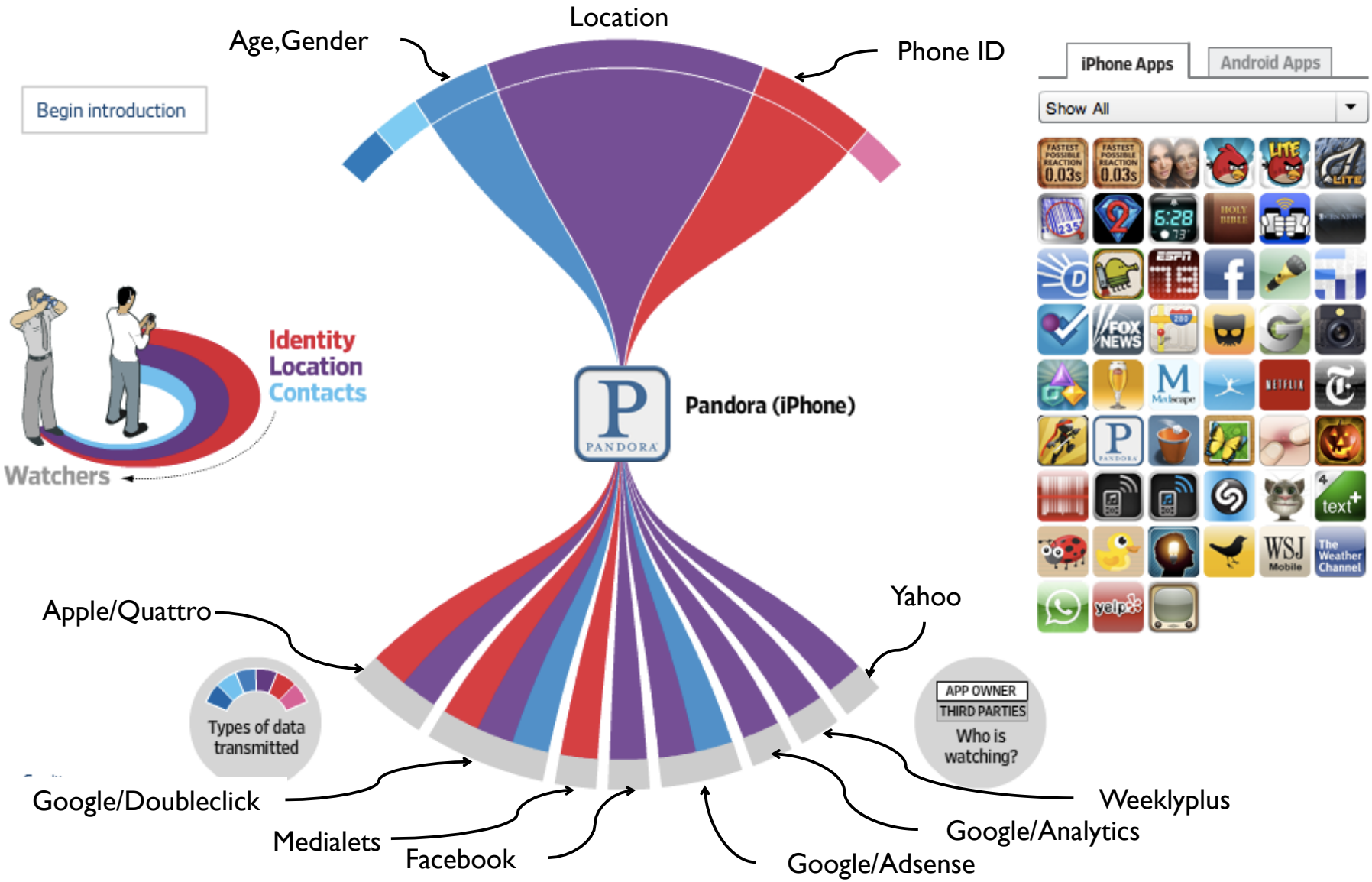
Spies, fraudsters and confidence men have long engaged in what's called social engineering to manipulate people into divulging confidential information, often after completing thorough reconnaissance on their victims. Now those tricks have been adapted for the Internet era.

Today, we make ourselves easy targets by posting troves of information about ourselves and our jobs online, say security experts. Blogs and professional networks such as LinkedIn are particularly useful sources for criminals, since many people share details about their roles at work, which can be used to help determine corporate hierarchies, among other things. That makes it easy for a hacker to whip up, for example,

