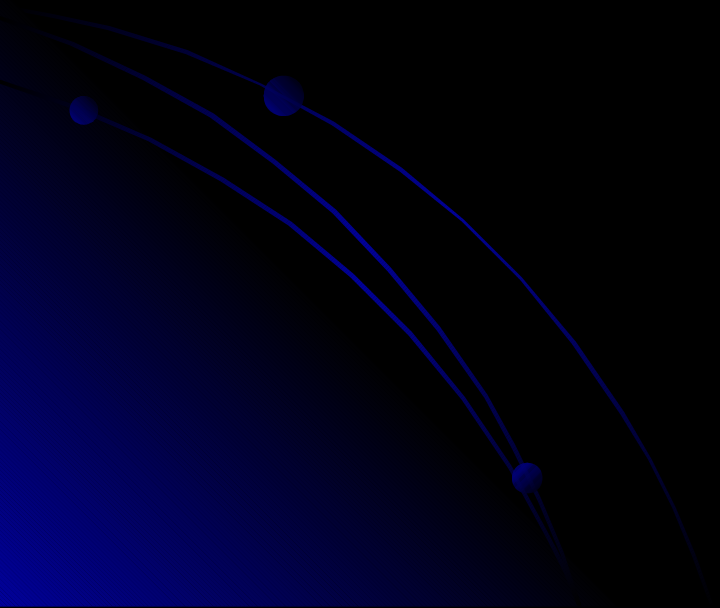
CEG 4420: Computer Security Last Lecture

Prabhaker Mateti

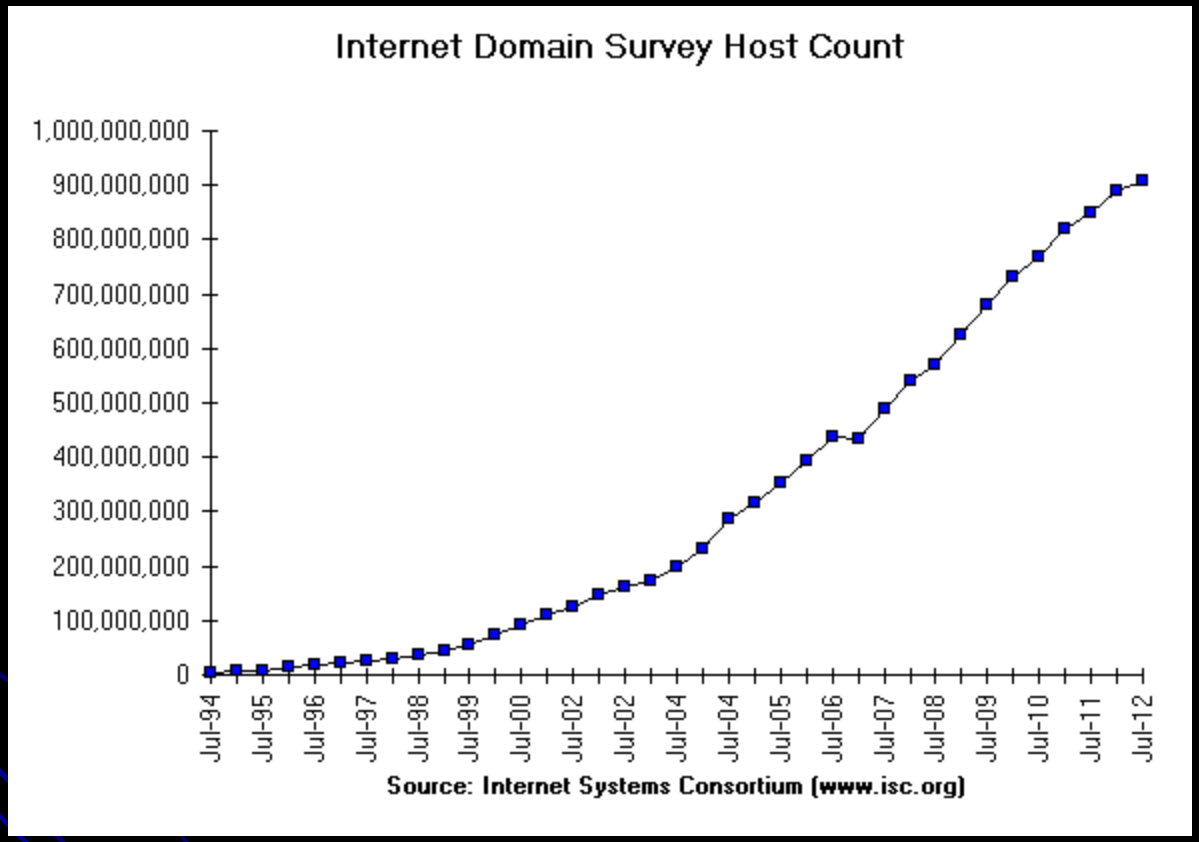
Internet Growth



Internet host count

1981	213
1986	5,089
1998	29,670,000
2000	93,047,785
2005	317,646,084
2010	768,913,036
2011	818,374,269

source: www.isc.org


Internet Domain Survey Host Count
1,000,000,000
900,000,000
800,000,000
700,000,000
600,000,000
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
0
Jul-94
Jul-95
Jul-96
Jul-97
Jul-98
Jul-99
Jul-00
Jul-02
Jul-02
Jul-04
Jul-04
Jul-05
Jul-06
Jul-07
Jul-08
Jul-09
Jul-10
Jul-11
Jul-12
Source: Internet Systems Consortium (www.isc.org)

