Dan Kaufman
Director, Information Innovation Office

An analytical framework for cyber security

An analytical framework for cyber security

November 2011

What we hear.

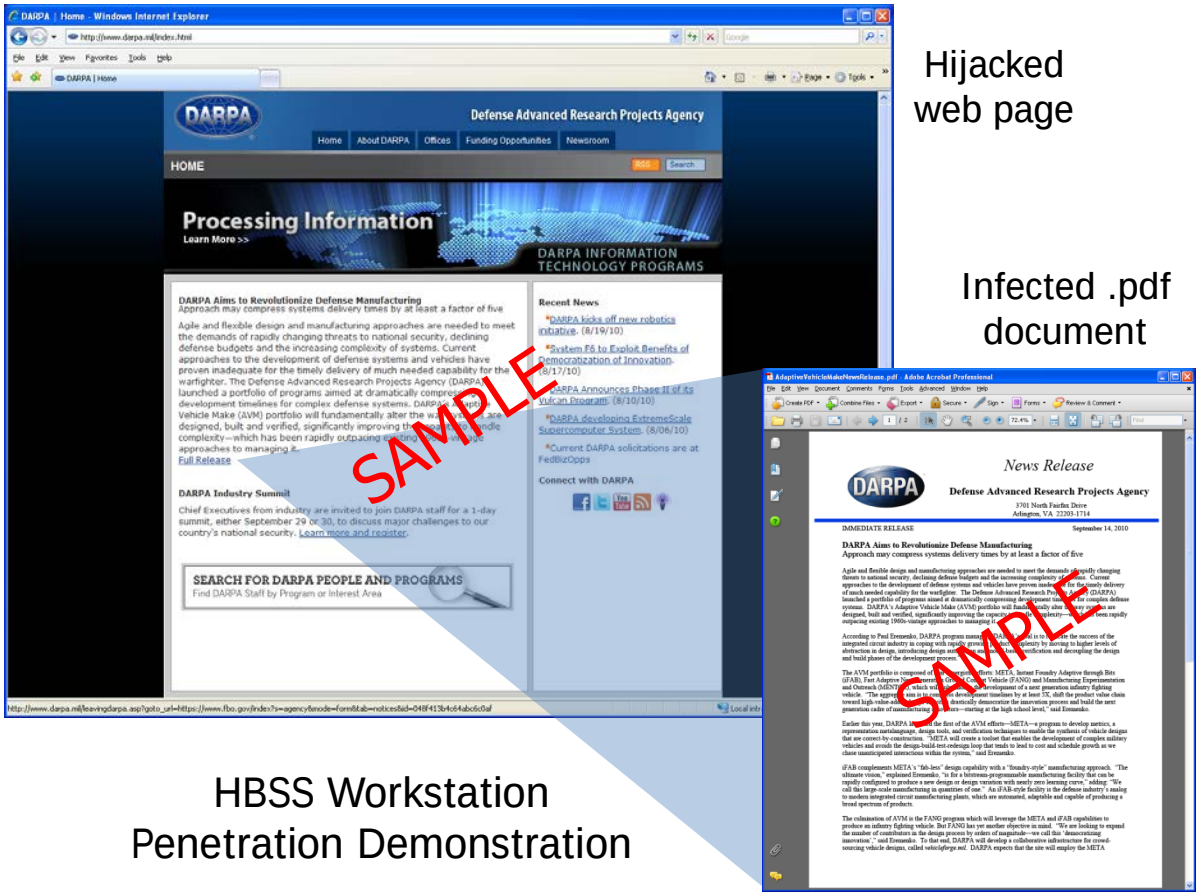
Attackers penetrate the architecture easily...

Goal

- Demonstrate asymmetric ease of exploitation of DoD computer versus efforts to defend.

Result

- Multiple remote compromises of fully security compliant and patched HBSS‡ computer within days:
  - 2 remote accesses.
  - 25+ local privilege escalations.
  - Undetected by host defenses.



Hijacked web page

Infected .pdf document

HBSS Workstation Penetration Demonstration

Total Effort: 2 people, 3 days, $18K

HBSS Costs: Millions of dollars a year for software and licenses alone (not including man hours)

‡ = Host Based Security System (HBSS)

Users are the weak link...