Please turn to page R4

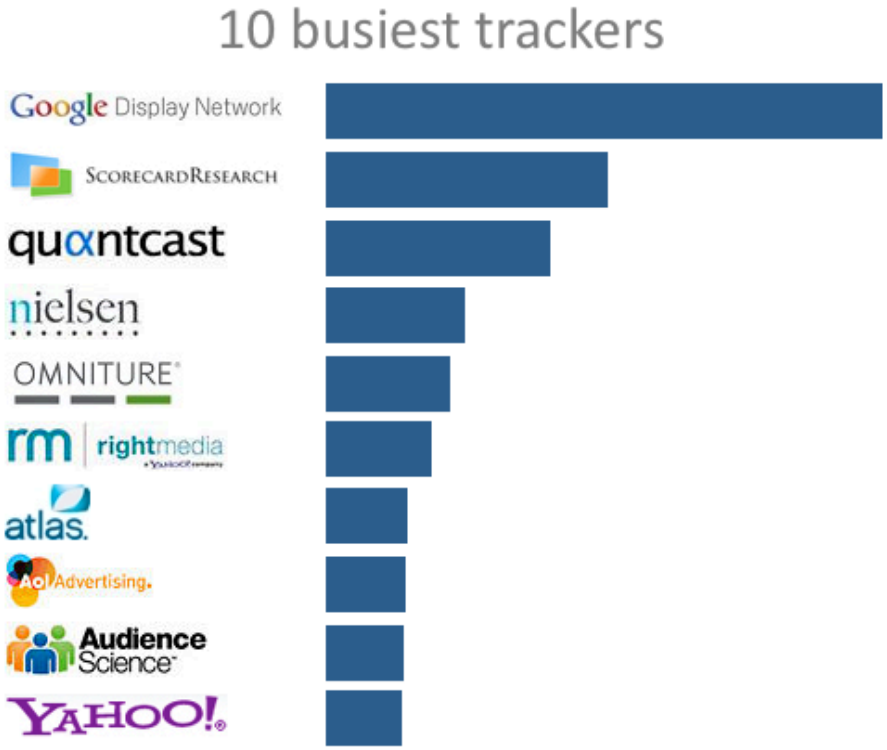
Privacy - mobile

Wall Street Journal
"What They Know" series
http://blogs.wsj.com/wtk-mobile

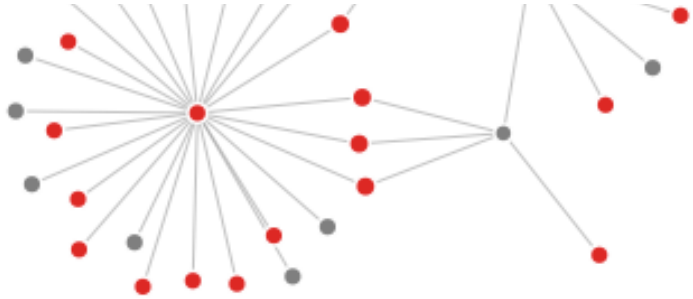


Browsing Privacy (?)

- New add-on to Firefox: Collusion (collusion.toolness.org)
- Visualizes web browsing tracking
- Results shown at right represent a few minutes of browsing, accessing Amazon, Tripadvisor, Netflix, Gmail
- Red dot means confirmed tracking site (by PrivacyChoice.org); gray dot means unconfirmed. Size of dot may reflect number of sites tracked
- Meaning of arcs not explained
- Mouse over dot to see who it is and what they are tracking

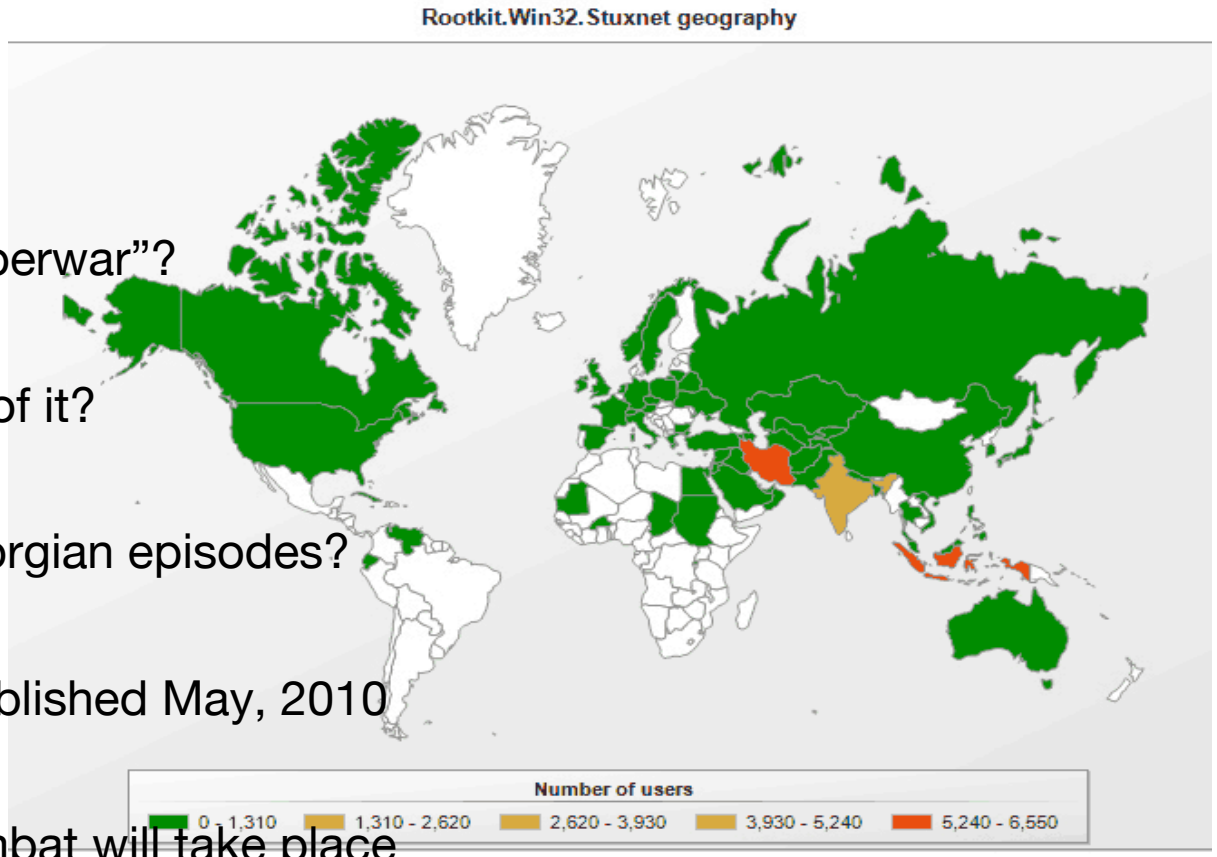


These trackers are the most prevalent on sites visited by our panel



Cyberwar?