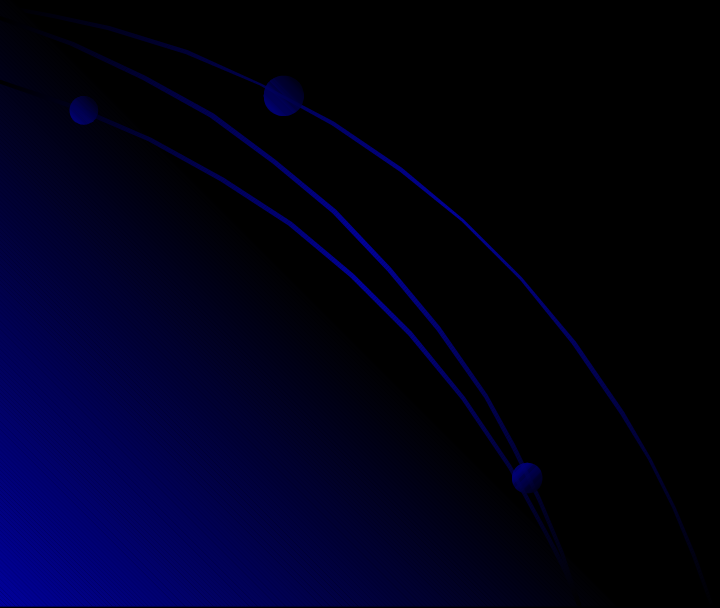
‘Computers’?

- Define `Computer’ System!
- Main frames
- PCs
- Smart Phones
- Embedded systems
- Usage without Internet?

Facts about data theft

- More than 12,000 laptops lost per week in US airports alone;
- One laptop is stolen every 53 seconds;
- Viruses cost US businesses $55 billion annually; and
- 25% of all PC users suffer from data loss each year.
- Source: http://www.technewsworld.com/ 01/20/2010

Top N Lists



Top Ten Web Sites in Security

1. www.cert.org/ US funded. Provides cyber alerts, defense and response to government agencies and industry partners.
2. www.infosyssec.org/ security portal with many tutorials.
3. www.phrack.org/ in-depth technical articles on exploits.
4. defcon.org/ Oldest and one of the largest hacker conventions.
5. www.securityfocus.com/ Hosts BUGTRAQ. white-hat site.
6. www.packetstormsecurity.org/ security portal. security tools and exploits.
7. www.schneier.com/ Security blog focused on crypto.
8. www.infowar.com/ takes a broader view of security and has articles about how countries can get affected.
9. www.undergroundnews.com/ "… does not restrict or censor"
10. www.microsoft.com/technet/security/default.mspx

Links to Others

- googleonlinesecurity.blogspot.com/2009/06/top-10-malware-sites.html
- www.techsupportalert.com/best_computer_security_sites.htm
- 20 useful IT **security Web sites**
- informationsecurityhq.com/10-top-websites-for-information-security/
- www.secureroot.com/topsites/

Top Internet Security Vulnerabilities

- Top Vulnerabilities in Windows Systems
  - W1. Windows Services
  - W2. Internet Explorer
  - W3. Windows Libraries
  - W4. Microsoft Office and Outlook Express
  - W5. Windows Configuration Weaknesses
- Top Vulnerabilities in Cross-Platform Applications
  - C1. Backup Software
  - C2. Anti-virus Software
  - C3. PHP-based Applications
  - C4. Database Software
  - C5. File Sharing Applications
  - C6. DNS Software
  - C7. Media Players
  - C8. Instant Messaging Applications
  - C9. Mozilla and Firefox Browsers
  - C10. Other Cross-platform Applications
- Top Vulnerabilities in UNIX Systems
  - U1. UNIX Configuration Weaknesses
  - U2. Mac OS X
- Top Vulnerabilities in Networking Products
  - N1. Cisco IOS and non-IOS Products
  - N2. Juniper, CheckPoint and Symantec Products
  - N3. Cisco Devices Configuration Weaknesses
- Source: http://www.sans.org/top20/

Top 125 Security Tools, 2012

- Sectools.org
- Each respondent could list up to 8.
- No votes for the Nmap Security Scanner were counted.
- The list is slightly biased toward "attack" tools rather than defensive ones.

