



DARPA's Cyber Analytical Framework: Opportunities for Cyber Researchers

Daniel J. Ragsdale, Ph.D.
Program Manager
Information Innovation Office



What we hear...

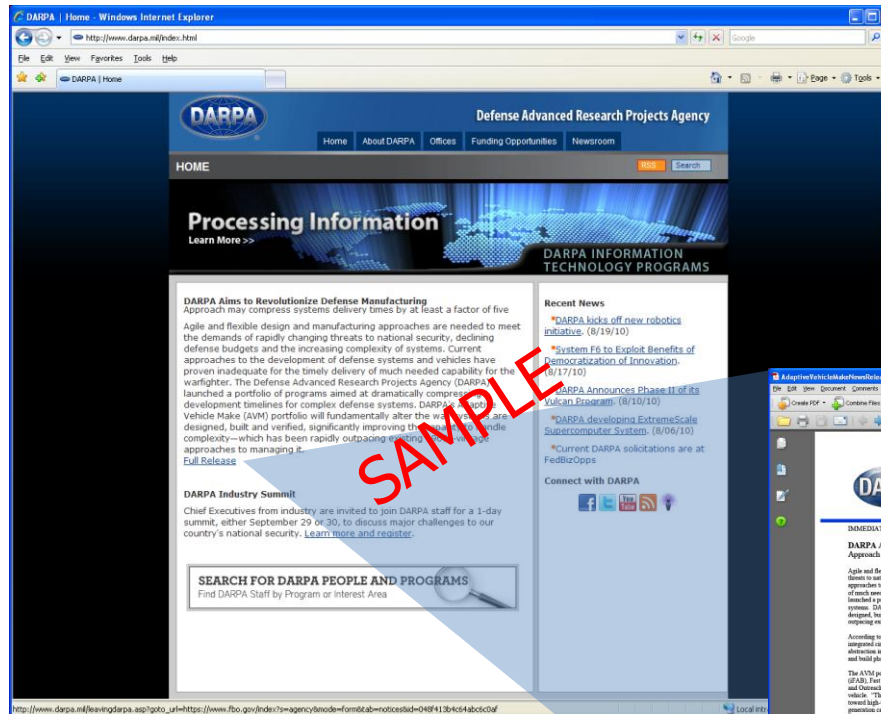


Adversaries penetrate the architecture easily...

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

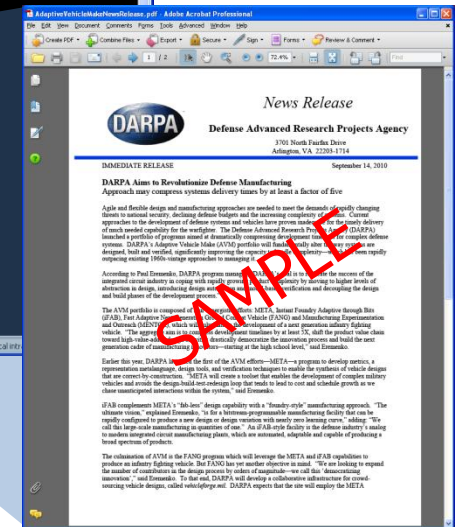
Result: Multiple remote compromises of fully security compliant and patched HBSS[‡] computer within days:

- 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



Our physical systems are vulnerable to cyber incidents...

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 demarche in the coming days," a State Department spokesman said Tuesday. The "express

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 wanted to not irritate the Americans," said James A. Ber and national security adviser at the Center for Strategic and International Studies. Google is their favorite child. The firm's chief advises President Obama on technology, and its actions are seen as the innovation that will drive the economy.

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. Ross, executive director of the Project for the New American Century, 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 for Human Rights Watch, "Google's infrastructure was hacked by a group of hackers who are likely state-sponsored."

"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...

