

# **What If We Got A "Do-Over?" DARPA's Clean-Slate Efforts**

---

Howard Shrobe  
Program Manager, DARPA I2O

*Prepared for CCSW 2012*

*October 18, 2012*





# Attackers penetrate the architecture easily...

## Goal

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

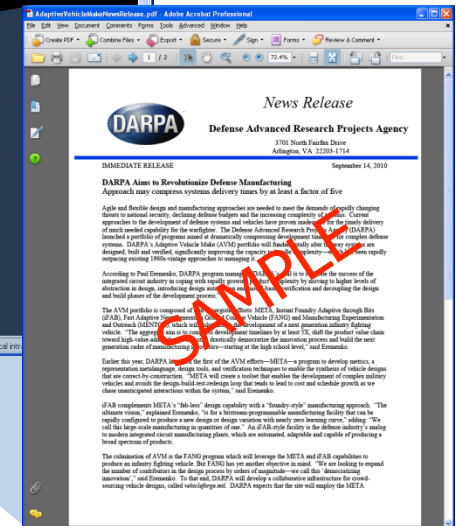
## Result

- Multiple remote compromises of fully security compliant and patched HBSS<sup>‡</sup> 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)

<sup>‡</sup> = 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 attacks...

A4 Nation

The Washington Post

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-

marche  
ment in  
the con  
next w  
spokes  
day.  
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,

ded a  
pes of  
China.  
nents  
with a  
n that  
Rod-  
Thurs-

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. Berger and national security at the Center for Strategic International Studies, their favorite child, Google. The firm's chief advises President Obama on technology, and its innovations are seen as the engine of 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, a senior 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 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.'"

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]

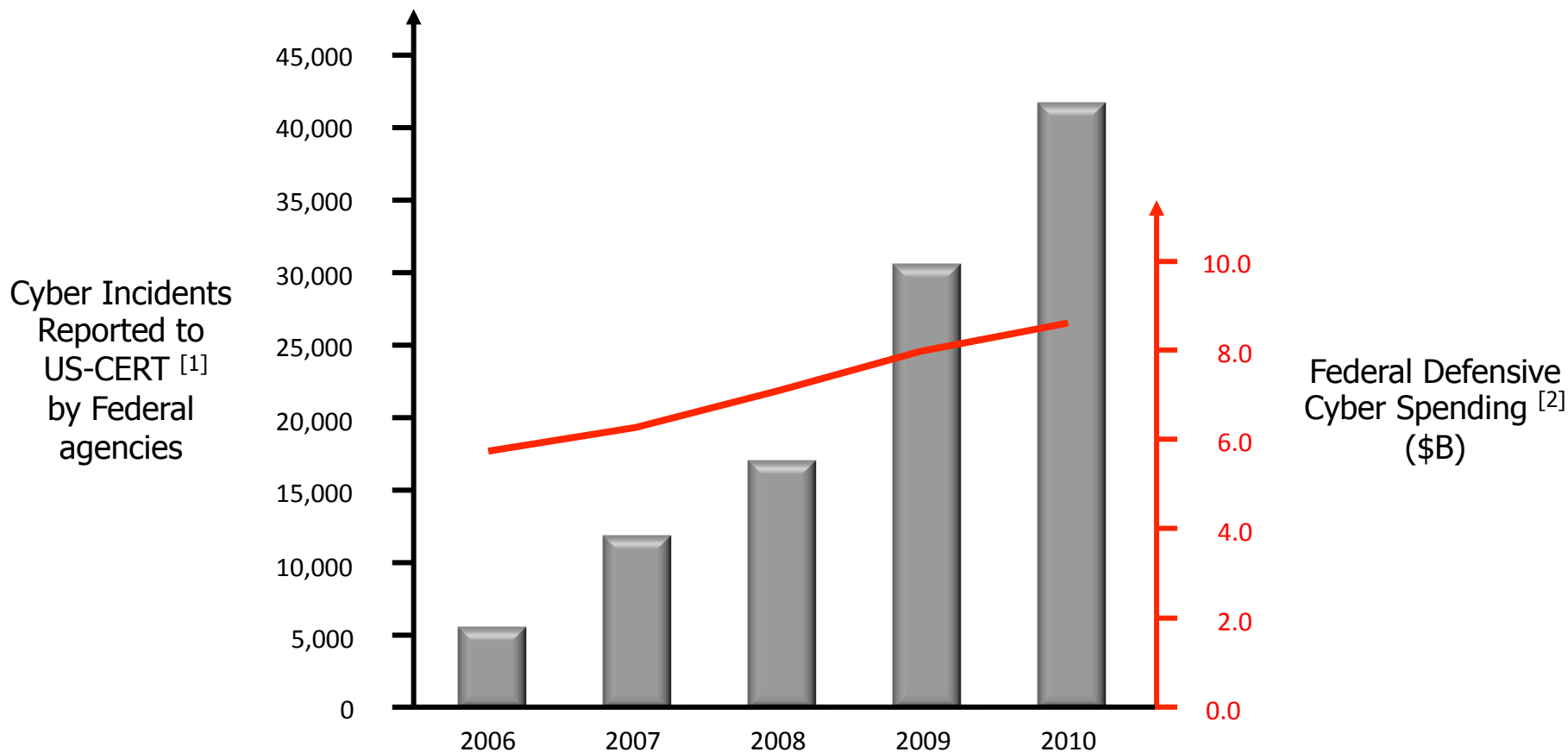


False speedometer reading  
Note that the car is in park...

[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.



## Ground truth...



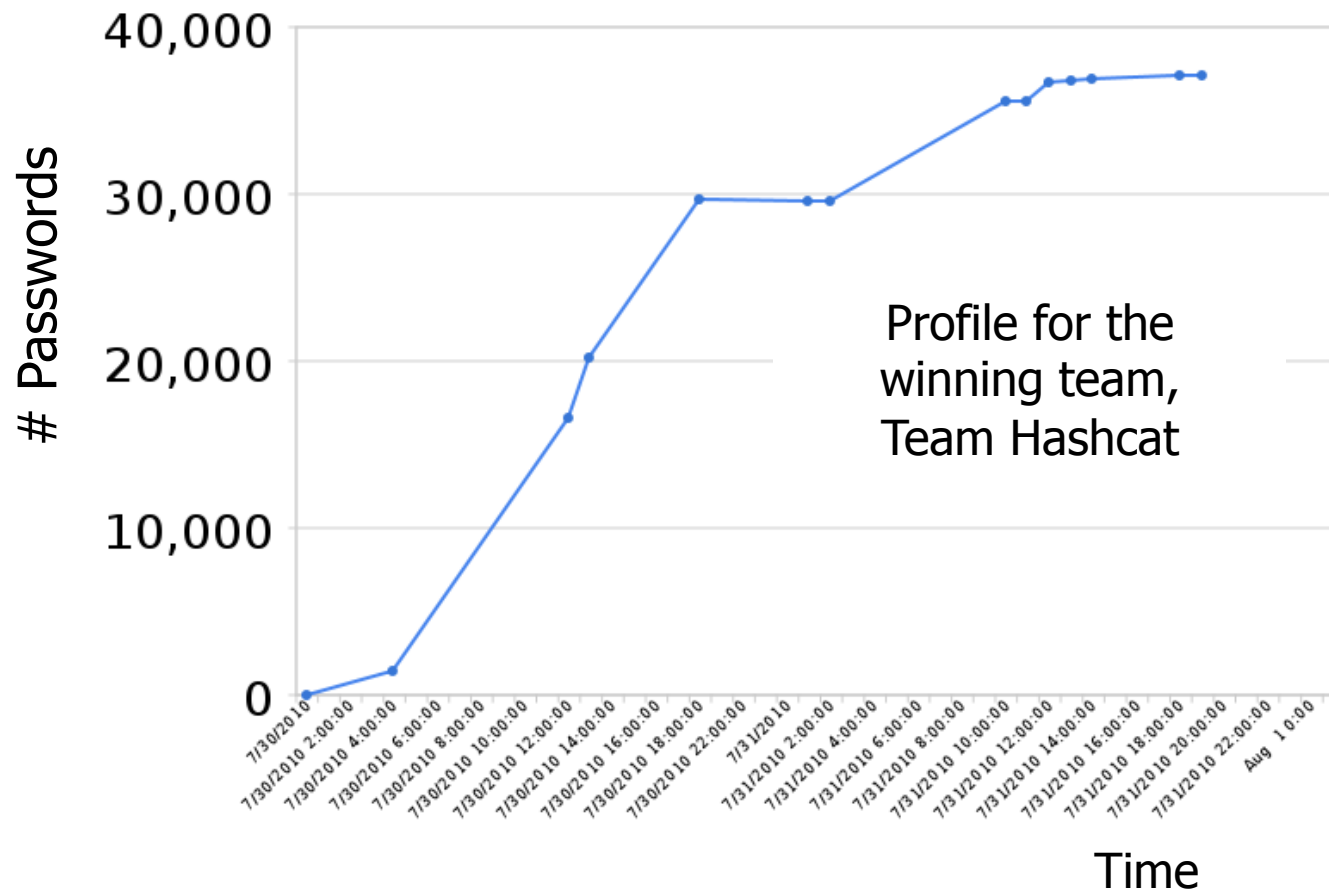
Federal Cyber Incidents and Defensive Cyber Spending  
fiscal years 2006 – 2010