Finweb = Jane123
DTS = 123Jane
PKI = JaneA123
DiskCrypt = Jane123A
Gmail = Jane123A

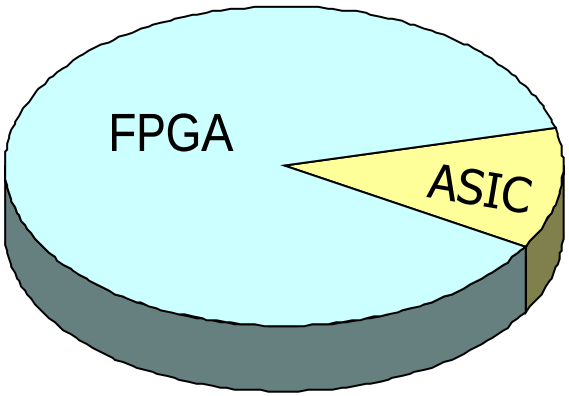
The supply chain is potentially compromised...

Approximately 3500 ICs.

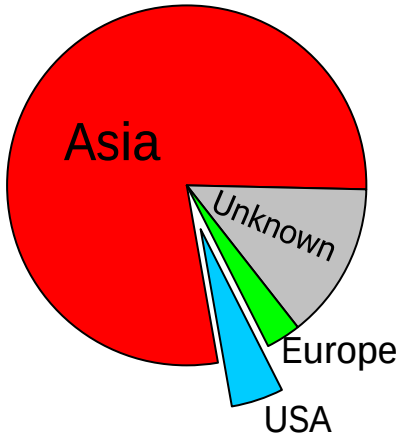
- 200 unique chip types.
- 208 field programmable gate arrays (FPGAs).
- 64 FPGA and 9 ASIC types across 12 subsystems.

78% of FPGAs and 66% of ASICs manufactured in China and Taiwan.

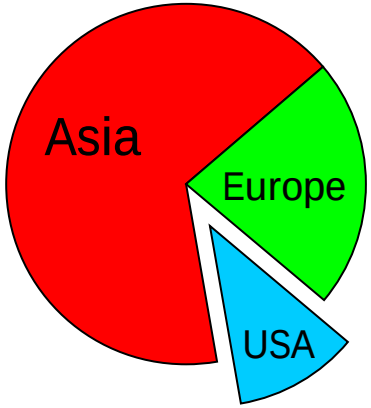
JSF FPGA & ASIC Usage



FPGA Manufacture Location



ASIC Manufacture Location



Our physical systems are vulnerable to cyber attacks...

A4 Nation s The Washington Post 219180096 SATURDAY, JANUARY 16, 2010

U.S. plans to issue official protest to China over attack on Google

BY ELLEN NAKASHIMA

The United States will issue an official protest to the Chinese government over a major espionage attack targeting Google's computer systems and rights activists' e-mail accounts that the search-engine giant said originated in China.

"We will be issuing a formal de-

cident" and seek an explanation, he said. The move may signal a shift for an administration that has been reluctant, according to China experts, to press sensitive issues such as human rights, lest it offend a country whose cooperation it seeks in other areas.

On Tuesday, in a rare disclosure by a major firm, Google announced that its "corporate infrastructure" had been hacked and

Google, were affected.

Google also said it will no longer filter Internet searches on its Chinese search engine, Google.cn. Although it did not directly accuse China, the Silicon Valley technology titan threatened to pull out of the country if the government does not allow it to operate uncensored. Chinese officials said that their laws ban hacking and that China's Internet is open,

day. She is expected to allude to the incident. "When she talks about this issue, China will be one of the countries she points to," an administration official said.

"You couldn't have picked a worse company to hack if you

Officials said the administration has raised concerns about cybersecurity and Internet freedom with China before. But by formally protesting to the Chinese, the United States is elevating the issues to a new level, policy experts said. Richard N. Ro-

said his analysis of results from a technology firm investigating the attacks suggests that they "were not state-sponsored or the work of an elite, sophisticated group such as the Chinese military."

Nonetheless, said Sophie Richardson, Asia advocacy director

Chinese cyber attack:
"Highly sophisticated and targeted attack" on Google corporate infrastructure (known as Aurora)