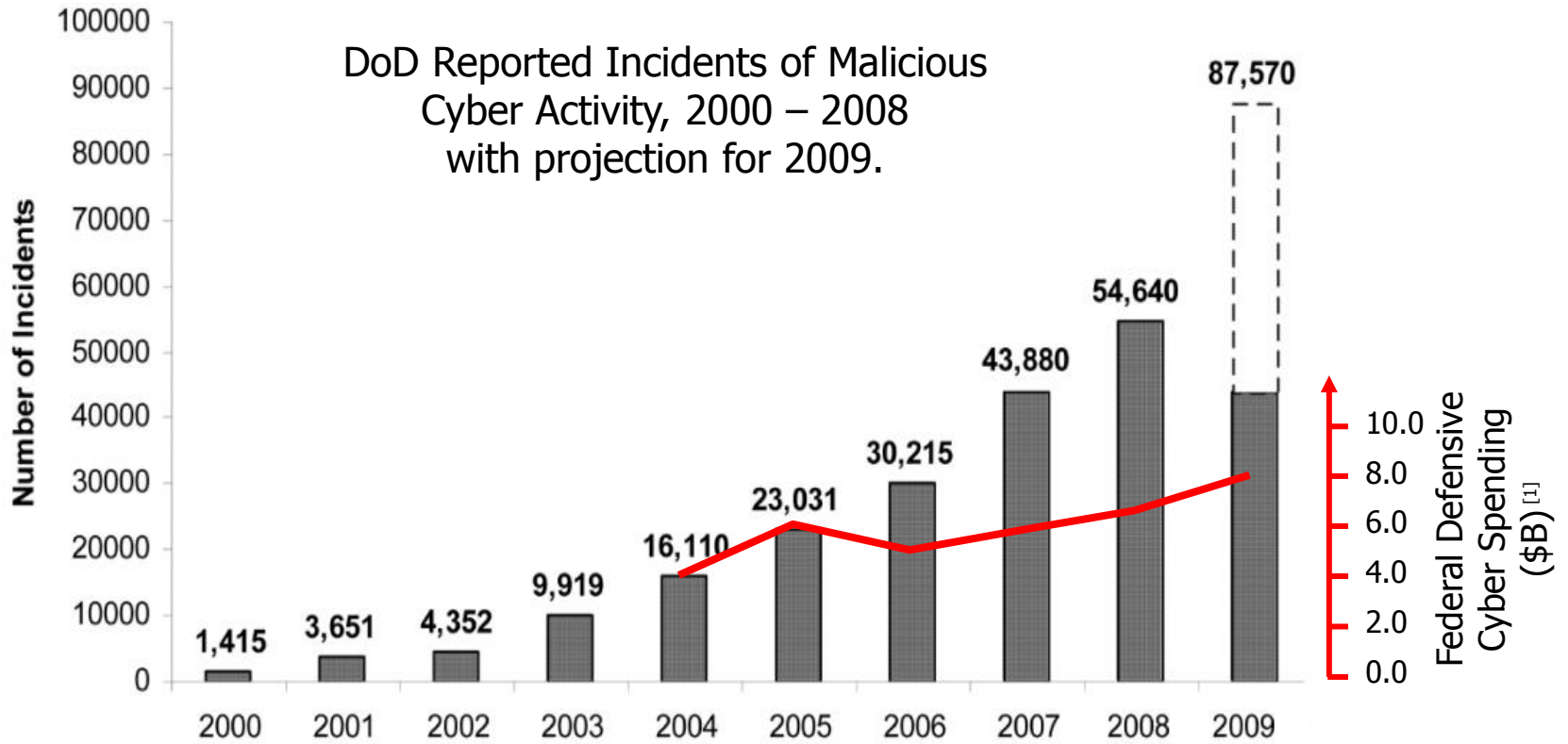
[1] K. Koscher, et al. "Experimental Security Analysis of a Modern Automobile," in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.



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



Ground truth...