- [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



## 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 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:

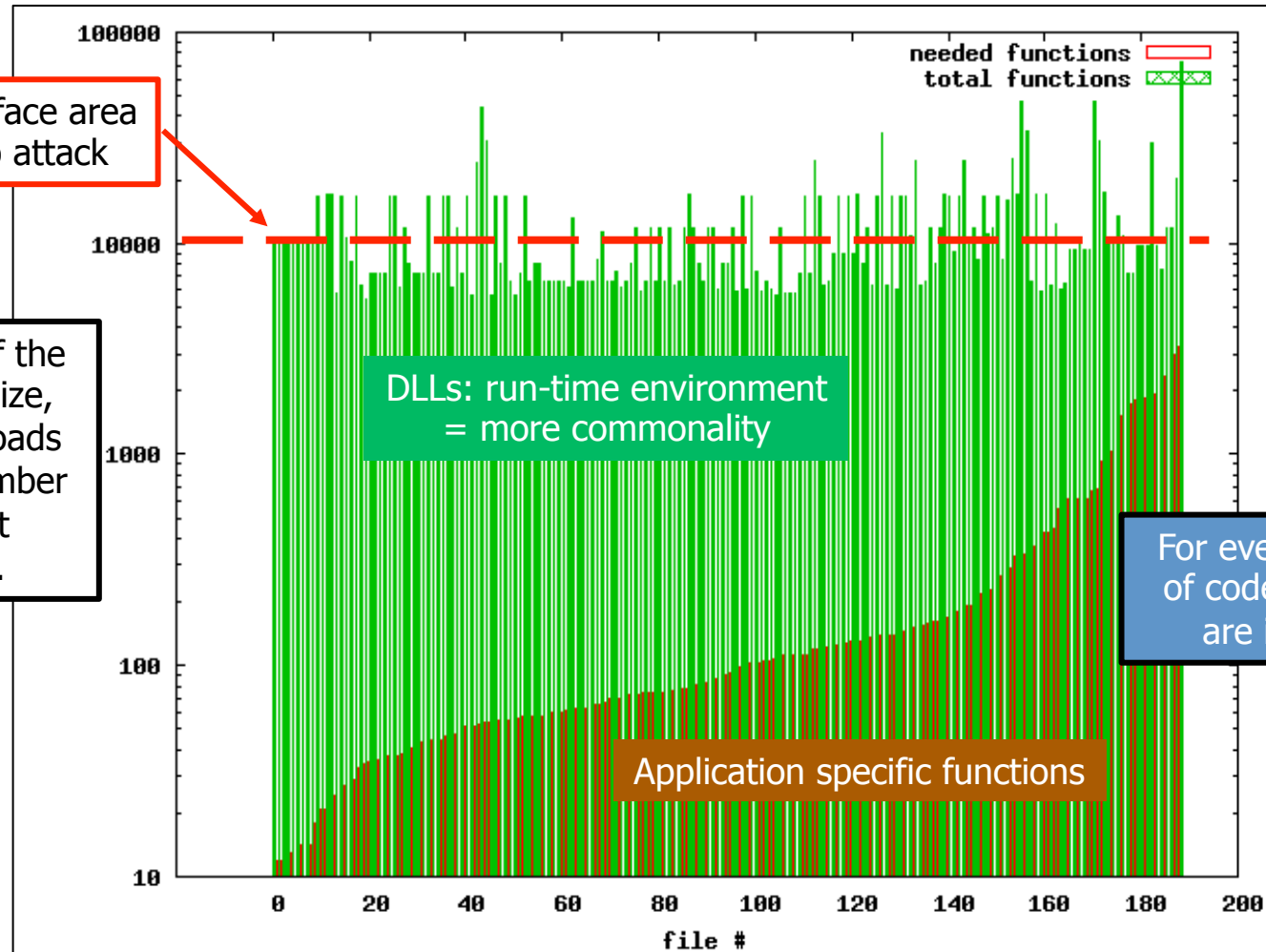
Vendor Replied – Fix in development

Awaiting Vendor Reply/Confirmation

Awaiting CC/S/A use validation



These layers increase the attack surface...





# We amplify the effect by mandating uniform architectures



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

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.

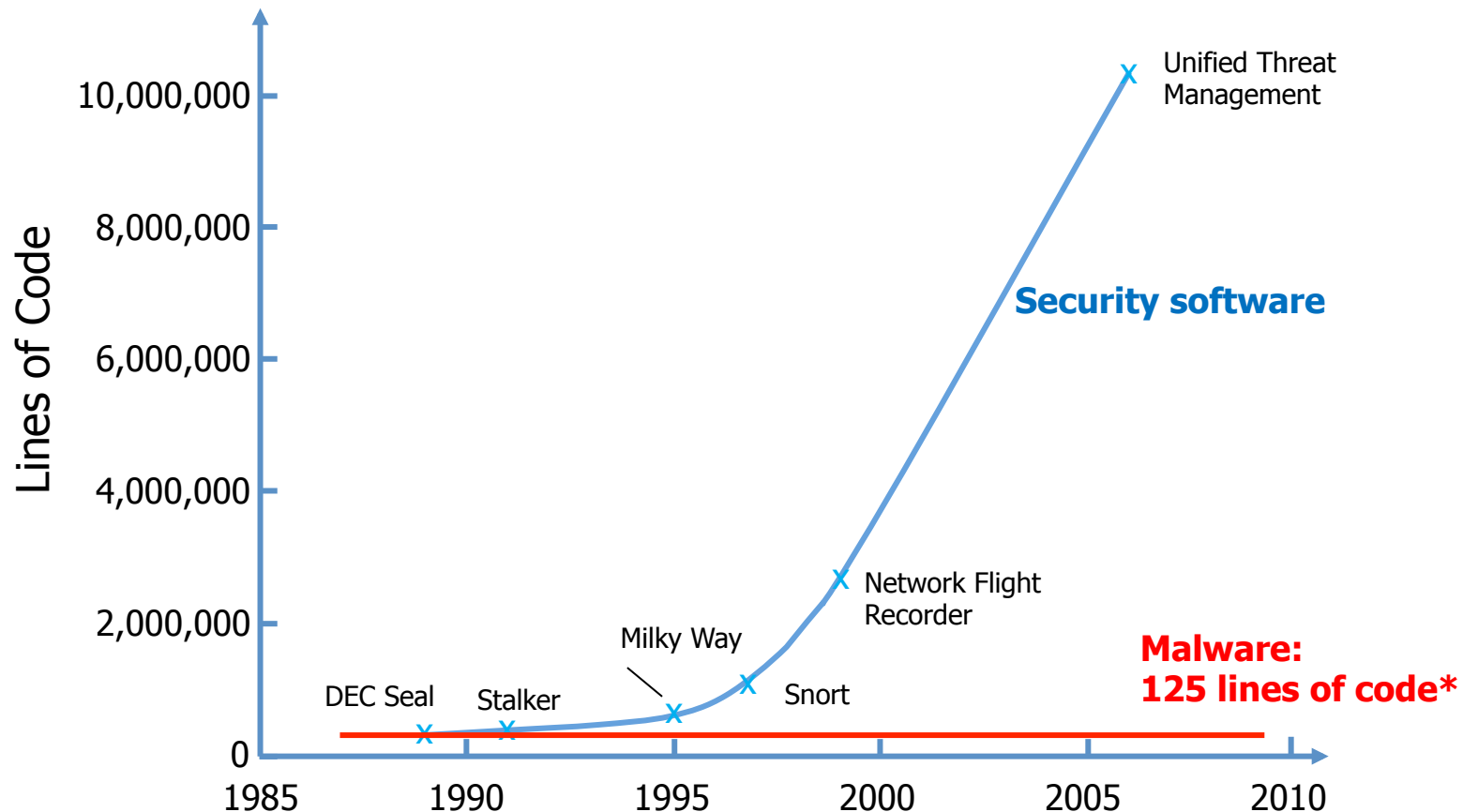
DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista™ operating system, and to deploy standard secure desk tops for Windows XP™. Information is more secure, overall network performance is improved, and overall o

Agencies with these op  
must adopt these standa  
requested to submit their  
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).