Open Web Application Security

- not-for-profit worldwide charitable organization focused on improving the security of web application software.
- free and open software license.
- www.owasp.org/

Black/? Hat Sites/Conferences

- Suspend all judgments (other than technical quality).
- defcon.org/ annual conference in Las Vegas. Excellent presentations by “hackers”.
- blackhat.com/ Conferences and training!
- shmoocon.org/ “… refusal to take anything about the Internet seriously…”
- recon.cx/ reverse engineering. annually in Montreal

Top 25 Software Errors, 2010

1. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
2. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
3. Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
4. Cross-Site Request Forgery (CSRF)
5. Improper Authorization
6. Reliance on Untrusted Inputs in a Security Decision
7. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
8. Unrestricted Upload of File with Dangerous Type
9. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
10. Missing Encryption of Sensitive Data
11. Use of Hard-coded Credentials
12. Buffer Access with Incorrect Length Value
13. Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')
14. Improper Validation of Array Index
15. Improper Check for Unusual or Exceptional Conditions
16. Information Exposure Through an Error Message
17. Integer Overflow or Wraparound
18. Incorrect Calculation of Buffer Size
19. Missing Authentication for Critical Function
20. Download of Code Without Integrity Check
21. Incorrect Permission Assignment for Critical Resource
22. Allocation of Resources Without Limits or Throttling
23. URL Redirection to Untrusted Site ('Open Redirect')
24. Use of a Broken or Risky Cryptographic Algorithm
25. Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

- http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf

Recent (Last 5 Years) Attacks

Attacks on Sony

- Sony's PlayStation Network system was hacked, affecting more than 100 million online accounts worldwide and forcing the company to shut down the popular online gaming service. April 2011.
- Database at Sony Ericsson's Eshop, Canada breached. May 2011.
- Sony in Greece.
- Sony in Japan.
- Sued George Hotz, 21. Hacked the fully locked Sony PS3 console in 2010 to run homebrew applications and released the method through his website.
- Sony lawsuit demanded that social media sites including YouTube hand over IP addresses of people who visited Hotz's pages and videos.

Systems of US Congress

- The Senate's Sergeant at Arms reported last year that computer systems of Congress and executive branch agencies are probed or attacked
  - 1.8 billion times per month,
  - costing about $8 billion annually.

Cell Phone Malware

- More mobile phones than people in many countries.
- ZeuS botnet: Using infected HTML forms on the victim's browser, obtains cell number, sends a text message containing the new malware SymbOS/ Zitmo.A!tr designed to intercept and divert banking transactions. September 2010
- Jailbreaking w/ no knowledge of security
  - ssh Apple's default root password "alpine"

Cell Phone Malware

- Droid Dream Light, May 2011, Trojan
- invoked on receipt of android.intent.action.PHONE_STATE intent (e.g. an incoming voice call).
- contacts remote servers and supplies the IMEI, IMSI, Model, SDK Version and information about installed packages.
- capable of downloading and prompting installation of new packages

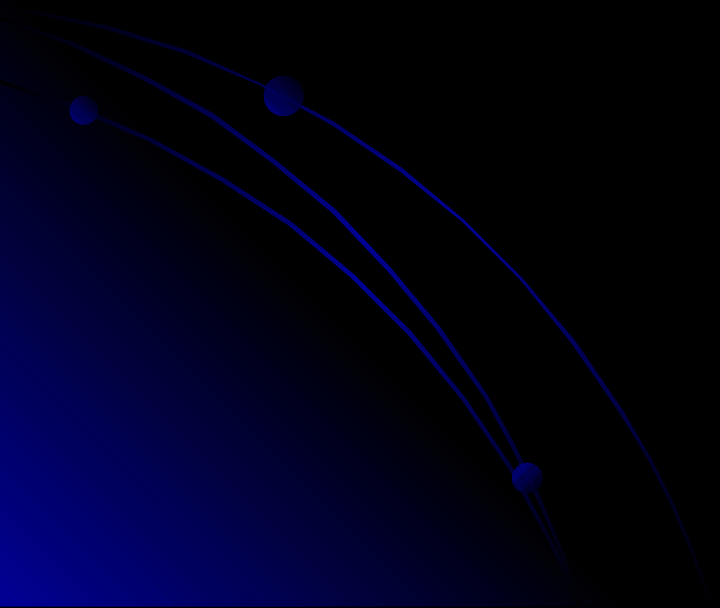
Estonia's infrastructure

- Baltic republic of Estonia
- first country in the world to experience cyber war.
- Government, financial and media computer networks were paralyzed by a series of attacks
- April 2007
- Estonia is a heavily wired country: 80 % of Estonians pay their taxes and do their banking on Internet.
- Decided to relocate a Soviet war memorial
- Russian hackers?
- Estonia instituting a real cyber army?