- What do we mean by “cyberwar”?
- Was Stuxnet an instance of it?
- What about Estonian, Georgian episodes?
- US Cyber Command established May, 2010
- Seems unlikely future combat will take place without some consideration and use of cyberattacks
- Many unresolved issues including attribution, policy (e.g. rules of engagement), collateral damage, first use, ….



OK, but those are anecdotes.
How can we measure where we are?

Where are we in cybersecurity? Possible coordinates

- Threat: how likely are attacks to occur?
- Vulnerability: how weak are our systems?
- Cost: how much are attacks costing us?

Where are we headed: are things getting better or worse? (a vector in this 3-space?)

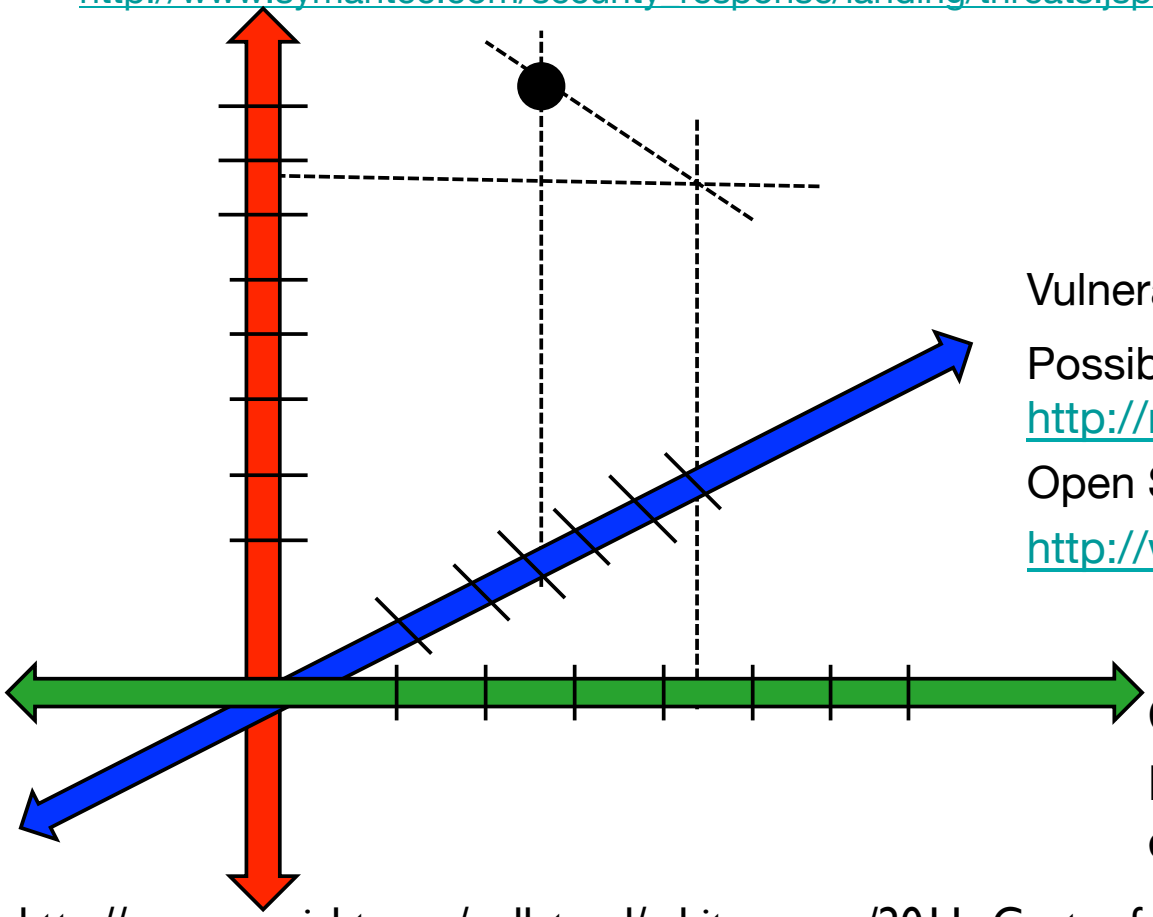
What can we observe?

Threat (# attacks/t ?)

Possible sources: Symantec Internet Security Threat Reports

(but note "a threat is an application with the potential to cause harm to a system…)

http://www.symantec.com/security_response/landing/threats.jsp



Are these axes orthogonal?

Vulnerability (# holes/t ?)