# We are divergent with the threat...



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



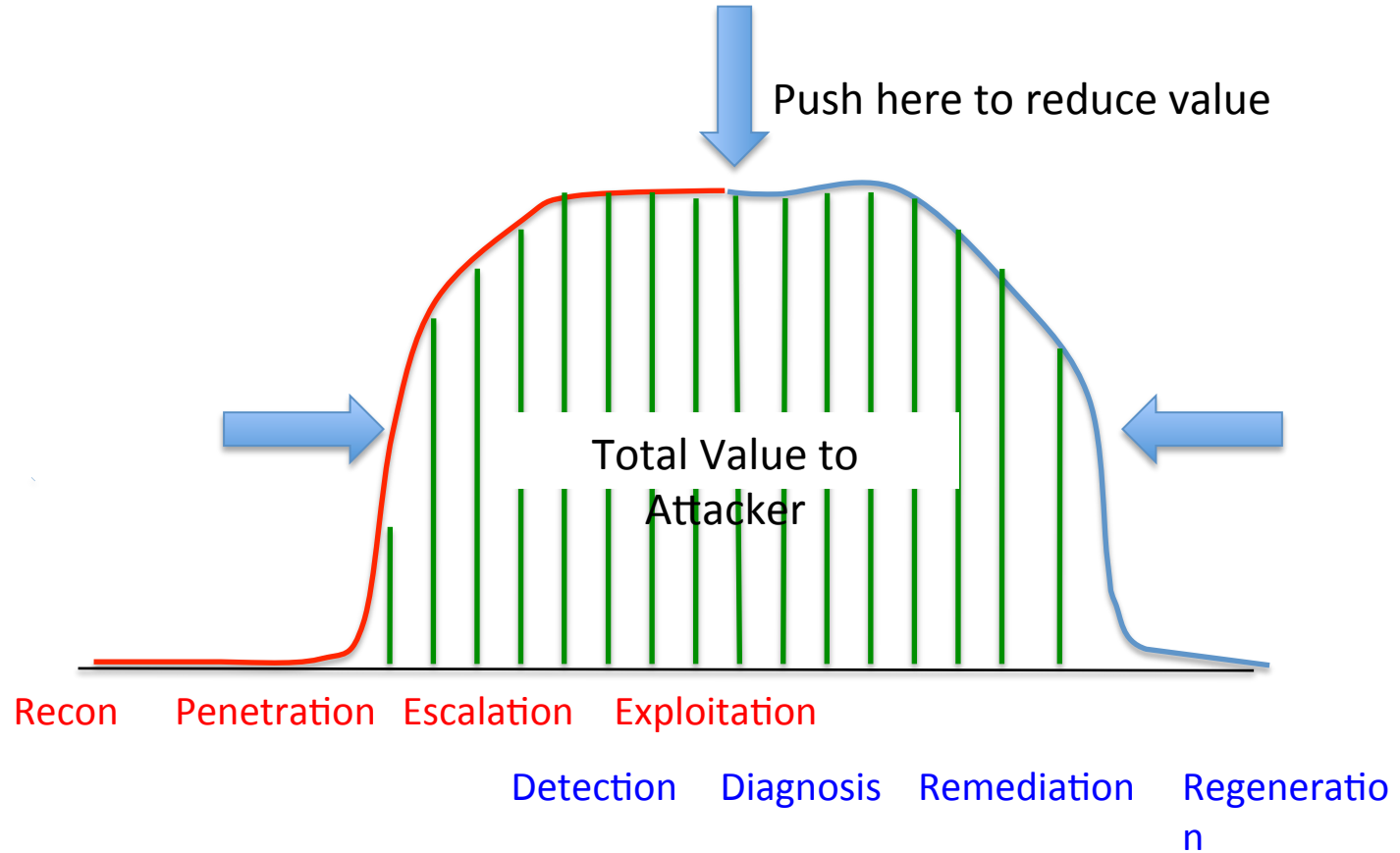
The US approach to cyber security is dominated by a strategy that layers security on to a uniform but insecure architecture.

---

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

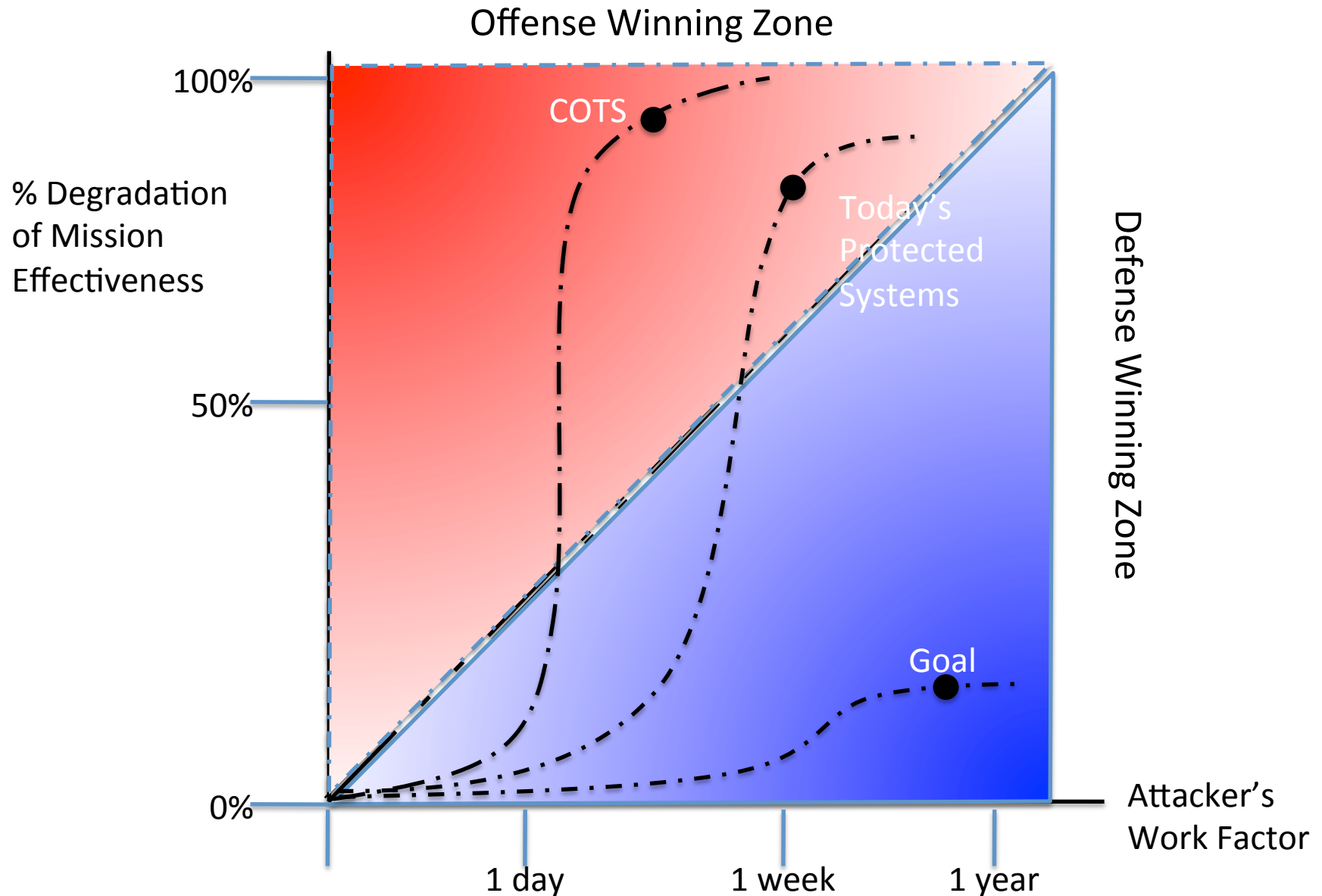


# Total Value to the Attacker





# Economic Tradeoff: Workfactor & Degradation





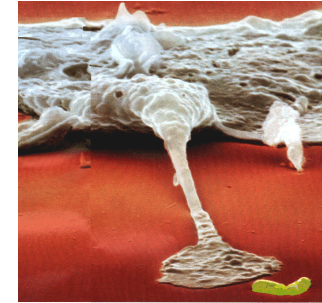
# My Thesis

---

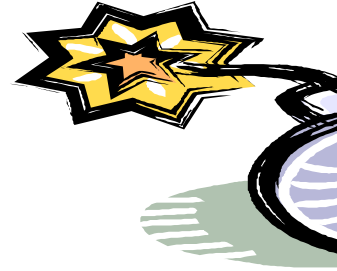
1. We are pursuing a losing strategy that is not convergent with the threat
2. We are in trouble because hosts are artificially vulnerable
3. This is true because of reasonable engineering decisions made in a different context
4. We need to go back to first principles and rebuild for both impenetrability and resilience
5. Biology offers many lessons and inspirations



# Biology and Computation: Two Design Styles



| Computation                                                        | Biological                                                                  |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Near Perfect Components                                            | Fallible components                                                         |
| Core design formed in era of scarcity                              | Abundance of resources                                                      |
| Core design formed in isolated environment                         | Evolution in ecosystem of predators and parasites                           |
| Evolutionary pressure from market: price, performance and features | Evolutionary pressure from ecosystem: survivability                         |
| Self-regulation and adaptation rarely considered. Runs open-loop.  | Self-regulation and adaptation are core mechanisms. Closed loop control.    |
| No enterprise-wide survivability mechanisms                        | Diversity for population survival<br>Public-health systems in human society |