Stuxnet

- Worm targeted at a “unique” target in the world
- Target = A nuclear facility using specific equipment.
- Infects many, but does not hurt any, except one.
- Sohisticated internals
- Developed by country-level attackers?
- More details at http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Viruses/stuxnet-2011-pm.pptx

Controversies



Being Able to Read the Source

- Enables exploits
  - Reverse Engineering not required
  - Internal Structure is understood
  - Weaknesses can be seen at the design level
- Enables fast fixes
- Intellectual Property Rights and Privileges
  - Not (very) relevant in this course
  - Think: Why do we make laws that let patents expire?

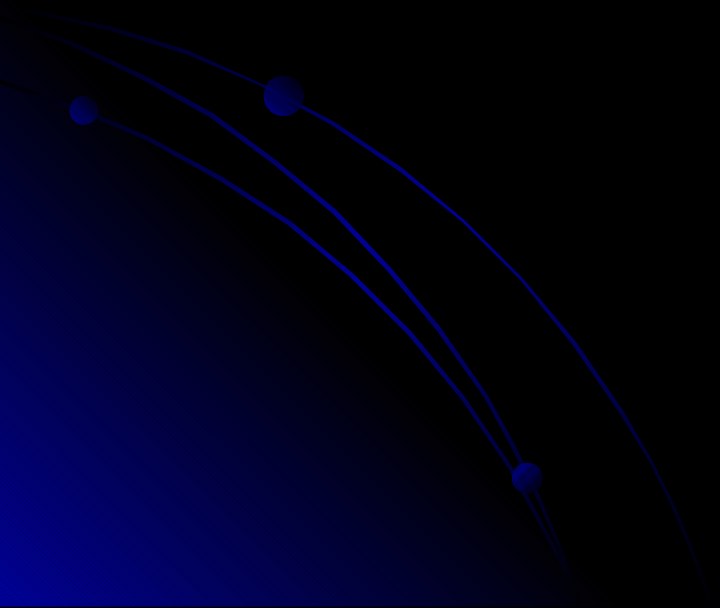
Security Through Obscurity

- Use secrecy (of design, implementation, etc.) to ensure security.
- May have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them.
- We really mean "security implemented solely through obscurity."
- Obscurity is not always bad.
- Is Obscurity Ever Good?
- TBD Read an opinion: www.darkreading.com/blog.asp? blog_sectionid=326&WT.svl=blogger1_1

WikiLeaks

- PBS was targeted in retaliation for broadcasting "Frontline: Wiki Secrets“ in May 2011
  - www.pbs.org/wgbh/pages/frontline/wikileaks/ The inside story of Bradley Manning, Julian Assange and the largest intelligence breach in U.S. history

Course Specific Items



Course Title?

- Other titles for the Course
  - Internet Security
  - Network Security
  - Computer Security
  - System Security
  - Cyber Security
- Integrated View of Security Issues
- Selection of Most Relevant Topics
- Narrowest Title that Covers the Topics

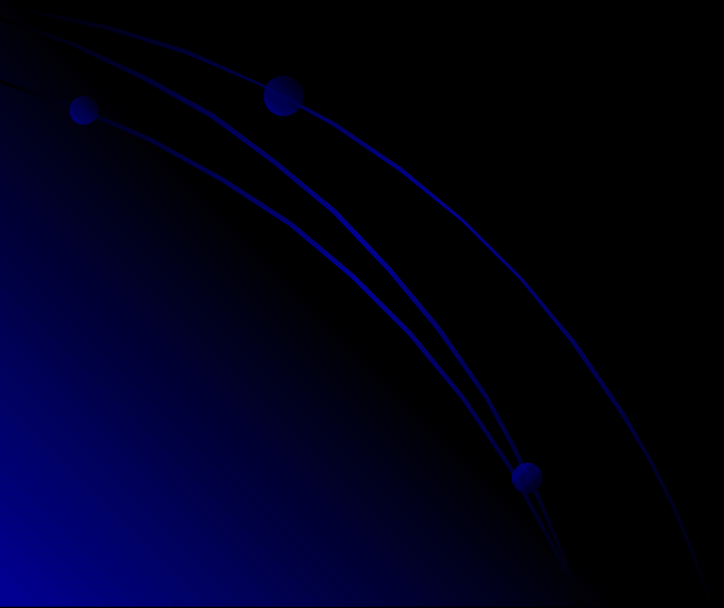
New or Revised * courses

- CEG 234N Secure Computing Practices 4
- CEG 235N System Security 4
- CEG 4420 * Internet Security 4
- CEG 430N Security Attacks & Defenses 4
- CEG 439N Secure Cloud Computing 4
- CS 419 * Crypto and Data Security 3
- CEG 4350 * Operating Systems 4