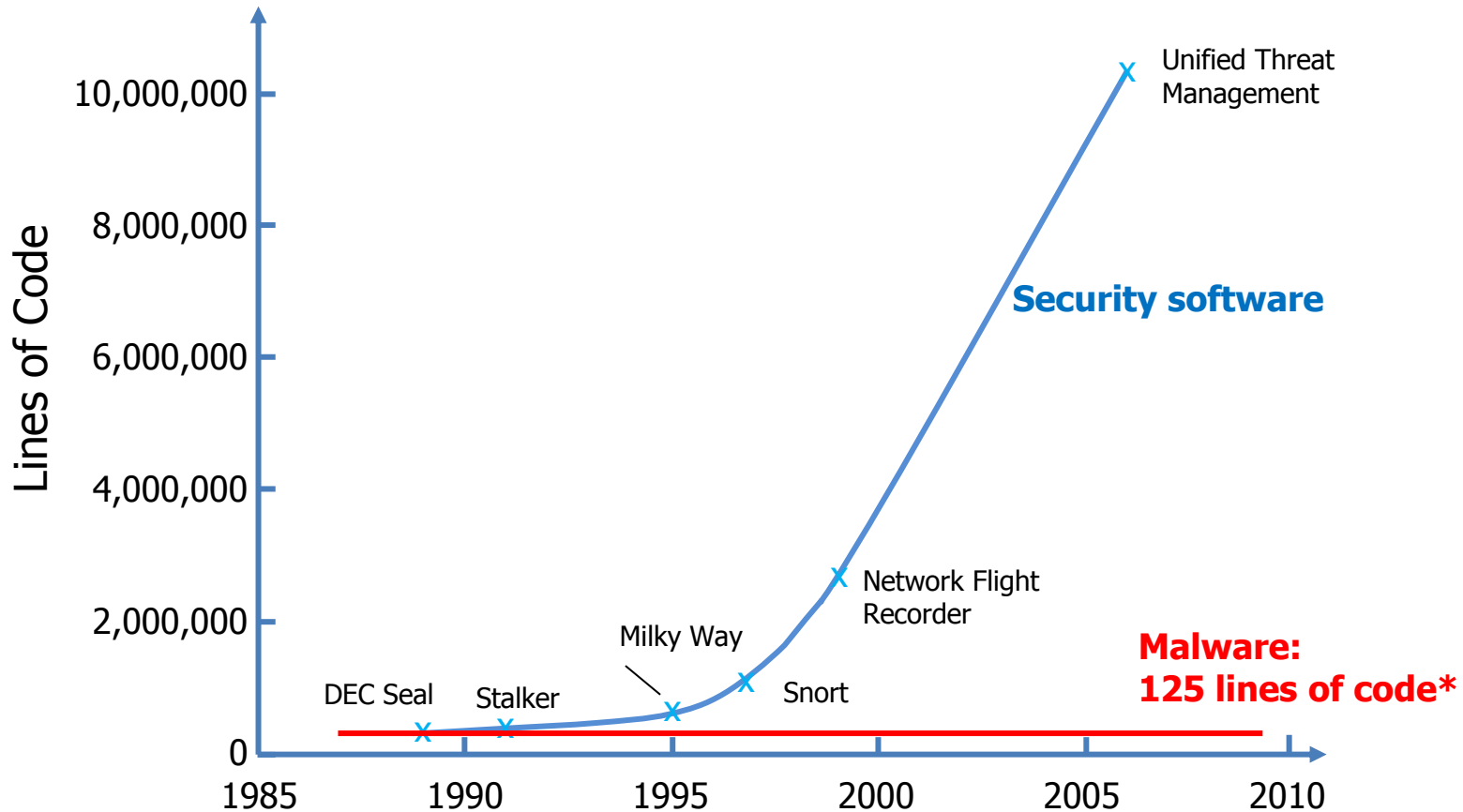
[1] INPUT reports 2004 – 2009



Why?



We are divergent with the threat...