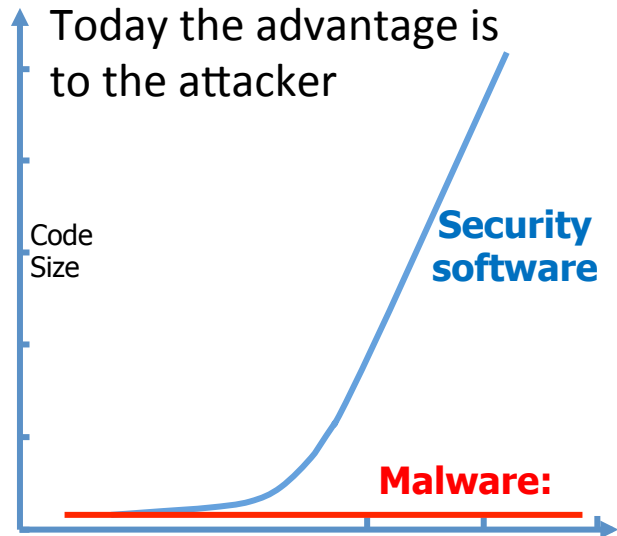


# CRASH

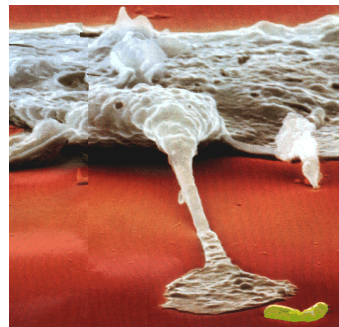
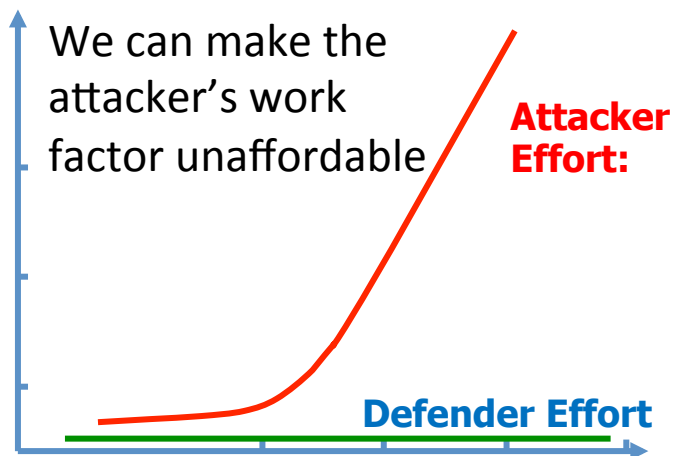
---



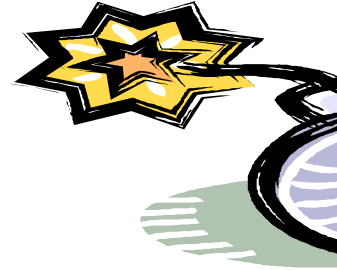
# Today's Designs Are Not Convergent with The Threat



- Today's practice reflects a fortress mentality
- We erect perimeter protections
- And when they are breached, we patch and pray



- Instead we should learn from biology how to design secure, adaptive and resilient systems.



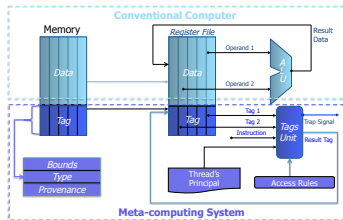
## CRASH

---

# Innate Immunity: Complete Mediation Through Hardware Enforcement



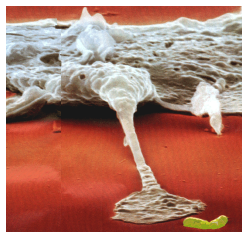
# CRASH & MRC apply biological principles



## **Systems are easily penetrated**

### **Innate Immunity:**

- New hardware architectures
- New operating system
- New programming tools, languages & formal methods
- Eliminate all common technical vulnerabilities



## **Cleanup is too costly and unpredictable**

### **Adaptive Immunity Middleware:**

- Isolate and monitor behavior
- Diagnose and find root causes of vulnerabilities
- Support rollback and replay to quickly adapt & reconfigure
- Generate patches to fix problem once and for all



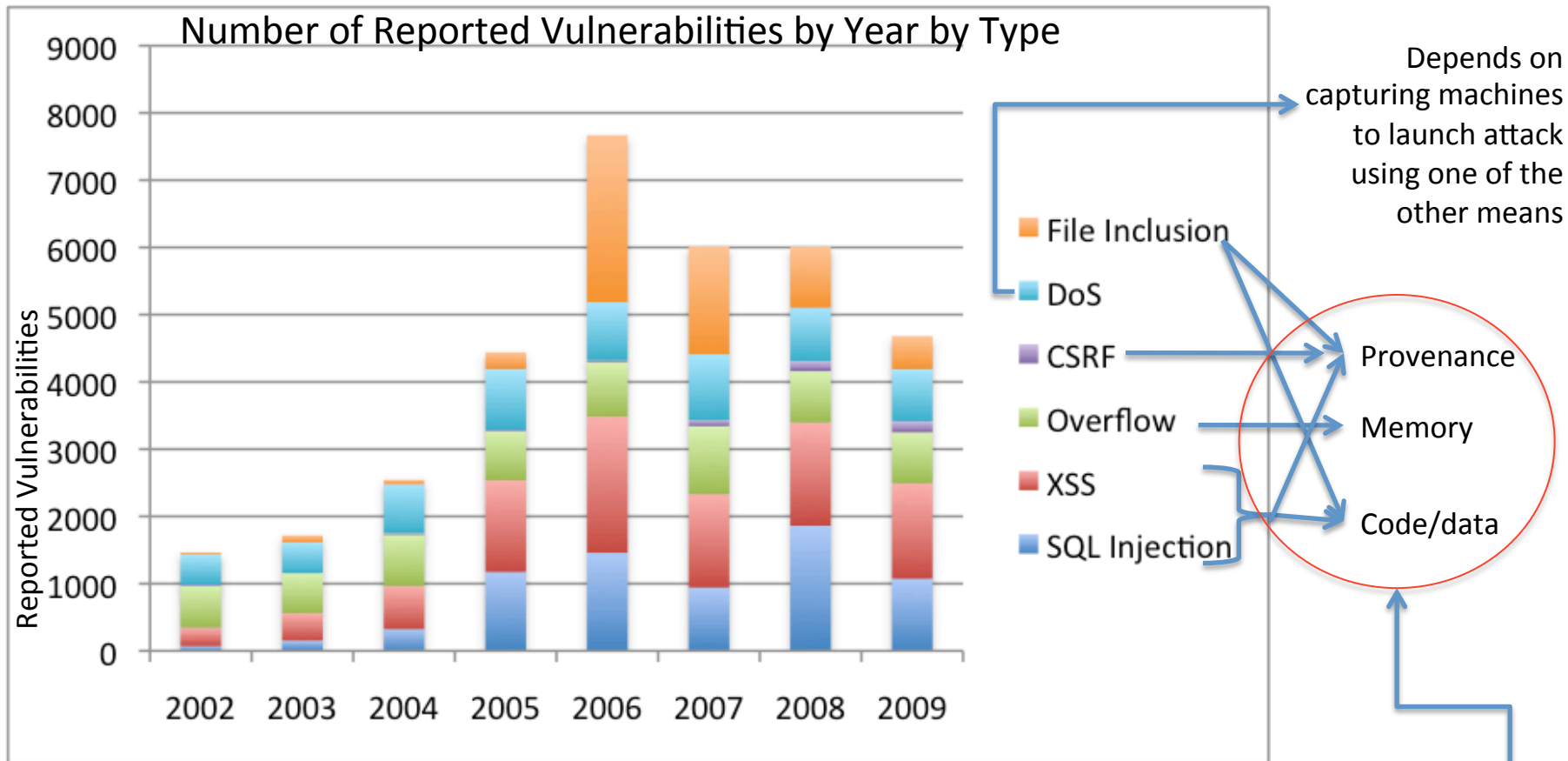
## **If one machine can be penetrated, they all can** **Static systems are easy to attack**

### **Diversity techniques:**

- Make each system unique
- Make each system change over time
- Raise work factor of attacker for each system
- Preserve manageability and usability



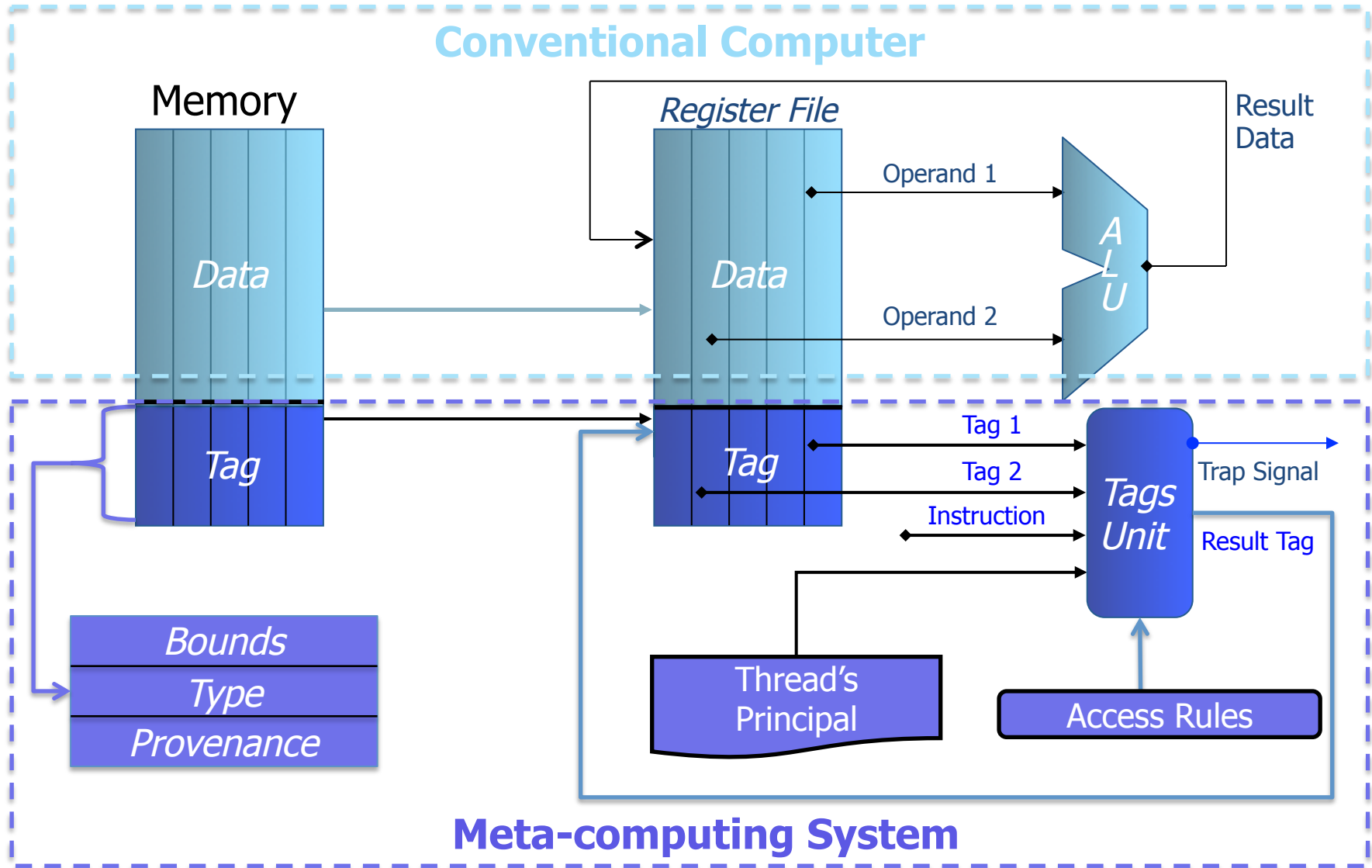
# Almost all current technical vulnerabilities are manifestations of a few root causes