Ethics: A Personal Opinion

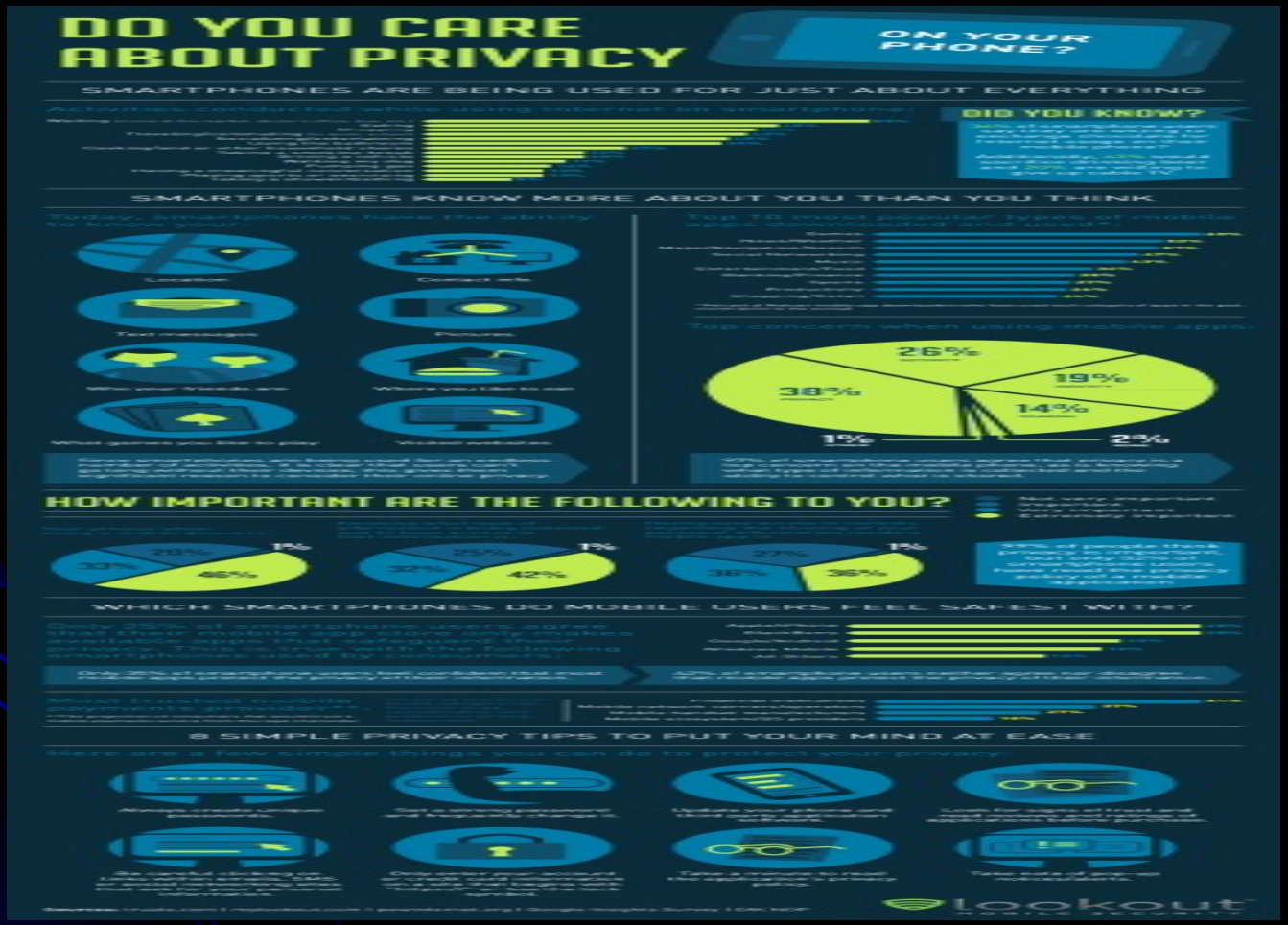
- Ethics violations on small scale DOES NOT NECESSARILY IMPLY violations on large scale.
- Cf. The movie: Crash (2004) - IMDb

Big Issues



ww.privacyrights.org

- “More than 220 million records containing sensitive personal information have been leaked in security breaches in the United States since January 2005. This site tracks every breach and provides links to resources businesses should consult if they experience a security breach and aren't sure how to respond”


DO YOU CARE ABOUT PRIVACY
ON YOUR PHONE?
SMARTPHONES ARE BEING USED FOR JUST ABOUT EVERYTHING
DID YOU KNOW?
SMARTPHONES KNOW MORE ABOUT YOU THAN YOU THINK
26%
19%
38%
14%
1%
2%
HOW IMPORTANT ARE THE FOLLOWING TO YOU?
WHICH SMARTPHONES DO MOBILE USERS FEEL SAFEST WITH?
8 SIMPLE PRIVACY TIPS TO PUT YOUR MIND AT EASE
lookout

Privacy

- Gov't: We want stored emails, phone locations.
- The Electronic Communication Privacy Act of 1986
  - e.g., govt can get past cell phone geolocation data without warrant
- www.eff.org/issues/national-security-letters
- A new bill (May 2011) proposes requiring a warrant to seize email, cell phone location, or … stored in the cloud.