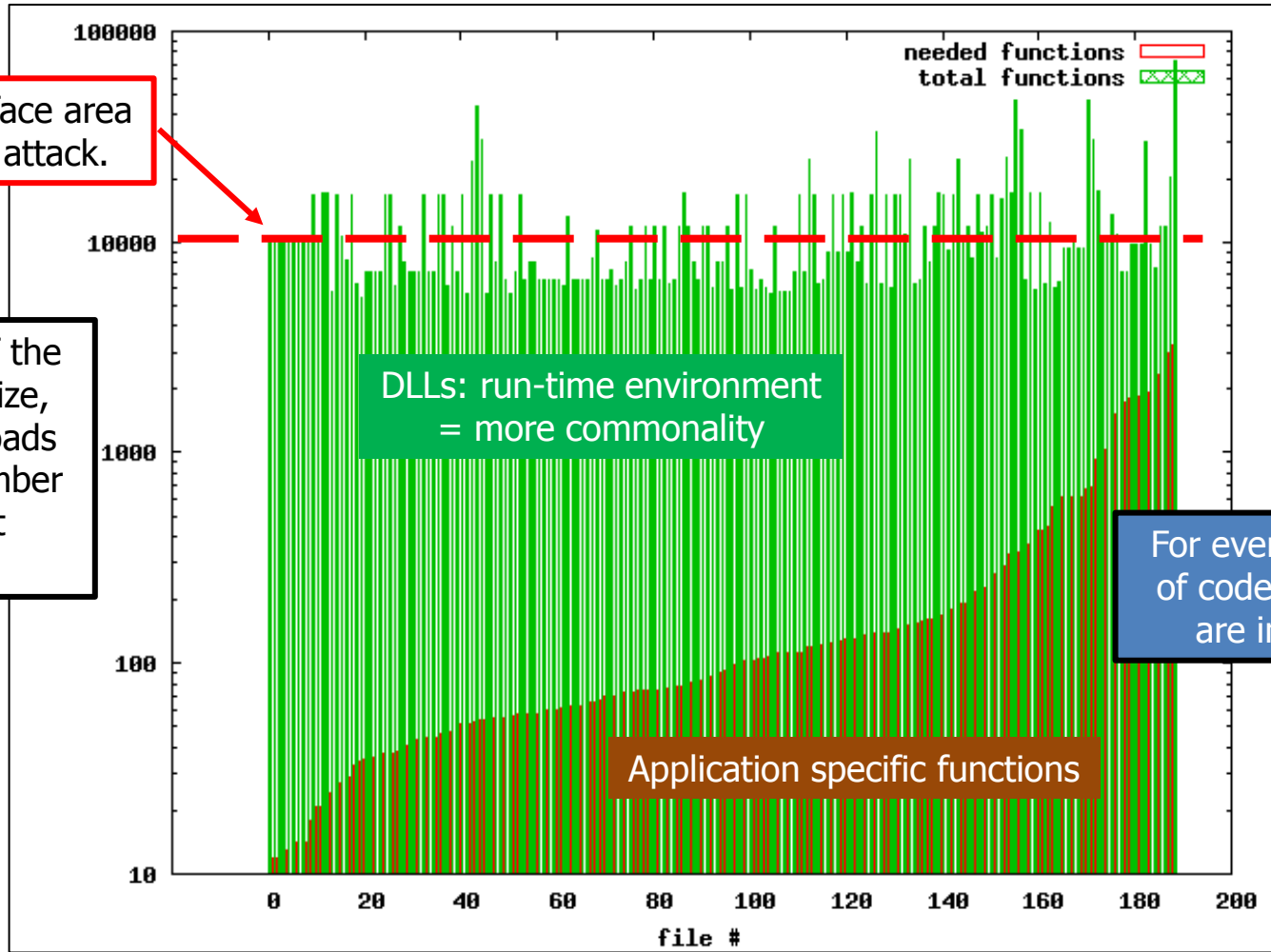
* Malware lines of code averaged over 9,000 samples



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.