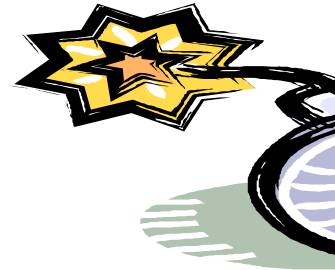


The innate system only has to protect these very few key semantic properties



# "Meta-Computing" prevent code injection, memory corruption and information flow violations





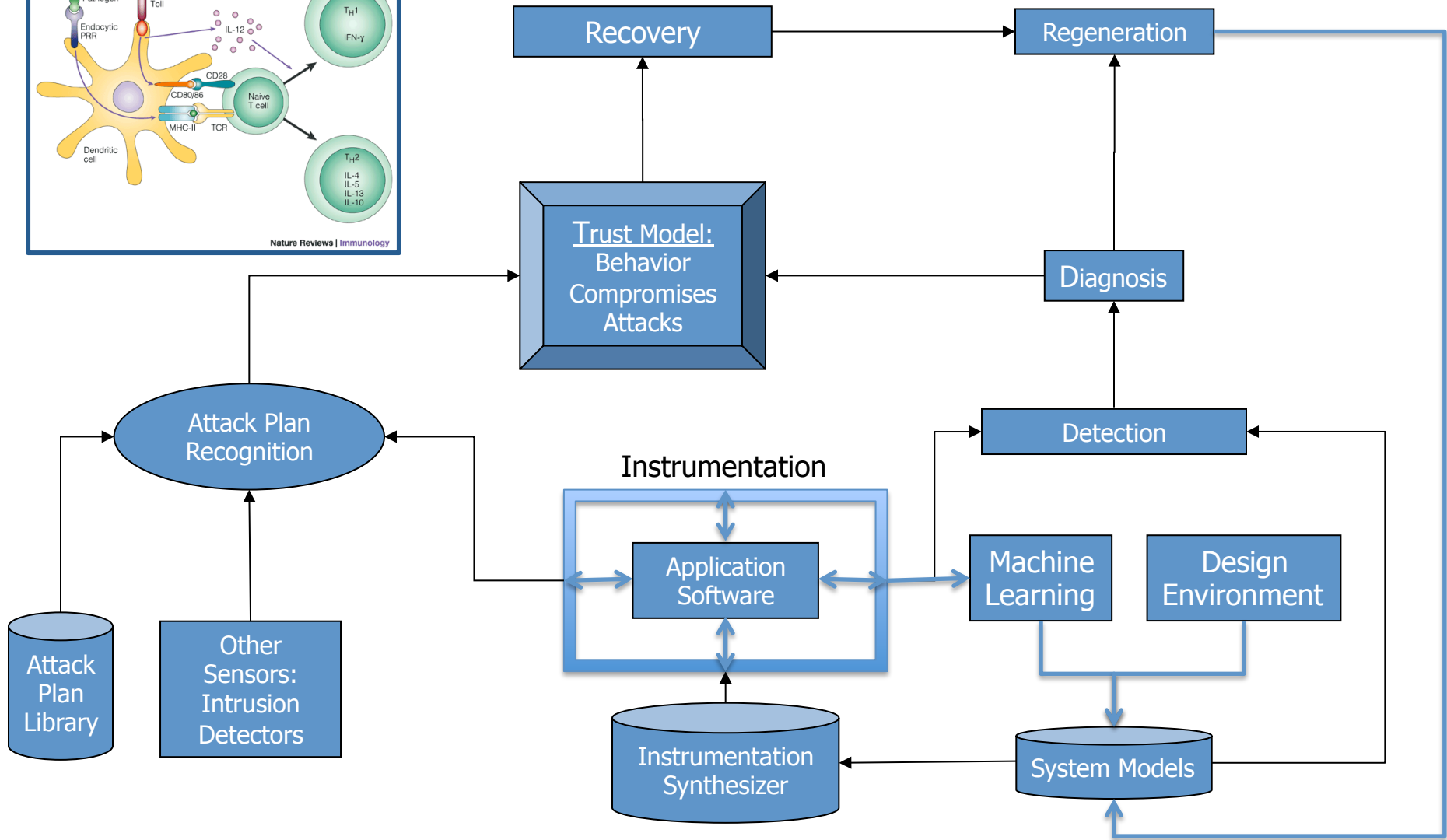
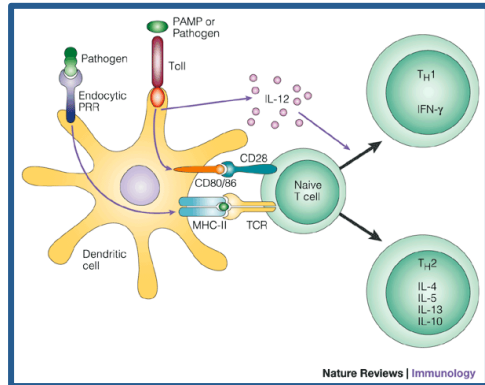
## CRASH

---

# Adaptive Immunity: Middleware for Diagnosis & Repair



# Software that detects, diagnoses and recovers from attacks and that patches its own bugs



UNCLASSIFIED

DISTRIBUTION F - Further dissemination only as directed by DARPA Public Release Center or higher DoD authority

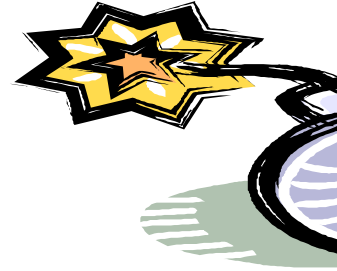


# Evolutionary Programming for Patch Generation

Automatically Finding Patches – Stephanie Forrest U New Mexico

| Program            | Lines of Code | Path Length | Program Description | Vulnerability                  |
|--------------------|---------------|-------------|---------------------|--------------------------------|
| nullhttp           | 5575          | 768         | webserver           | remote heap overflow           |
| openldap io.c      | 6519          | 25          | directory protocol  | non-overflow denial-of-service |
| lighttpd fastcgi.c | 13984         | 136         | webserver           | remote heap overflow           |
| atris              | 21553         | 34          | graphical game      | buffer overflow                |
| php string.c       | 26044         | 52          | scripting language  | integer overflow               |
| wu-ftpd            | 35109         | 149         | FTP server          | format string                  |
| TOTAL              | 108784        | 1164        |                     |                                |