Possible sources: NIST NVDB, http://nvd.nist.gov

Open Source VDB

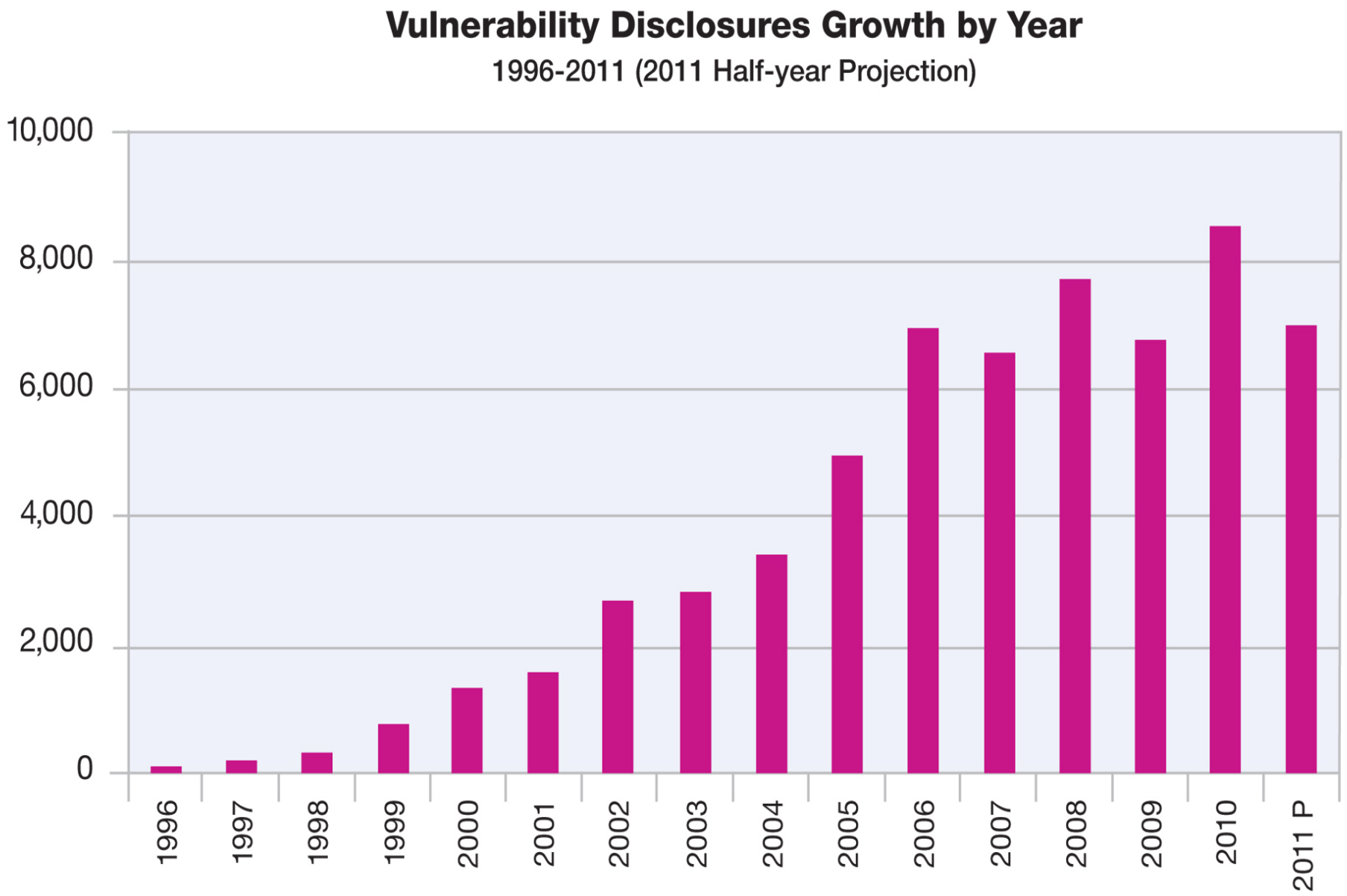
http://www.osvdb.org/

Cost ($ or $/t) (Whose cost?)