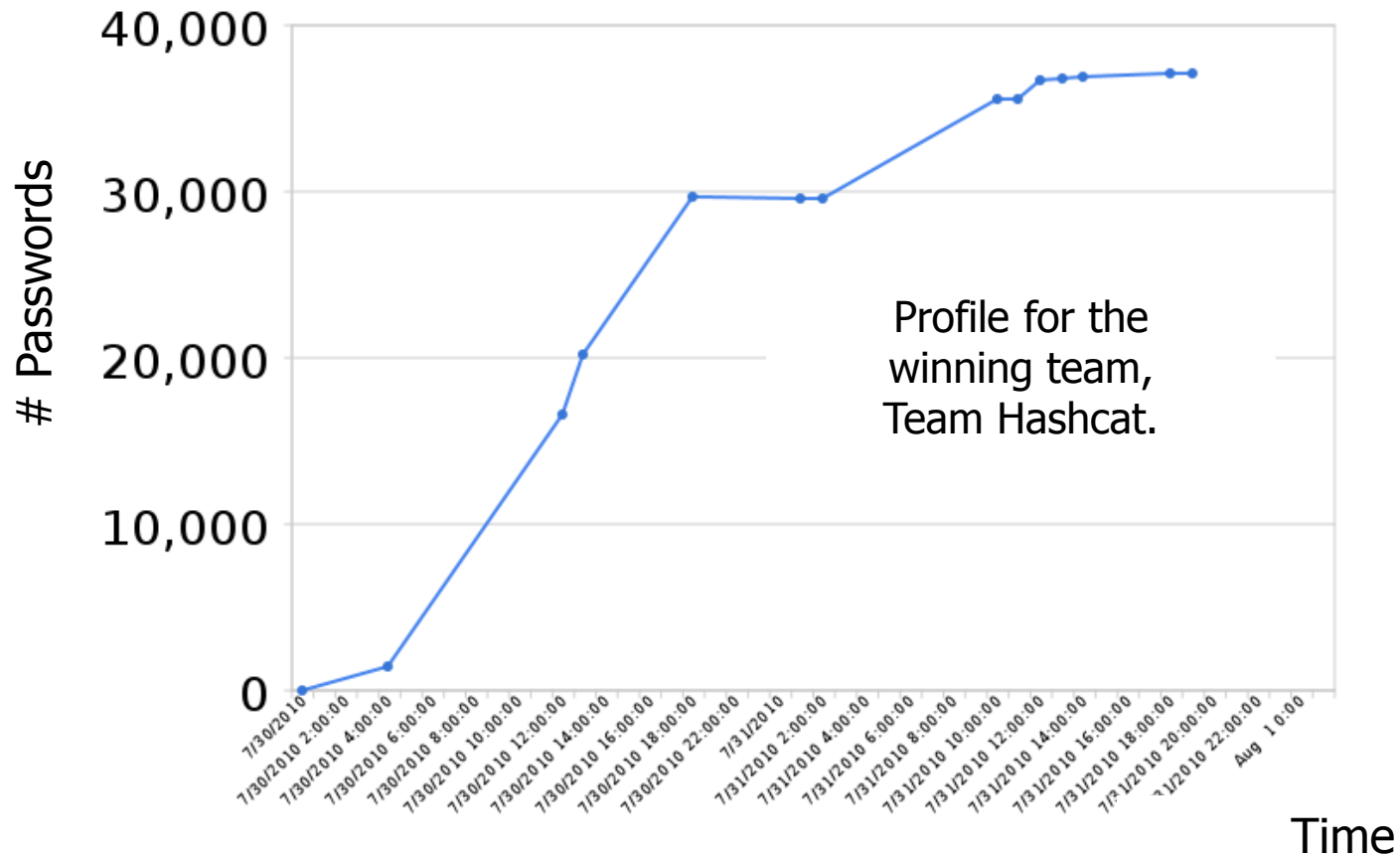


For every 1,000 lines of code, 1 to 5 bugs are introduced.



Users are being exploited by adversaries...

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...

Current vulnerability watch list:

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



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 thei
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.

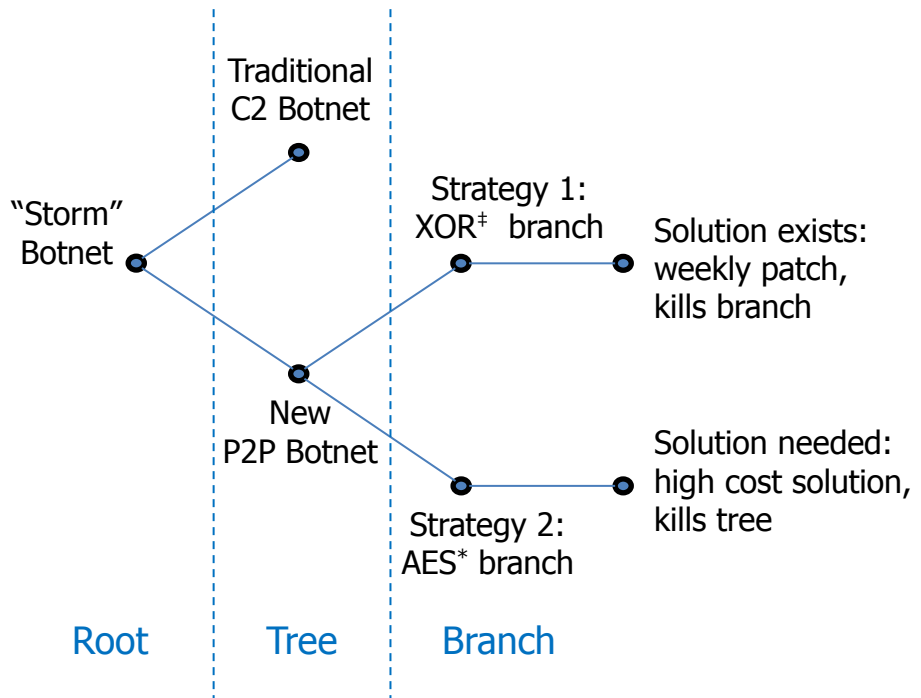
We do this to create tactical breathing space, but it is not convergent with an evolving threat.