Patched 65 out of 105 Bugs at an Average cost of \$8 per patch



CRASH

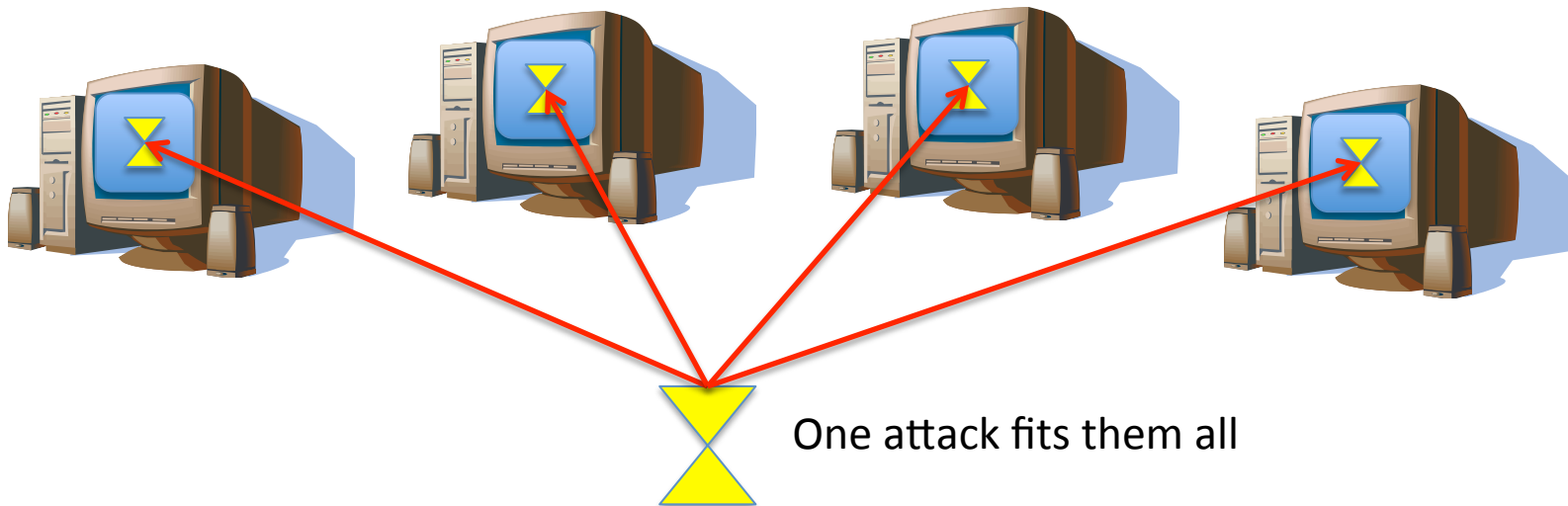
---

Eliminating Monoculture



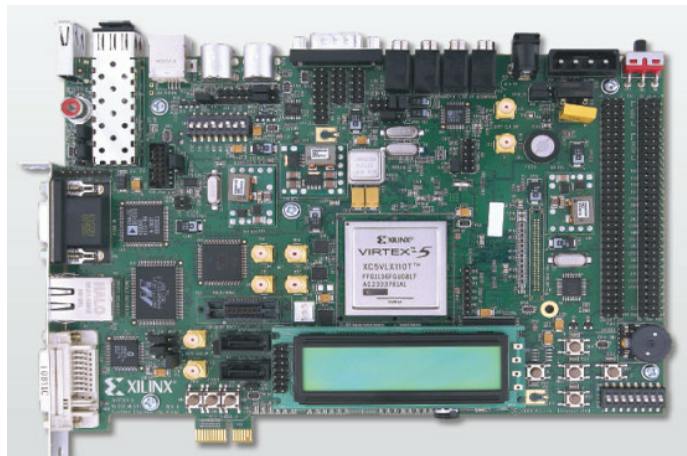
## Monocultures are not survivable

- The attacker's work factor is proportional to Entropy
  - When all systems are the same, a single attack disables them all
  - When a single system never changes, the same attack will work repeatedly
- We currently have a computational monoculture.





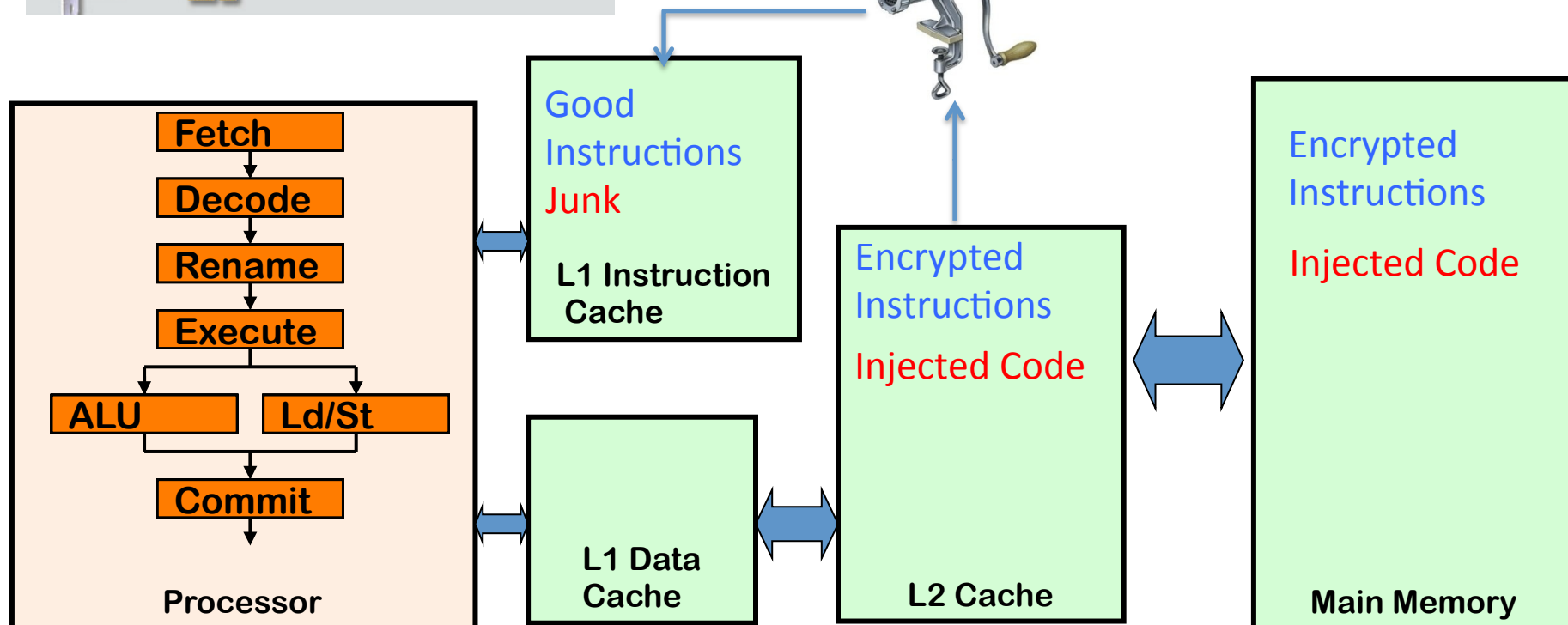
# Instruction Set Randomization eliminates code injection



OpenSPARC T1 Board:

- Boots Linux
- Low energy/power consumption
- Low latency
- Strong encryption

Simha Sethumadhavan - Columbia



UNCLASSIFIED

Approved for public release; distribution is unlimited.



# Multi-compiler produces millions of functionally identical but distinct binaries

existing approach: all users run identical binaries, all susceptible to same exploit

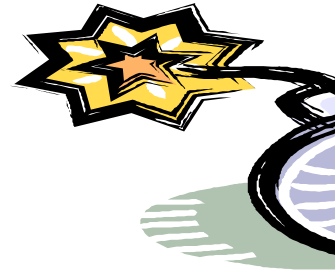


new approach: different users run different binaries, cost to attacker rises dramatically



Michael Franz – UC Irvine

- Front end compilation identical for all copies
- Make arbitrary but equivalent choices in the backend for each copy
  - Noop insertion
  - Equivalent instruction sequences
  - Memory layout
- Support rapid recompilation “in the cloud” for large scale deployment



MRC

---

## Employing Collective Defense in The Cloud



# Clouds On The Horizon

The drive to cloud computing:

- The White House released a 25-point plan in December for reforming government IT, and it included a **requirement that agencies adopt a cloud-first policy** for new IT deployments
- *“...we have found it is easier to secure the cloud... coming up with a defensible system is important and cloud computing is one way to help make that possible. By shifting to a cloud architecture, the US would save money and be better placed to protect vital computer networks.”* (Gen Keith Alexander, Nov 7, 2011)

| Motivations                                                                              | Concerns                                                                                               |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Economic efficiency                                                                      | Monoculture<br>Added attack surface of hypervisor                                                      |
| Manageability of large scale data centers                                                | Concentration of hosts on high speed network with few internal barriers -> Vulnerability Amplification |
| Availability of “fungible computation” on demand. Use on demand vs. build to worst case. | “Fate sharing” among unrelated computations.                                                           |
| Centralization of data for common analytics                                              | Obvious target for adversary<br>Single point of failure                                                |



# Mission-oriented Resilient Clouds: Turning Liabilities into Assets

## **TODAY**

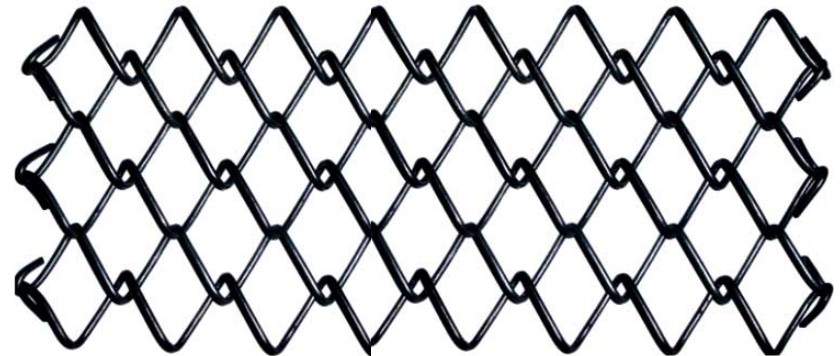
Each host Acts in isolation, making the enterprise weaker than the sum of its parts



- “Box” oriented
- Vulnerable components
- Static
- Shared vulnerabilities
- Implicit trust within enclave amplifies vulnerabilities