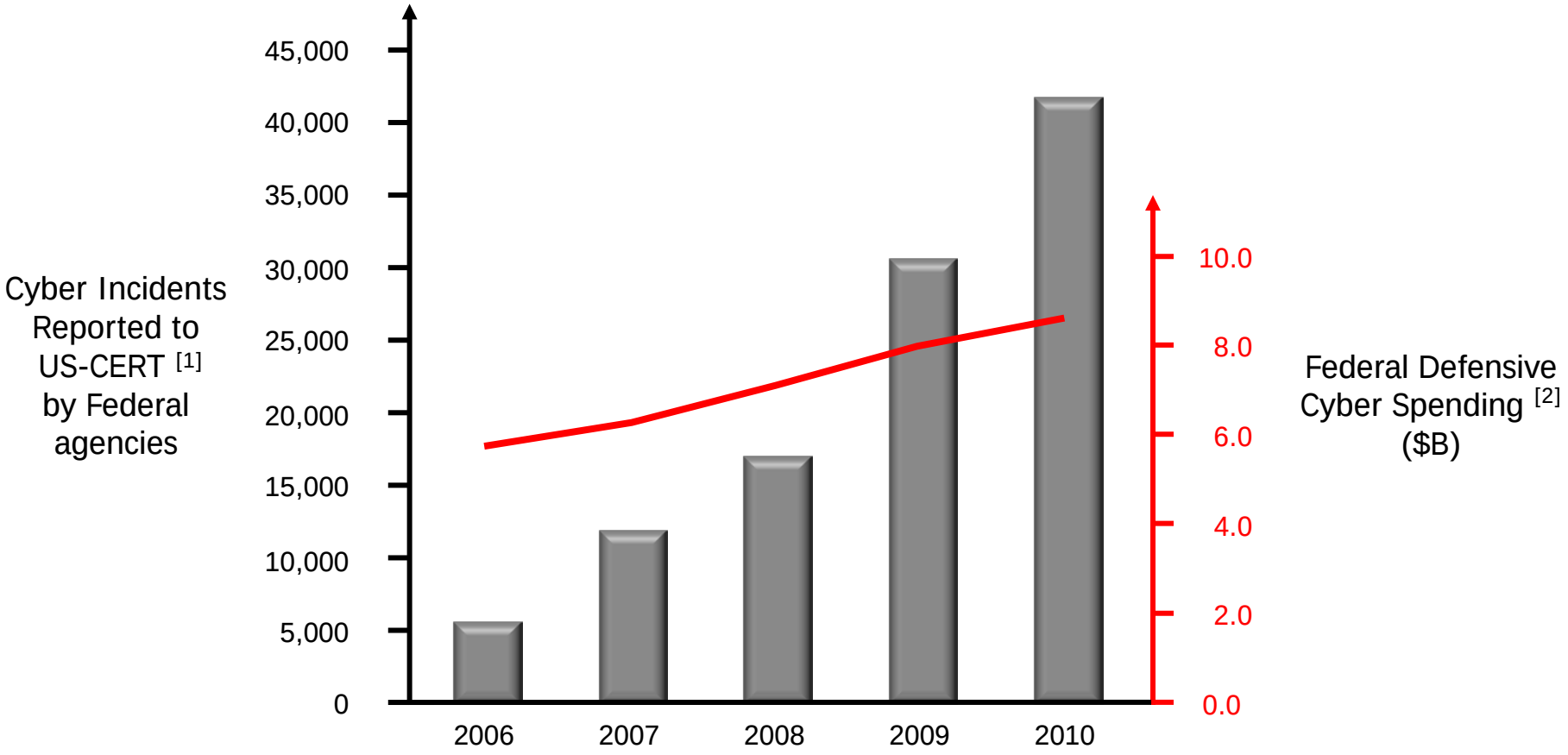
Small group of academics took control of a car using Bluetooth and OnStar. They were able to disable the brakes, control the accelerator, and turn on the interior microphone.[1]

False speedometer reading
Note that the car is in park...

[1] K. Koscher, et al. "Experimental Security Analysis of a Modern Automobile," in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.

We are doing a lot, but we are losing ground...

Ground truth...