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 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:

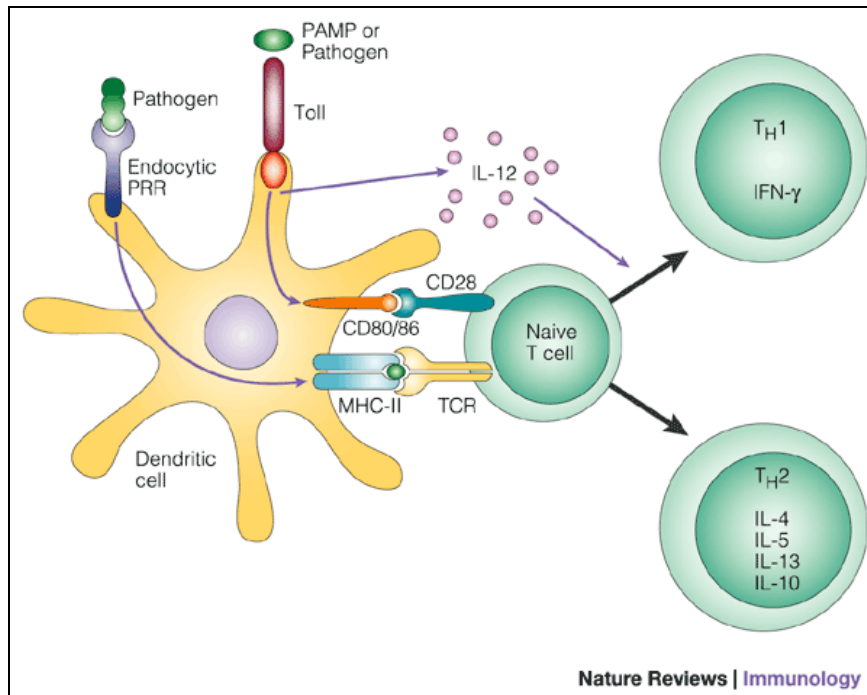
- Users as the best line of defense without impeding operations.
- Layered defense without increasing surface area for attack.
- Heterogeneous systems that are inherently manageable.



We missed it too...



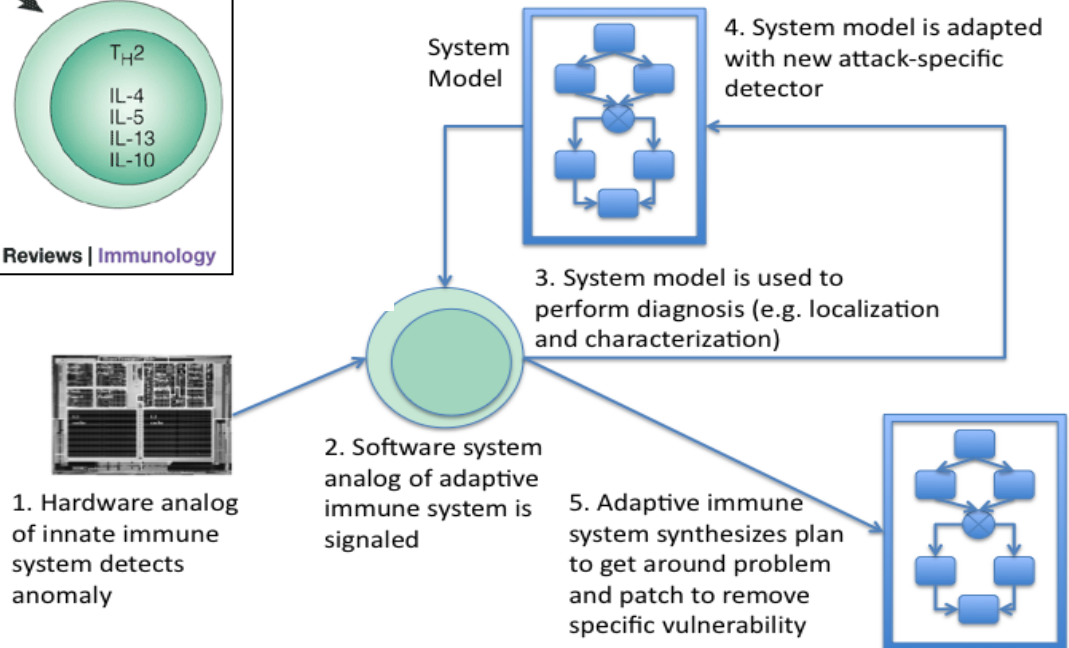
Getting convergent... New Programs....



- Preventing common attacks.
- Adapting in response to unanticipated attacks.
- Create diversity so attacker has to deal with heterogeneity.