## **RESILIENT CLOUDS**

Acting as a community makes the enterprise stronger than the sum of its parts



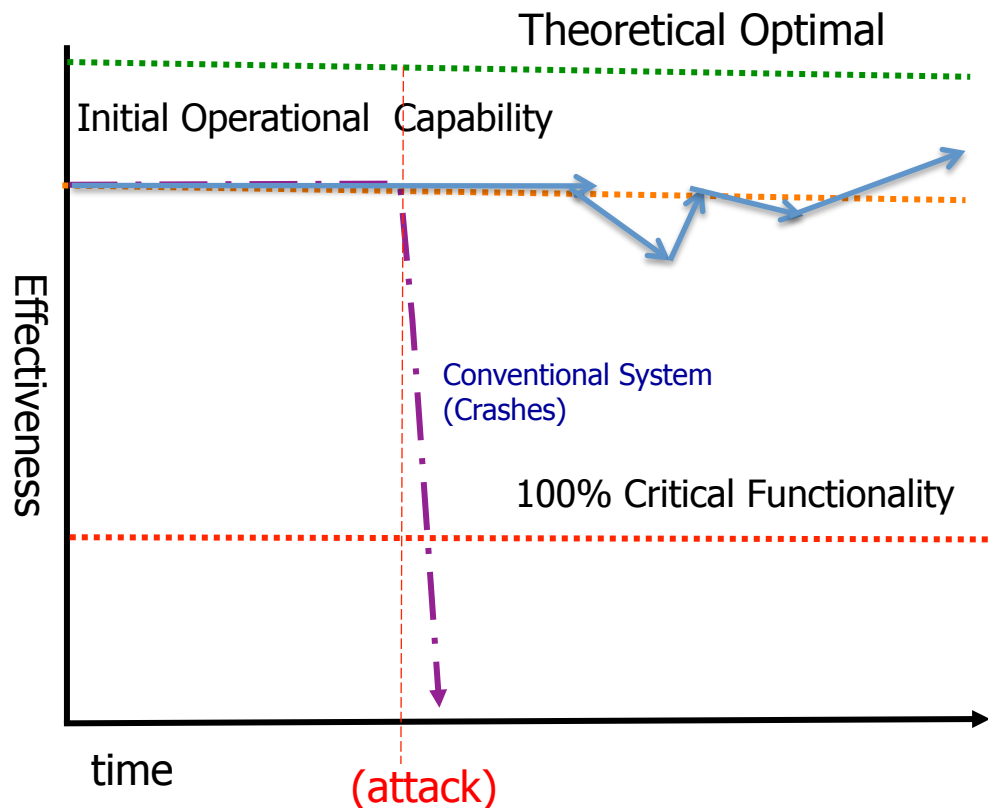
- Components from CRASH program
- Moving target
- Resilience through diversity
- Collective defense & diagnosis across enclave dampens vulnerabilities



# Mission-oriented Resilient Clouds

**Objective:** Sustain mission effectiveness. Different mission components have different security and performance needs and will make different trade-offs at run-time.

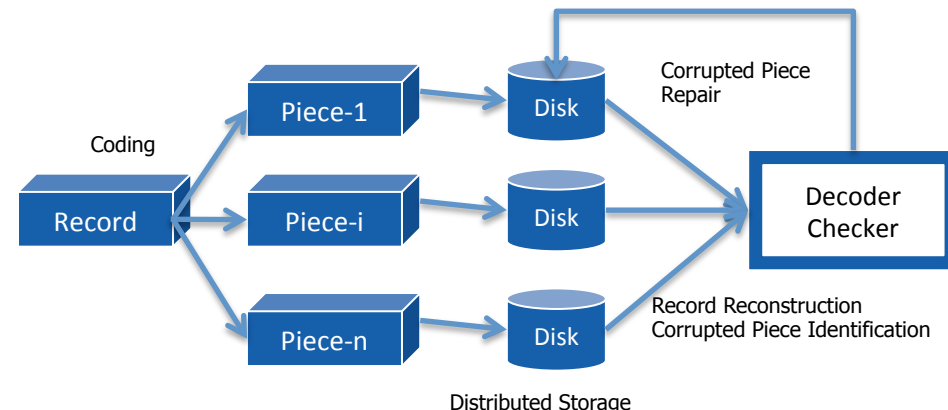
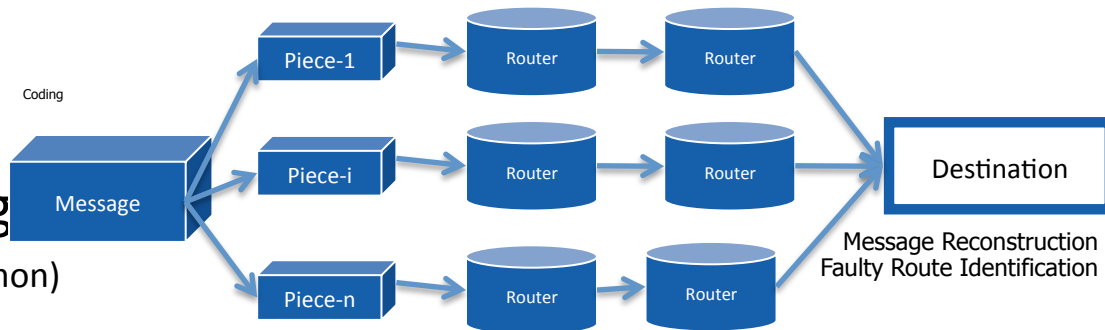
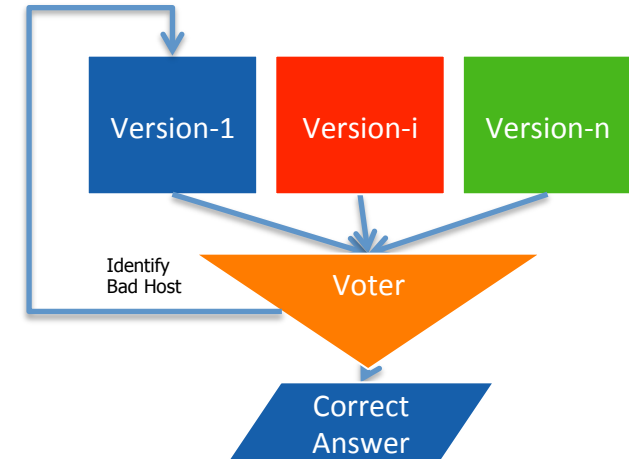
**Target:** Achieve at least 80% of optimal mission effectiveness while using at most 150% of the “base” resource requirements.





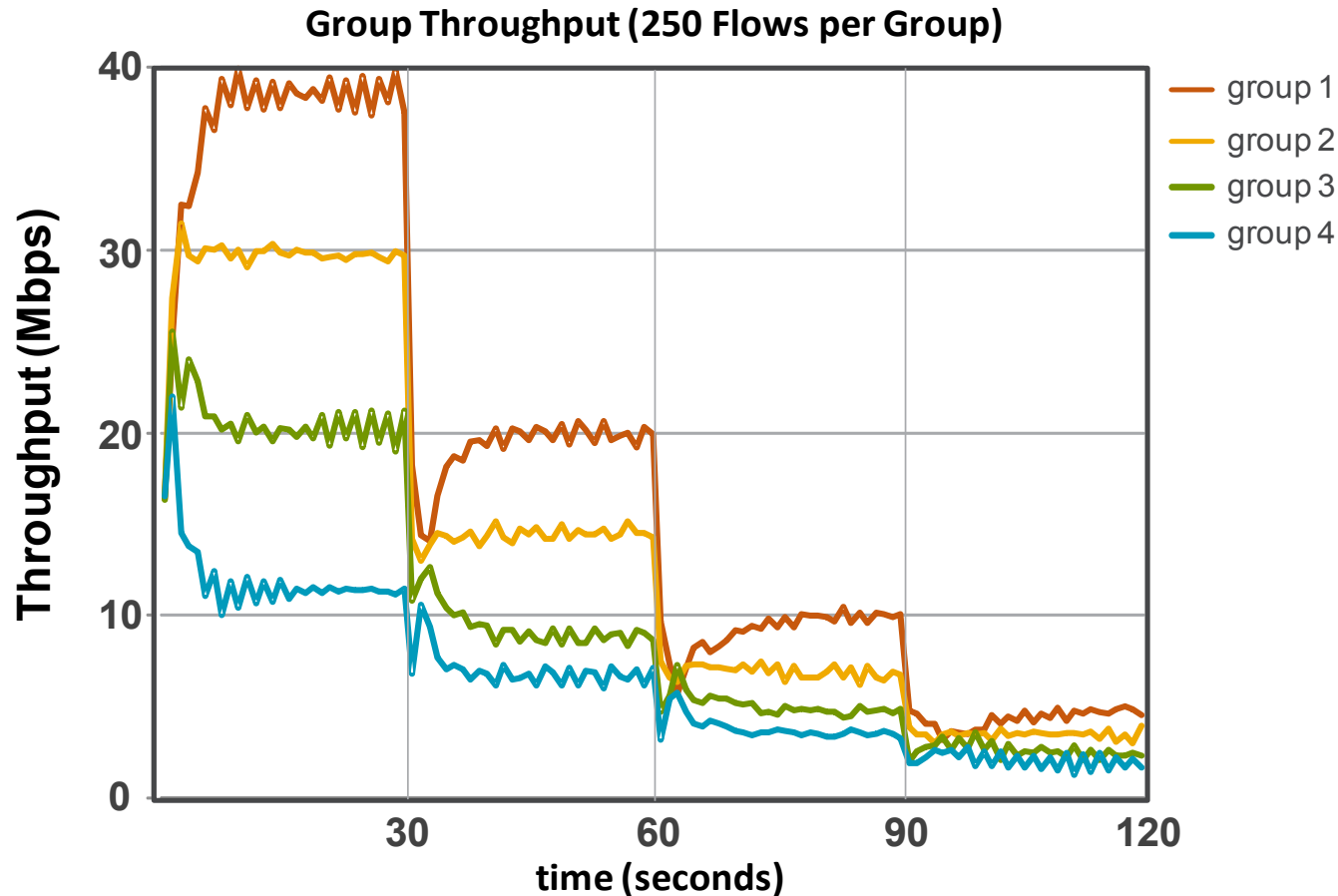
# Collective Defenses

- Scalable and Secure Consensus Protocols
  - Diversified hosts in consensus groups
  - Mixture of gossip, virtual synchrony, multicast protocols
  - Variety of Correct by Construction Algorithms (e.g. PAXOS)
- New CRASH and OpenFlow Based Routers
- Network provenance, “Introduction-Based” Routing
- Defensive Network Coding
  - Use of “M of N” codes (e.g. Reed-Solomon)
  - Pieces sent on separate paths
- Distributed Coded Storage
  - Records recoded using “M of N codes”
  - Pieces stored on separate servers