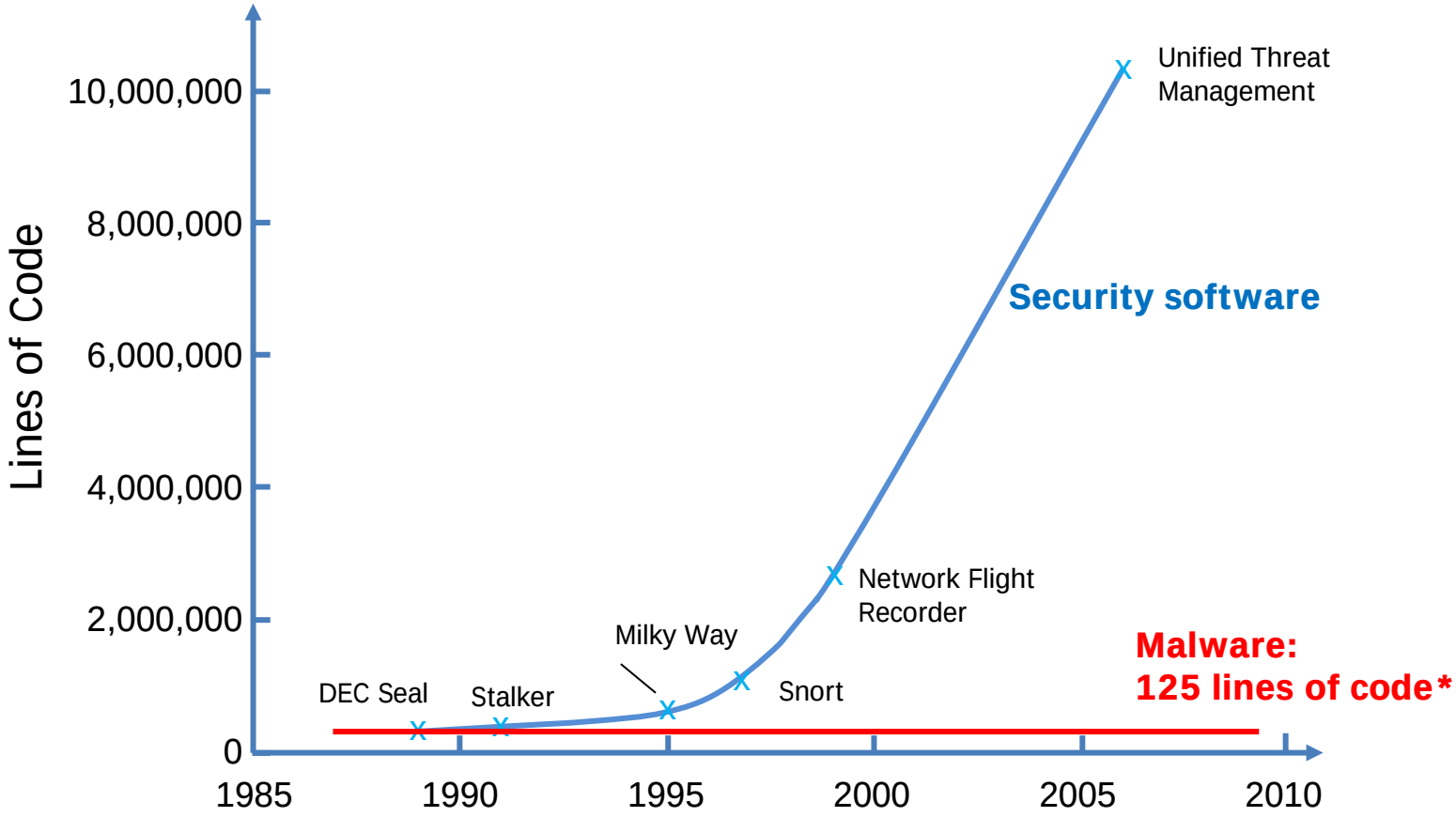
Federal Cyber Incidents and Defensive Cyber Spending
fiscal years 2006 – 2010

[1] GAO analysis of US-CERT data.
GAO-12-137 Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements

[2] INPUT reports 2006 – 2010

Why?