New architectures guided by biology that eliminate common technical vulnerabilities

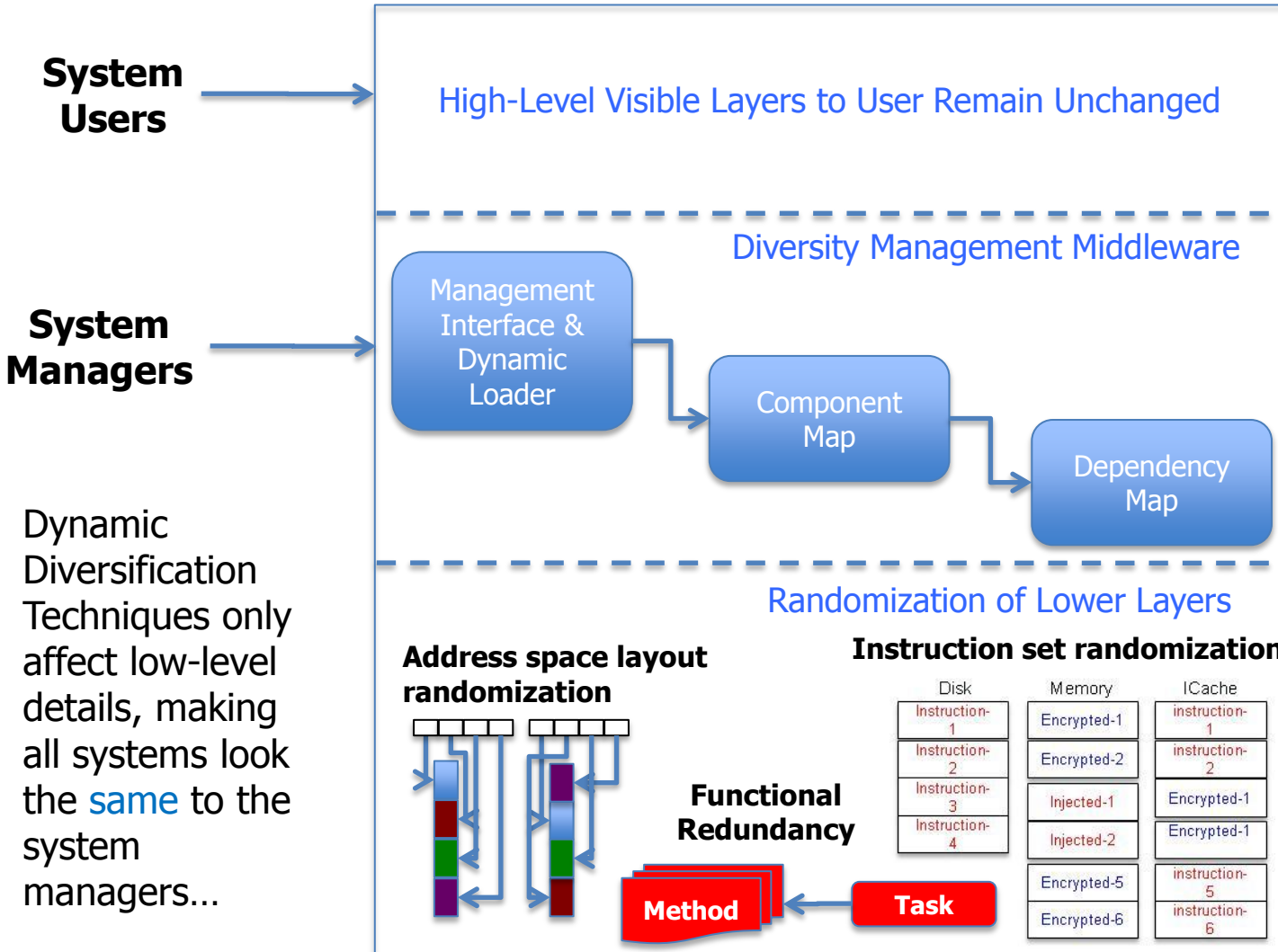
- Diagnoses root causes of vulnerabilities and builds situational assessment.
- Learns from previous attacks and gets better at self-protection.
- Increases and refreshes system diversity.



[‡] Clean-slate design of Resilient, Adaptive, Secure Hosts



The advantage of clean-slate design of resilient, adaptive, secure hosts (CRASH)



Dynamic Diversification Techniques only affect low-level details, making all systems look the **same** to the system managers...

...but vary the low-level details that adversaries exploit, making each system look **different** to the adversaries.