Will Internet ever be trustworthy?

- Non-Answers
  - Equate the question with:
    - “Will the world ever be trustworthy?”
- Internet is a man-made entity.
- Trustworthy = … ?
- Ok if cost is high?
- Will users get educated?

Trustworthy = No Cheating + …

- User authentication
- Host authentication
- Access authentication
- Message/Transaction authentication
- No repudiation

Trustworthy = … + Reliable + …

- Transactions/Operations/Services/…
  - Availability
  - correctly execute
  - Terminate
    - Successfully
    - Failures
  - Computer Resource consumption
    - CPU time
    - Memory
    - …

Trustworthy = + …?

Will Internet ever be trustworthy?

Predictions

Will Internet ever be trustworthy?

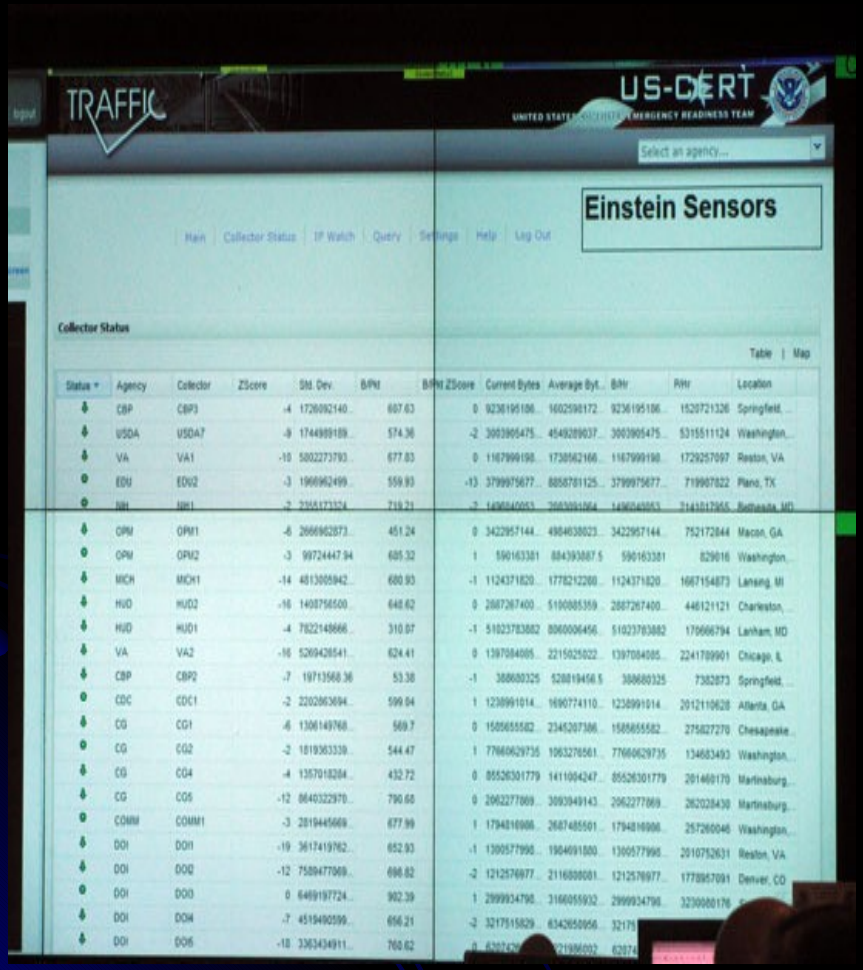
Analysis

US Preparedness

DHS' Classified NCCIC

- National Cybersecurity and Communications Integration Center (NCCIC)
- DHS-led inter-agency cybersecurity work
  - responding to cyber threats against government networks
  - monitoring network sensors across the government and
  - coordinating response to cyber attacks against power plants or communications networks.
- unclassified for one day 10/09/2010