Possible sources: Surveys, e.g., Poneman Inst. Report

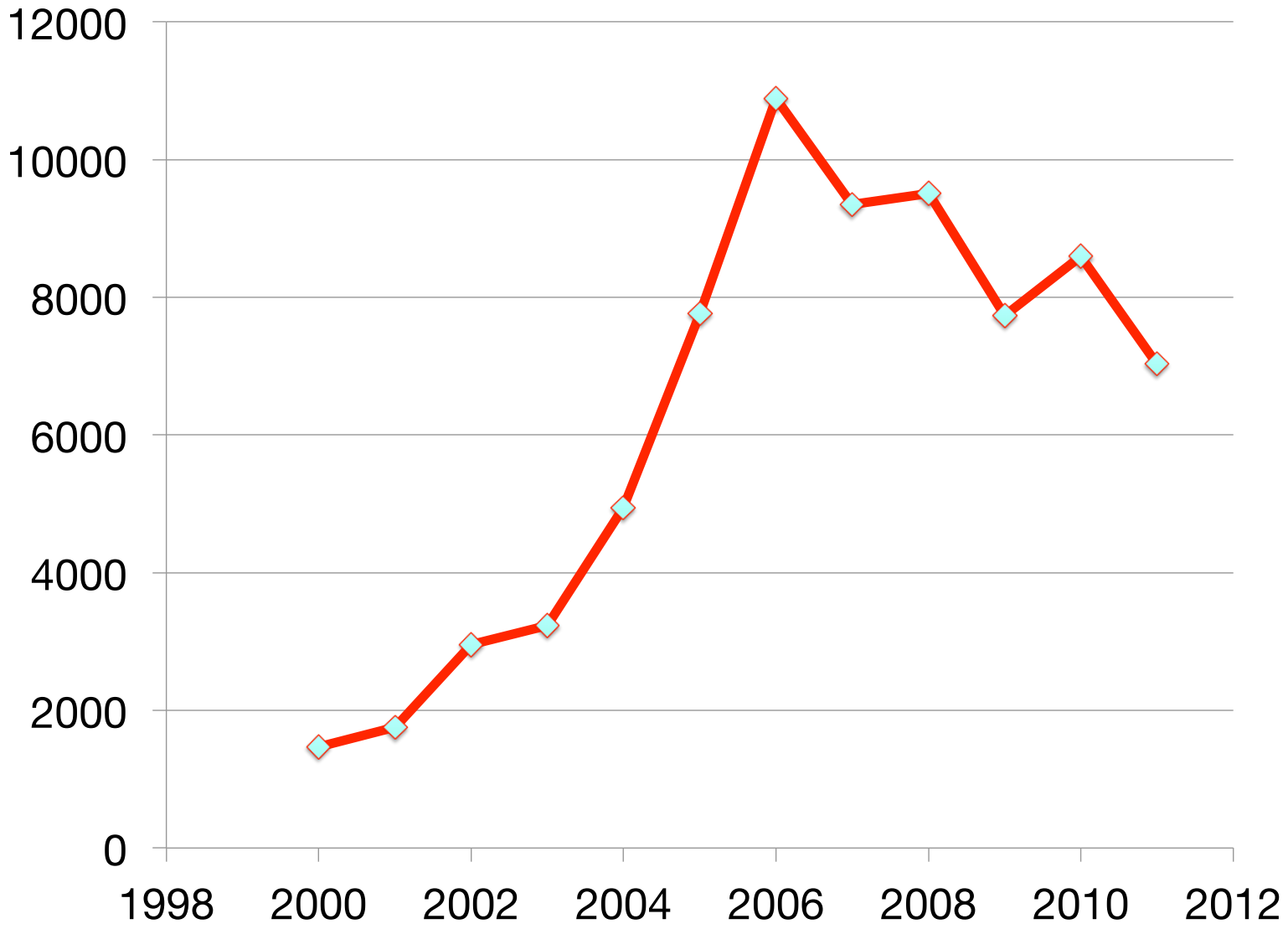
http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

But beware of survey bias



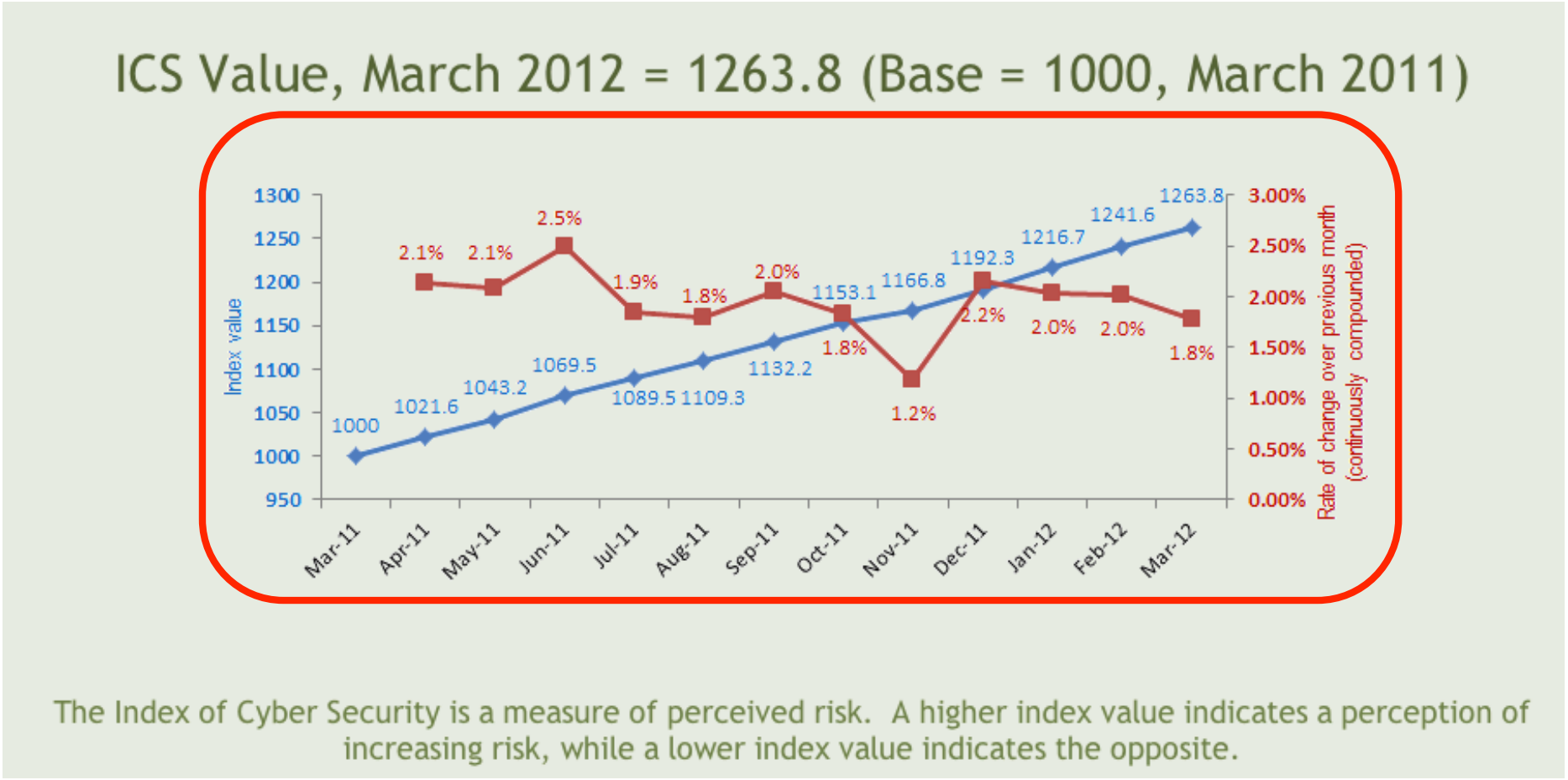
Source: IBM X-Force mid-year report, August, 2011

Open Source Vulnerability Database # Disclosures by year



Where are we headed?