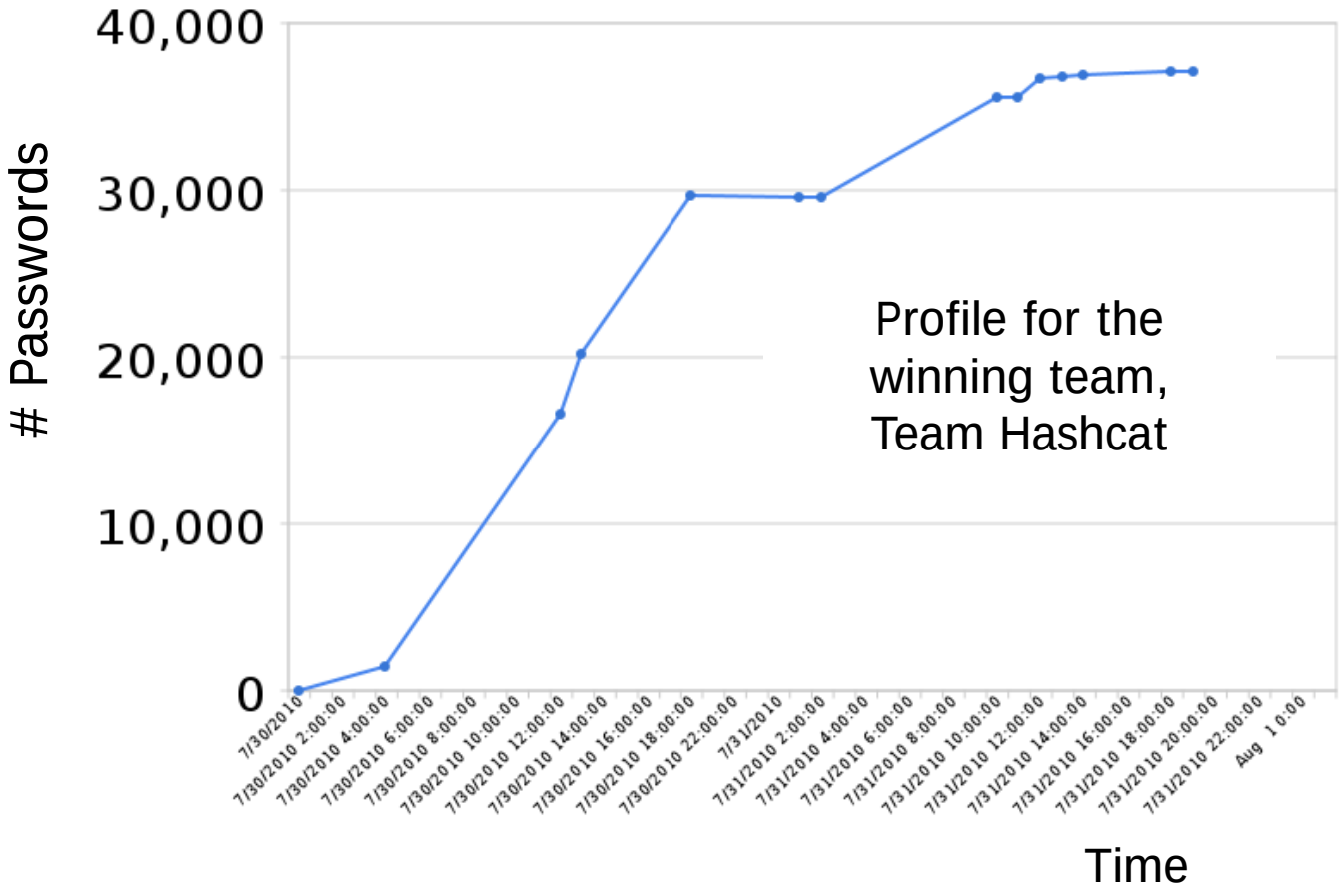
We are divergent with the threat...



* Public sources of malware averaged over 9,000 samples (collection of exploits, worms, botnets, viruses, DoS tools)

User patterns are exploitable...

A recent Defcon contest challenged participants to crack 53,000 passwords. In 48 hours, the winning team had 38,000.



Additional security layers often create vulnerabilities...

October 2010 vulnerability watchlist

Vulnerability Title	Fix Avail?	Date Added
XXXXXXXXXXXX XXXXXXXXXXXX Local Privilege Escalation Vulnerability	No	8/25/2010
XXXXXXXXXXXX XXXXXXXXXXXX Denial of Service Vulnerability	Yes	8/24/2010
XXXXXXXXXXXX XXXXXXXXXXXX Buffer Overflow Vulnerability	No	8/20/2010
XXXXXXXXXXXX XXXXXXXXXXXX Sanitization Bypass Weakness	No	8/18/2010
XXXXXXXXXXXX XXXXXXXXXXXX Security Bypass Vulnerability	No	8/17/2010
XXXXXXXXXXXX XXXXXXXXXXXX Multiple Security Vulnerabilities	Yes	8/16/2010
XXXXXXXXXXXX XXXXXXXXXXXX Remote Code Execution Vulnerability	No	8/16/2010
XXXXXXXXXXXX XXXXXXXXXXXX Use-After-Free Memory Corruption Vulnerability	No	8/12/2010
XXXXXXXXXXXX XXXXXXXXXXXX Remote Code Execution Vulnerability	No	8/10/2010
XXXXXXXXXXXX XXXXXXXXXXXX Multiple Buffer Overflow Vulnerabilities	No	8
XXXXXXXXXXXX XXXXXXXXXXXX Stack Buffer Overflow Vulnerability	Yes	8
XXXXXXXXXXXX XXXXXXXXXXXX Security-Bypass Vulnerability	No	8
XXXXXXXXXXXX XXXXXXXXXXXX Multiple Security Vulnerabilities	No	8
XXXXXXXXXXXX XXXXXXXXXXXX Buffer Overflow Vulnerability	No	7/29/2010
XXXXXXXXXXXX XXXXXXXXXXXX Remote Privilege Escalation Vulnerability	No	7/28/2010
XXXXXXXXXXXX XXXXXXXXXXXX Cross Site Request Forgery Vulnerability	No	7/26/2010
XXXXXXXXXXXX XXXXXXXXXXXX Multiple Denial Of Service Vulnerabilities	No	7/22/2010