US-CERT Einstein Sensors



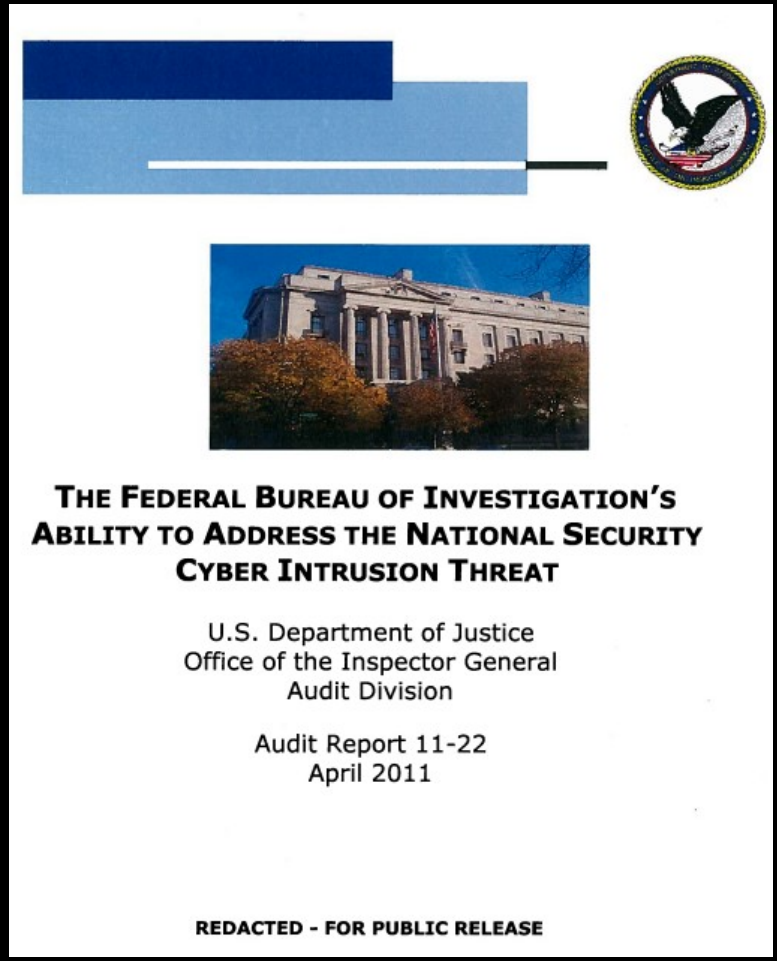
- This screen shows a selection of real-time information from network flow analyzers placed strategically within government networks nationwide.
- Einstein sensors is a series of technologies being deployed across the government for network monitoring, intrusion detection and intrusion prevention.
- "We identify not only cyber threats, but also monitor the cyber health of the nation."

NCCIC Fly-Away Kit

- NCCIC doesn't do malware analysis.
- However, for demo purposes, DHS brought out some of its digital forensics tools for reporters to see, including these.

DOJ report critical of FBI

- FBI in some cases lacks the skills to properly investigate national security intrusions.
- justice.gov/oig/reports/FBI/a1122r.pdf
- FBI cyber threat success: the taking down of the CoreFlood botnet.



THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT

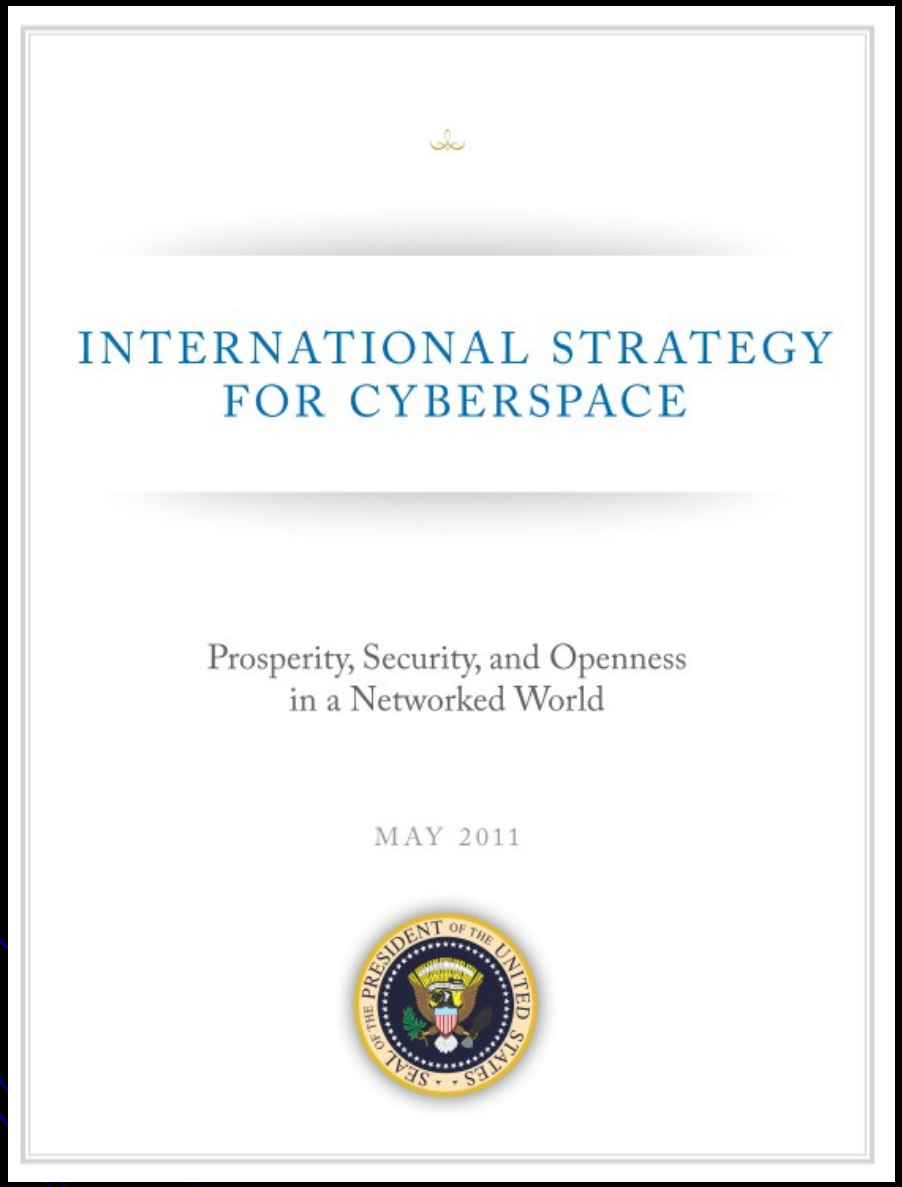
U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 11-22
April 2011