Are things getting better or worse?

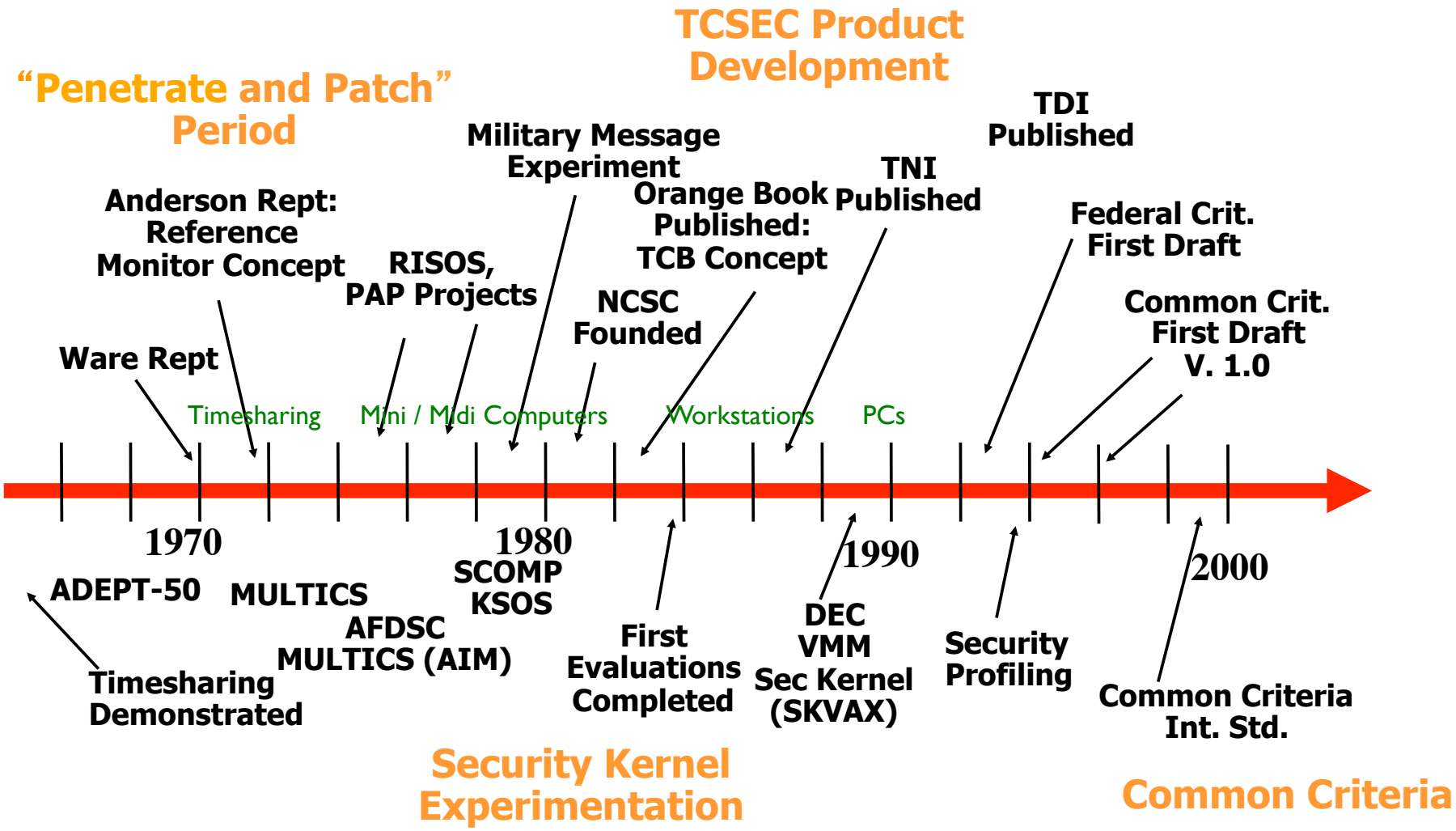


The Index of Cyber Security is a measure of perceived risk. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