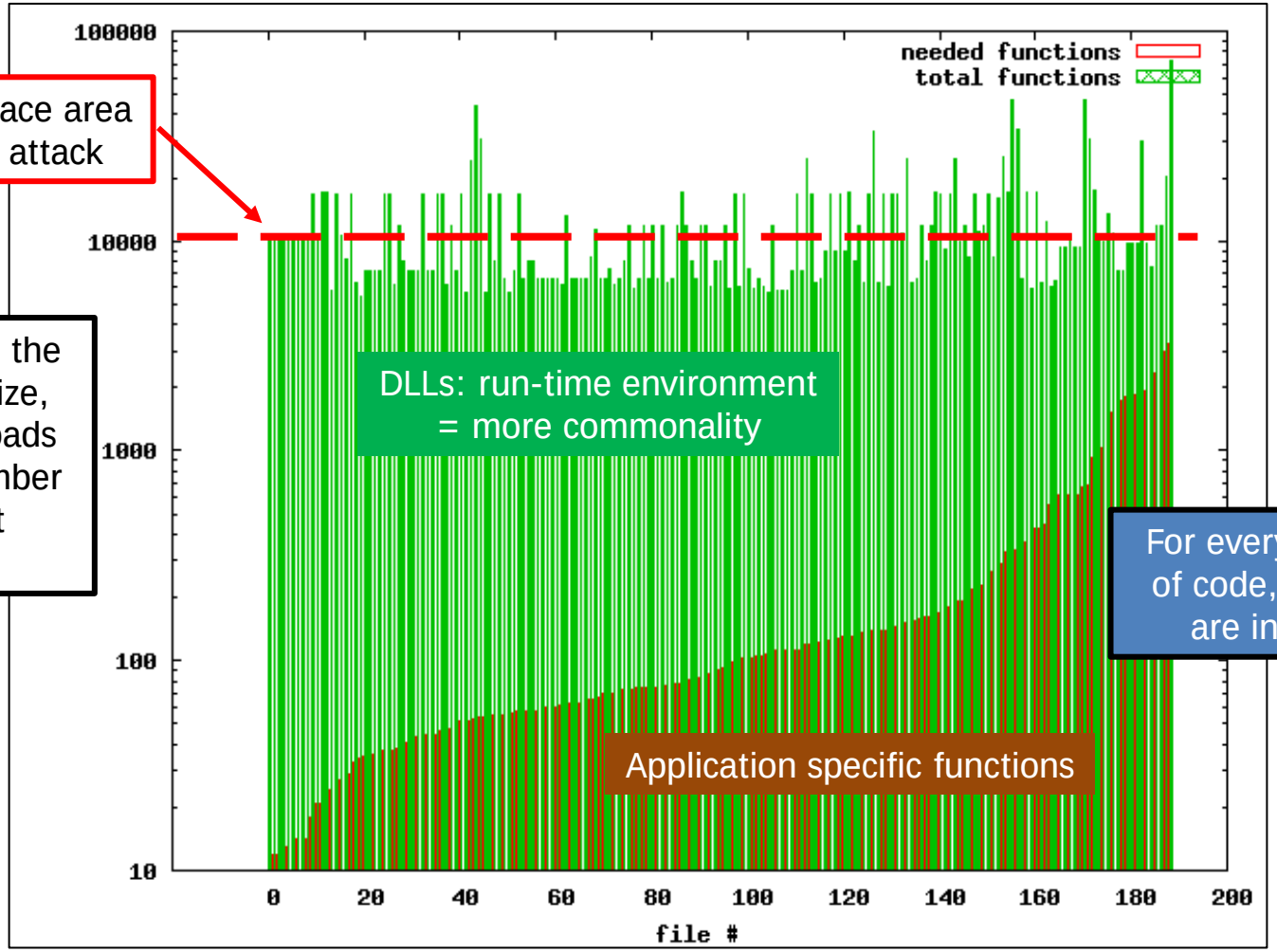

6 of the vulnerabilities are in security software

Color Code Key: Vendor Replied – Fix in development | Awaiting Vendor Reply/Confirmation | Awaiting CC/S/A use validation

These layers increase the attack surface...