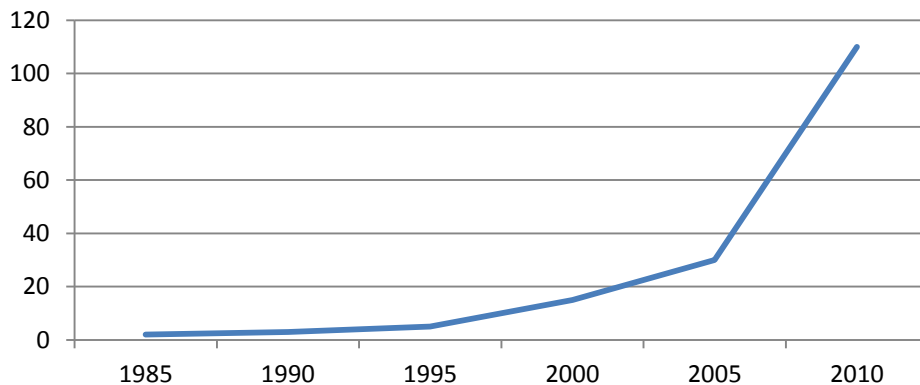
← Adversary



"Maker spaces" and Boutique Security Firms

- Small groups of motivated and like minded researchers have repeatedly shown significant talent and capabilities.
- Commodity high end computing, personal prototyping and fabrication capabilities, and open software tools remove barrier to entry.
- The new "home brew computer club"...
- This relationship needs to be mutually beneficial. DARPA intends to cultivate relations and become a resource.

Number of US Maker Spaces



NYC Resistor – Brooklyn, NY
Source: Make Magazine

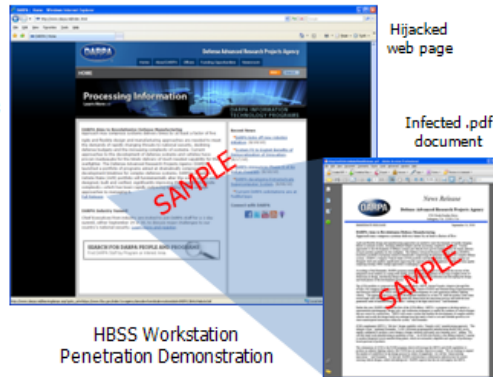
Existence Proof: Agile Cyber Projects

HBSS

DARPA Adversaries 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.

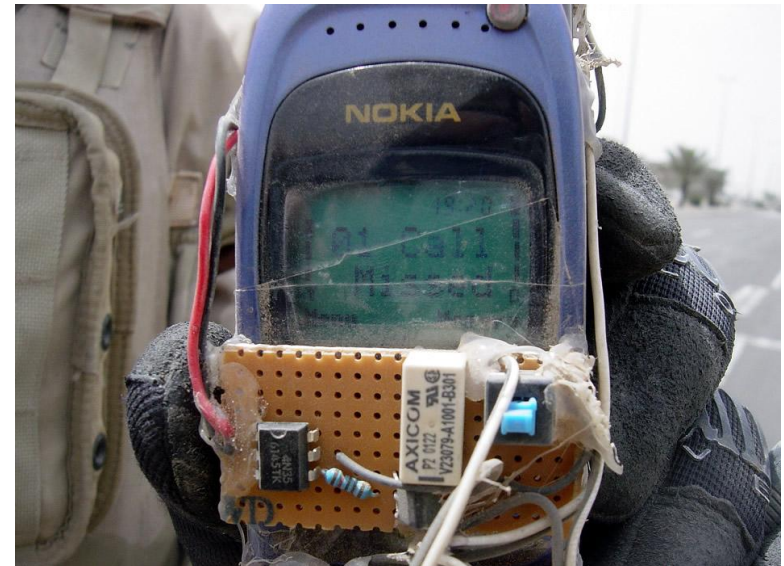
Total Effort: 2 people, 3 days, \$18K

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

® = Host Based Security System (HBSS)

2 people, 3 days = \$18k

IED WarVox



<http://imgur.com/OPhGr>

2 people, 3 weeks = \$0



www.darpa.mil



Encrypted computing in the cloud as privately as in your data center (PROCEED[‡])

It is theoretically possible to perform *arbitrary* computations on encrypted data without decrypting. Thus, preserving security *even on untrustworthy computational infrastructure*. [Gentry, 2009] ^[1]

What if all computation could be done on encrypted data?

- Secure computational outsourcing
- System hardware and software provenance concerns reduced
- Data provenance and availability remain concerns



Will your foreign-built computer steal your data?

Program Approach

- PROCEED is searching for efficient ways to compute on encrypted data that can be implemented on modern computers.
- Potential applications:
 - High assurance network guards.
 - Training simulators.
 - Image processing.

[‡] PROgramming Computation on EncryptEd Data (PROCEED)
^[1] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. 41st ACM Symposium on Theory of Computing (STOC), 2009.