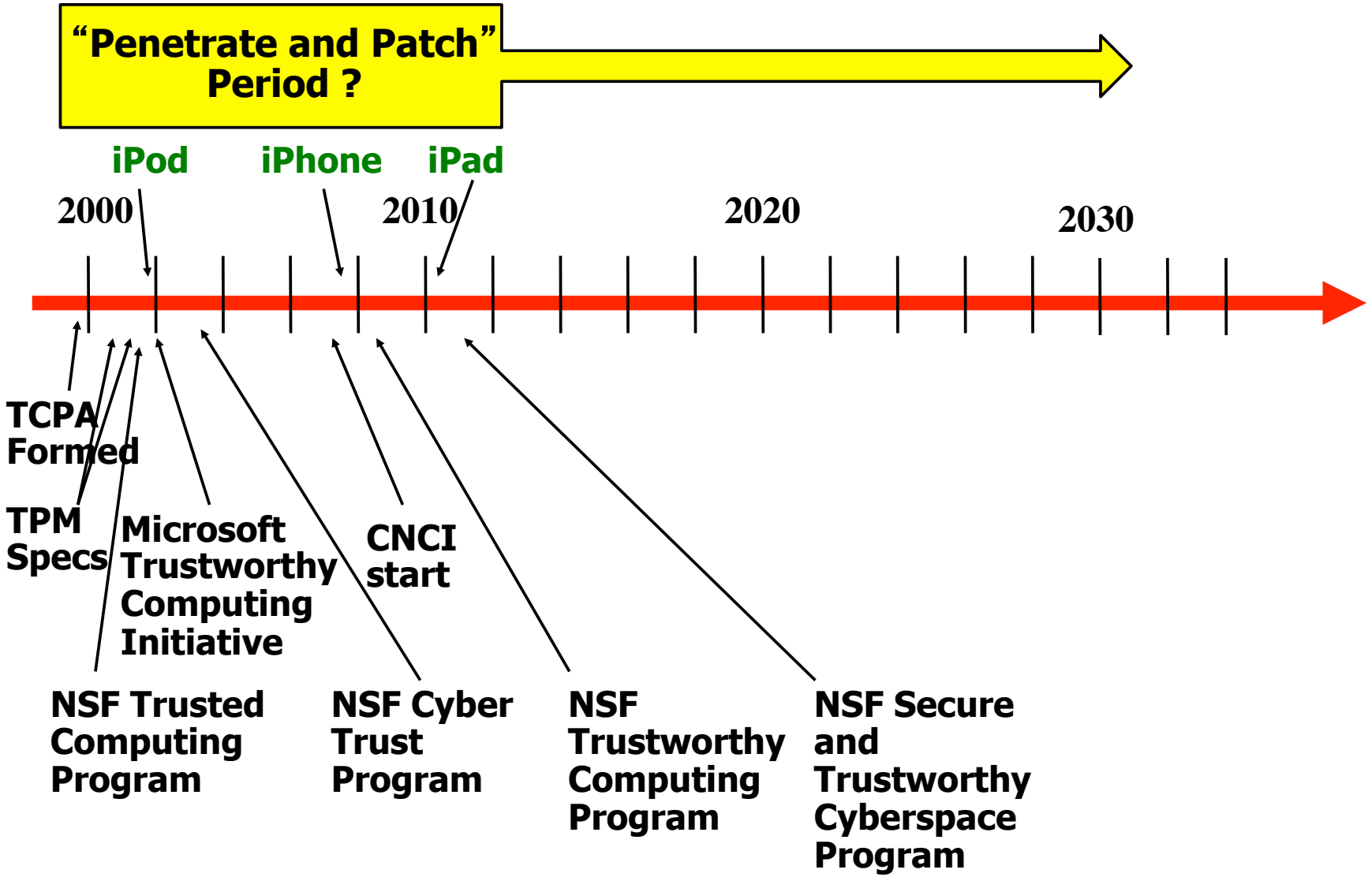
- Dan Geer, Mukul Pareek, developed and implemented sentiment-based index (ref. Consumer Confidence Index), based on 100 selected responders, higher number means more risk
- Reported monthly since March 2011 base 1000; currently 1241
- Plans to develop a “Cyber Security Prediction Market”

2. So how did we get into this state?

20th Century Computer Security: What Did We Do?



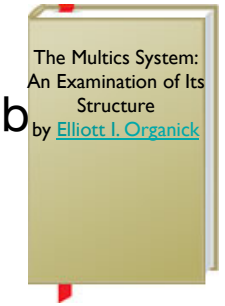
21st Century Cybersecurity – What's new?



20th Century: What did we learn?

Engineering lessons:

- Ways to think about access control: reference monitor, TCB
- Understanding/controlling information flow is key
- Covert (side) channels can't be ignored
- Fine-grained access controls can be implemented (capabilities) but people may not want to manage them
- Engineering principles for system security (MULTICS)
- People will click on any dialog box that gets in the way of doing the job
- Detecting intrusions is important but hard



Fundamental technology:

- Protocols for public key agreement (Diffie-Hellman)
- How to do public key (asymmetric) cryptography (RSA)
- What it means to prove programs or protocols "correct" (and how hard it can be, and how machines may assist)

Market lessons:

- It's really hard to persuade industry to adopt technologies we developed
- You can sell security more easily if it's a box or a token
- Or if it's invisible
- Getting security into curricula is hard

Computer Security in the 21st Century: What are we learning?

The threat is real and growing

- Spam is a business
- Other threats are driven by other economic drivers
- Politics also influences threat

Some of the things we learned in the 20th c. are relevant

- Virtualization is useful
- Covert channels (aka side channels) are real
- Users will ignore irritating pop-ups

We are learning some new tricks

- Applications of advances in model checking
- Software defect finding
- Reverse engineering of binaries