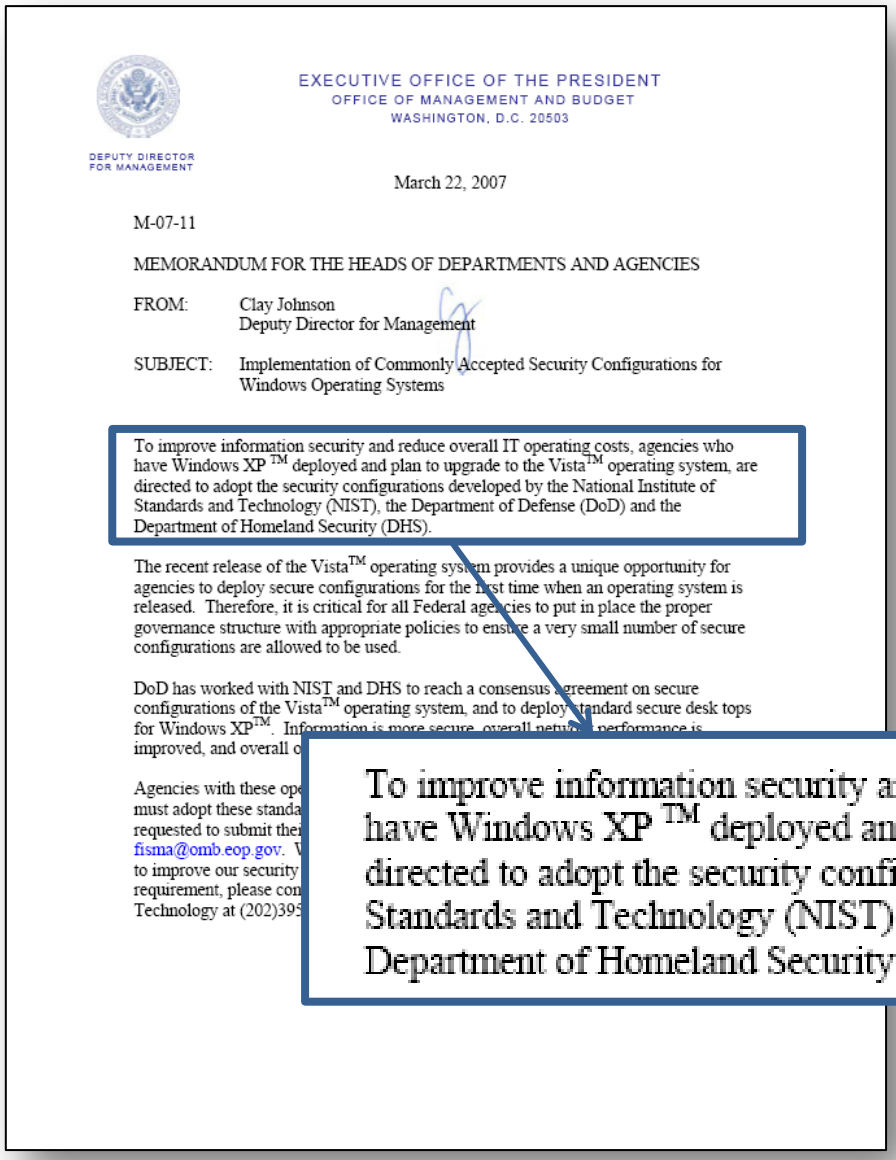
Constant surface area available to attack

Regardless of the application size, the system loads the same number of support functions.



For every 1,000 lines of code, 1 to 5 bugs are introduced.

We amplify the effect by mandating uniform architectures



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

March 22, 2007

M-07-11

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson
Deputy Director for Management

SUBJECT: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

To improve information security and reduce overall IT operating costs, agencies who have Windows XP ™ deployed and plan to upgrade to the Vista™ operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

The recent release of the Vista™ operating system provides a unique opportunity for agencies to deploy secure configurations for the first time when an operating system is released. Therefore, it is critical for all Federal agencies to put in place the proper governance structure with appropriate policies to ensure a very small number of secure configurations are allowed to be used.

DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista™ operating system, and to deploy standard secure desk tops for Windows XP™. Information is more secure, overall network performance is improved, and overall o

Agencies with these ope
must adopt these standa
requested to submit ther
fisma@omb.eop.gov. V
to improve our security
requirement, please con
Technology at (202)395

To improve information security and reduce overall IT operating costs, agencies who have Windows XP ™ deployed and plan to upgrade to the Vista™ operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

The US approach to cyber security is dominated by a strategy that layers security on to a uniform architecture.

We do this to create tactical breathing space,
but it is not convergent with an evolving threat.

Technology is not the only culprit... nor the only answer.

Economics matter...