REDACTED - FOR PUBLIC RELEASE

“Science of Cyber-Security”

- Examines the theory and practice of cyber-security, and evaluates whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach.
- November 2010, DoD sponsored report
- http://www.fas.org/irp/agency/dod/jason/cyber.pdf

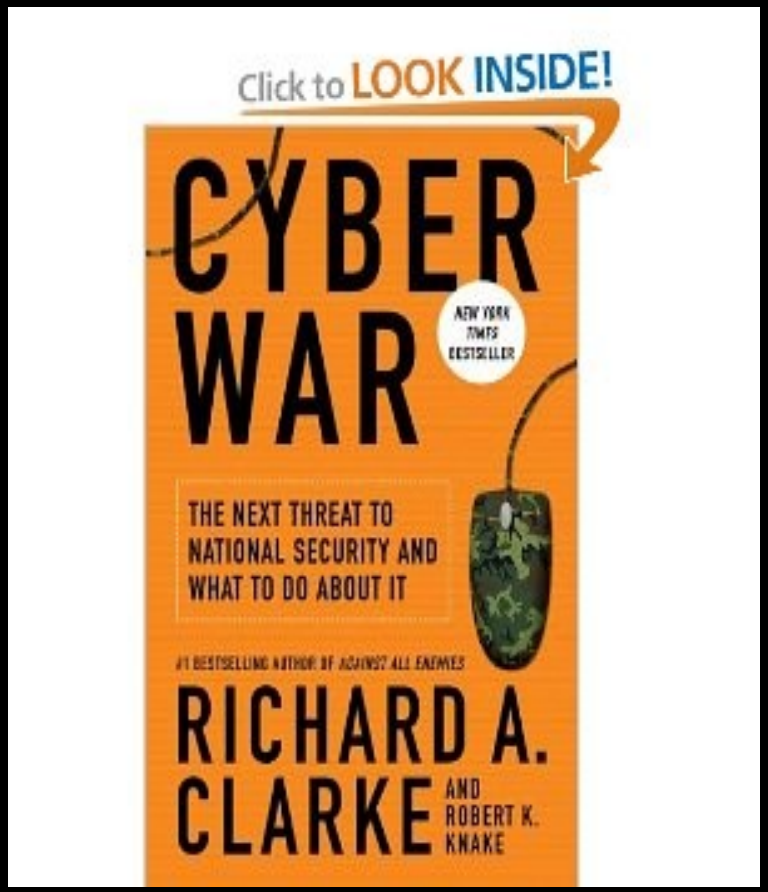

INTERNATIONAL STRATEGY
FOR CYBERSPACE
Prosperity, Security, and Openness
in a Networked World
MAY 2011

Cybersecurity Plan 2011

- International Strategy for Cyberspace
- protecting Web infrastructure
- freedom of expression and commerce via the Internet
- denying those benefits to terrorists and criminals
- “Cybersecurity threats and online technologies change quickly -- so quickly that any regulations for cybersecurity could be outdated before they are finalized.”

“Cyber War” A Book

- Current state of cyber warfare compares to the early days of nuclear weaponry:
  - Its enormous power is not yet understood and its use is not yet regulated.
- America vulnerable to electronic attack.
- Clark: former White House terrorism adviser
- washingtonpost.com/ review 2010/05/21
- 4/5 stars (95 Amazon reviews)



UK cyber weapons program

- Cyber weapons as "an integral part of the country's armory"
- Cyberspace represented "conflict without borders"
- Cybersecurity a tier one priority
- Extra £650m
- May 2011

Random Quote

“ Restrictions of free thought and free speech is the most dangerous of all subversions. It is the one un-American act that could most easily defeat us.”

- William O. Douglas,
US Supreme Court, 1939-1980