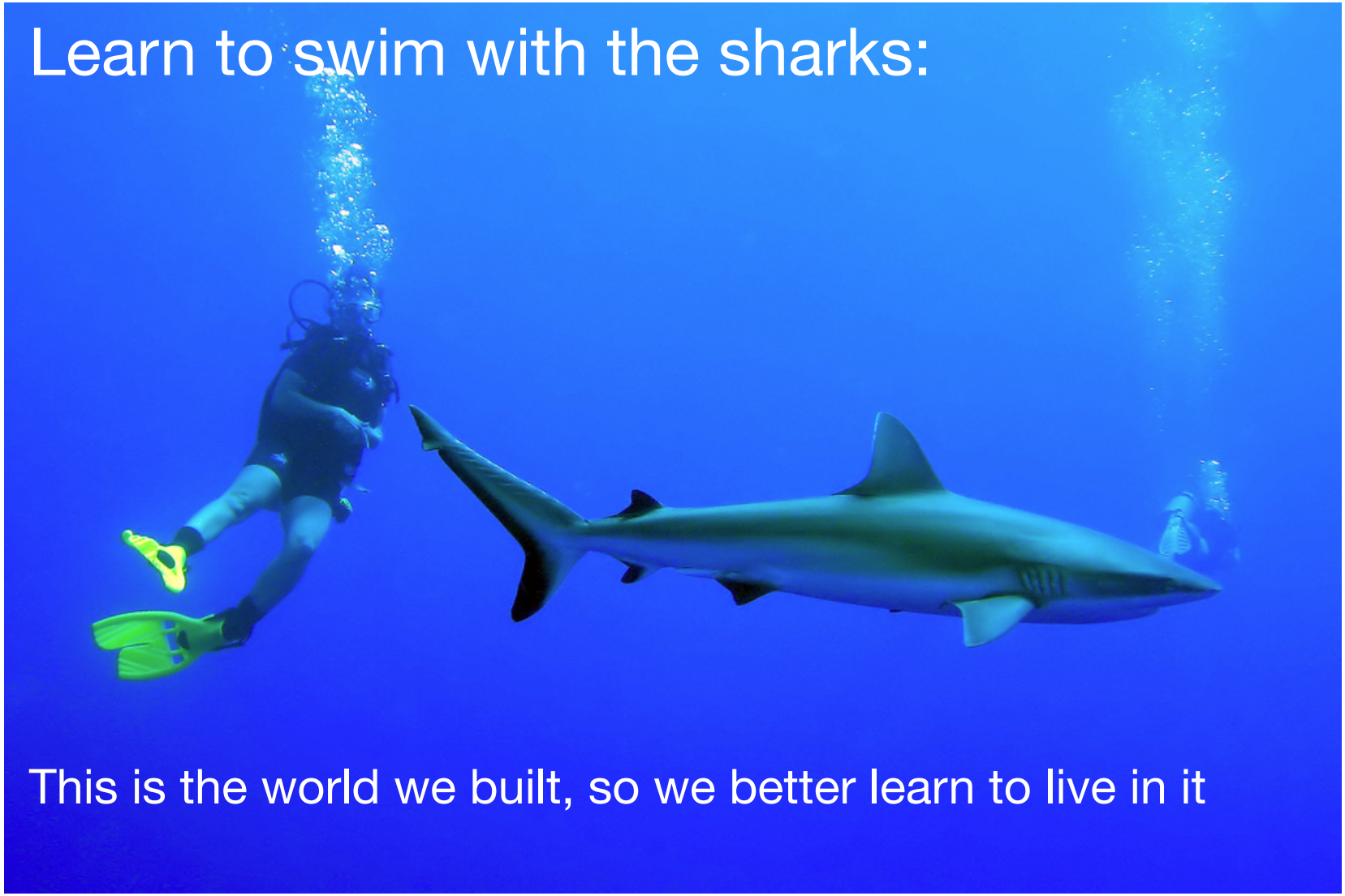
Monitoring is essential, but insufficient

Control systems, embedded systems makers need to understand and respond to the threats brought by interconnection of nearly everything

Cybersecurity is much more than a technical issue

3. Where are we headed?

4. What must we do?



Some research implications

Study monitoring and detection

- Embrace big data for understanding behavior

Study containment, intrusion tolerance, recovery, forensics

- Expect compromise and plan for it

Study means to make it harder for attackers

- Moving target, camouflage, deception

5. How do we get out of here?

What would it take to change the game?

Build a more seaworthy vessel

Research implications - 1

- Study sound, deployable construction methods
  - Safe, usable programming languages
  - Practical and sound composition methods
  - Information flow specification and control
- Study methods for detecting and removing flaws
  - Static and dynamic analysis
  - Binary rewriting
- Study methods to promote trustworthy operation
  - Configuration validation / monitoring
- Study what influences adoption / uptake

Research Implications - 2

Study the economics with the technology

Study the psychology/usability with the technology

Study the potential effects of regulatory strategies

Summary

1. Our basis for understanding our cybersecurity state at a national level, in terms of vulnerabilities, costs, and threats needs work.

2. We know quite a bit about how to engineer secure systems, and an increasing amount about how to find flaws in systems and reverse-engineer malware, but we know much less about how to get this technology used to build systems that are acceptable to users in terms of cost and convenience. We also lack scientific foundations for many of our engineering principles.

3. On the technical side, we should follow a two-pronged strategy: adapt to a world in which little technology is trustworthy and at the same time get more trustworthy systems in place.

4. In addition to studying the technology, we must study the context -- human, economic, regulatory -- if we want the technology to affect the real world.

Note: this list largely neglects privacy issues, except to the extent that insecure systems are unlikely to be able to assure privacy either.

Read!

Subscribe to
IEEE Security & Privacy at
www.computer.org/security

Request free printed copies of
The Next Wave from
Kathleen Prewitt, via e-mail to
TNW@tycho.ncsc.mil

What do you think would make a difference?

Thank you!

Carl Landwehr
Carl.Landwehr@gmail.com