There are multiple choices for addressing the supply chain vulnerability:

- Resort to manufacturing all chips in trusted foundries.
  This is not feasible or sustainable.
- Screen all chips in systems critical to National Security or our economic base.
  Despite recent advances in screening technology, this is not feasible, affordable, or sustainable at the scales required.

Process	Trusted Design and Untrusted FAB			Untrusted Design ASIC			Untrusted Design FPGA		
	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3	Phase 1	Phase 2	Phase 3
P_D	90.0%	99.0%	99.9%	80.0%	90.0%	99.0%	90.0%	99.0%	99.9%
P_{FA}	10^{-3}	10^{-5}	10^{-7}	10^{-3}	10^{-4}	10^{-6}	10^{-3}	10^{-5}	10^{-6}
# of Transistors Evaluated	10^5	10^6	10^8	10^5	10^6	10^8	10^5	10^6	10^7
Time to Evaluate*	480 H	240 H	120 H	480 H	240 H	120 H	480 H	240 H	120 H

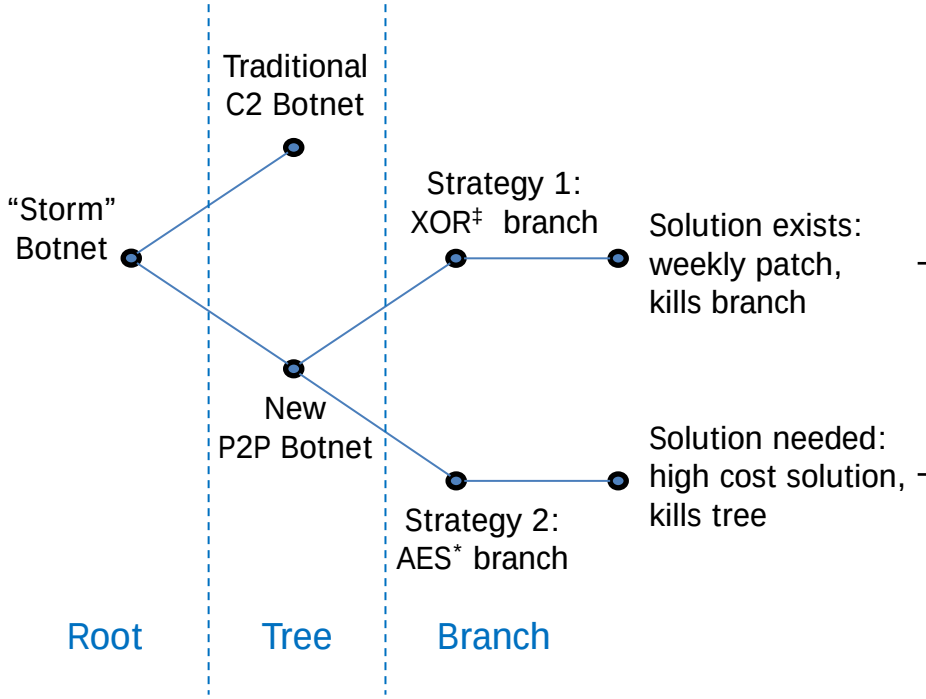
- 3,500 IC's on the F-35
- Single FPGA = 400 million transistors
- Modern chips = 2.5 billion transistors

Selective screening coupled with diplomatic sanctions may create new solutions that are both feasible and sustainable.

Business incentives matter...

Understanding them in the context of 'game theory' reveals the problem.

Bot Herder strategy example:



Bot Herder Cost	Bot Herder Return		Antivirus Cost	Antivirus Return
	Short	Long		
Small	High	High	Low	High
Small	High	0	High	Low

The security layering strategy and antitrust has created cross incentives that contribute to divergence.

‡ = "exclusive or" logical operation

* = Advanced Encryption Standard

Layering and uniformity have created unintended consequences... we are in need of new choices...

Examples:

Belief	Approach	Example	Unintended consequence
Defense in depth	Uniform, layered network defense	Host Based Security System	Larger attack surface introduces more areas of exploitability for attackers... Homogeneous targets that amplify effects...
Users are best line of defense	Operator hygiene	15 character password	Users take short cuts and become enemy assets...
The interplay of technology, policy, incentives will favor better security.	Antitrust law rulings, use of COTS	Competition and independence in security software and COTS	Cross incentives that undermine security

We need new choices that create:

Users as the best line of defense without impeding operations.
Layered defense without increasing surface area for attack.
Heterogeneous systems that are inherently manageable.

We missed it too...

...let's fix it.

Cyber Colloquium

#DARPACyber