# Network Optimization - Nash Bargaining



- Bottleneck bandwidth halved every 30 seconds due to, e.g., DoS flooding attack
- Nash Bargaining rapidly adjusts bandwidth allocations to remain consistent with priorities

Stu Wagner - ACS



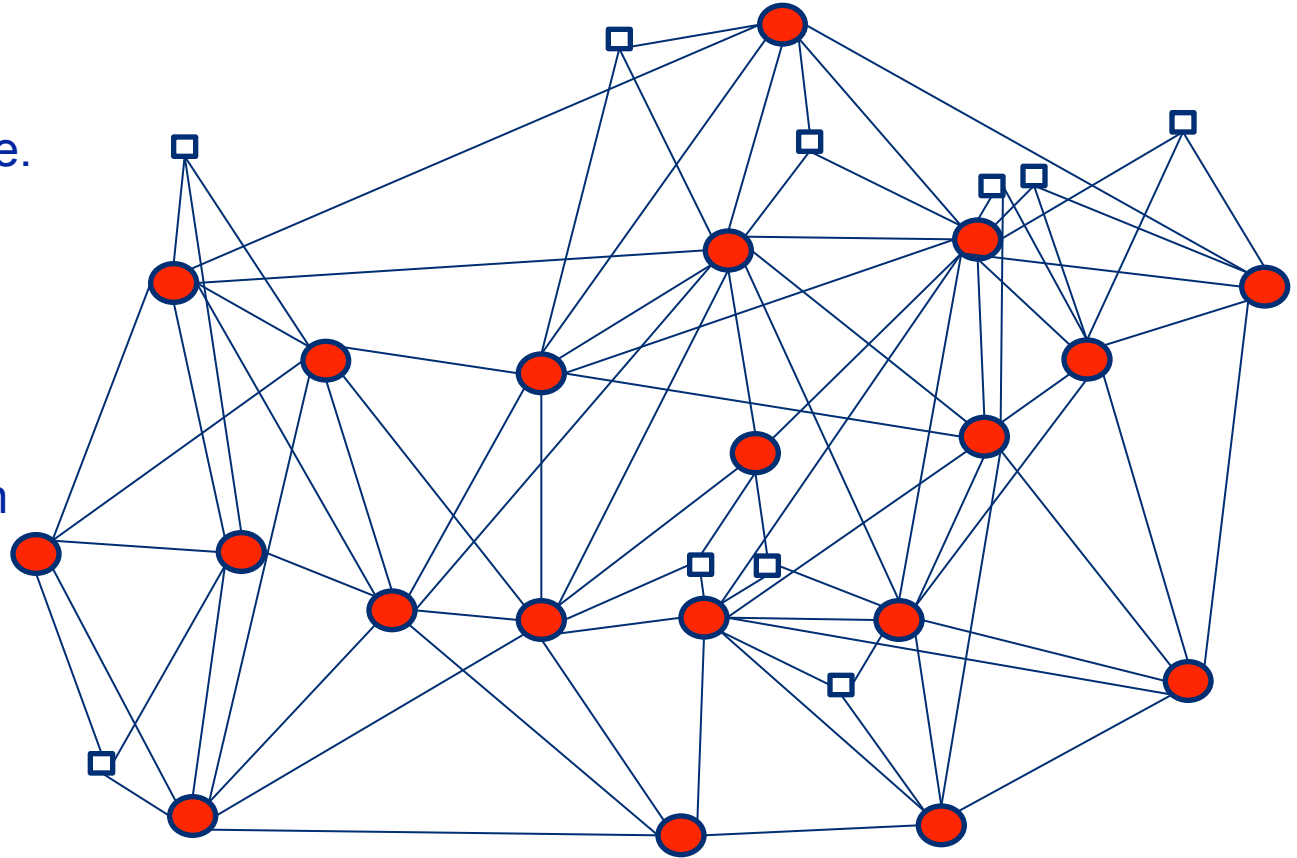
# Diversity can lead to Robustness

20 overlay nodes, 10 Clients

**Red version:** secure with 90% probability over a certain unit of time. No diversity.

Resulting system with optimal placement:

Communication between each pair of clients is available with probability 90% over the same unit of time





# Exploiting Three Diverse Versions

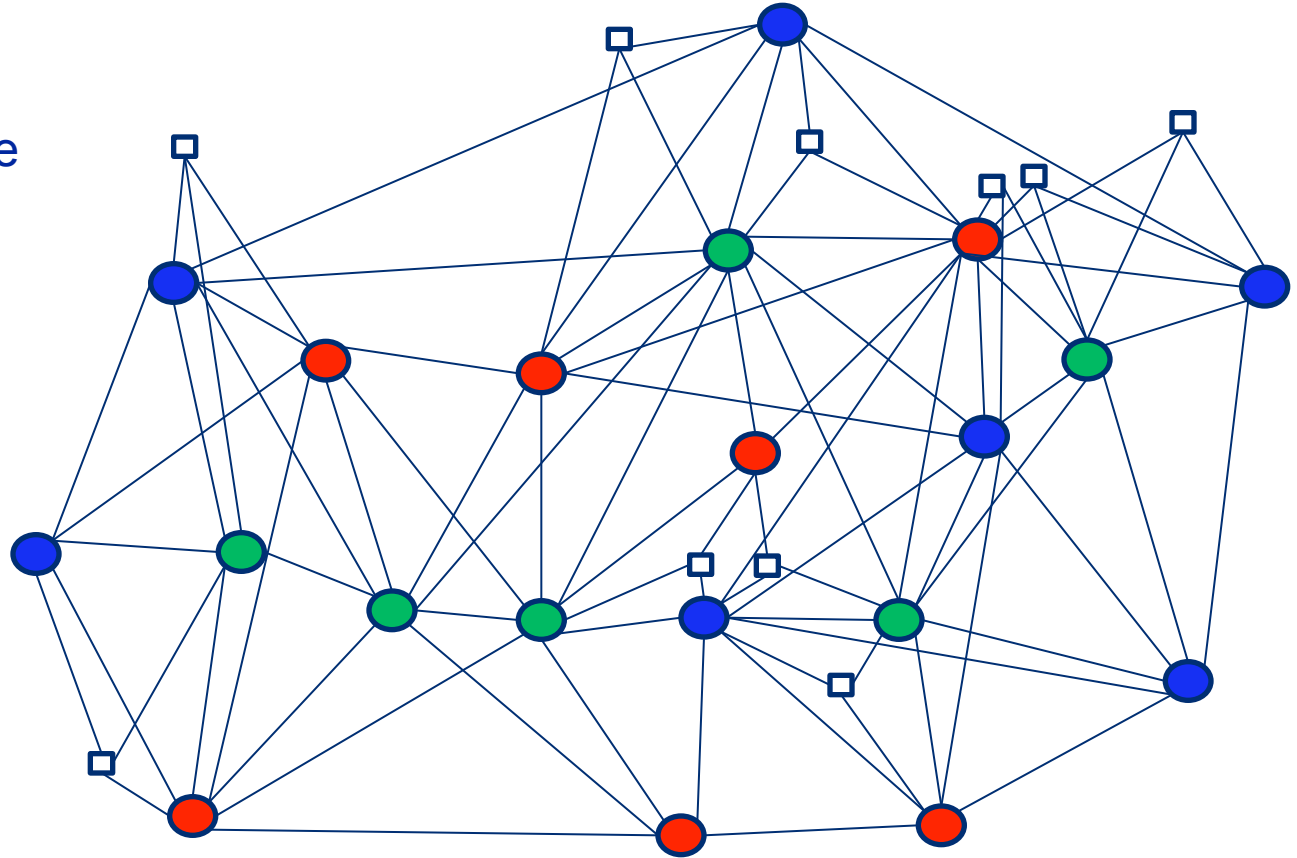
20 overlay nodes, 10 Clients

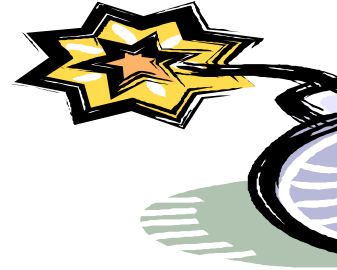
**Red version:** secure  
with 90% probability  
over a certain unit of time

**Blue version:** 85%

**Green version:** 80%

Resulting system with  
optimal placement:  
communication between  
each pair of clients  
is available with  
probability 99.7%  
over the same  
unit of time





# HACMS

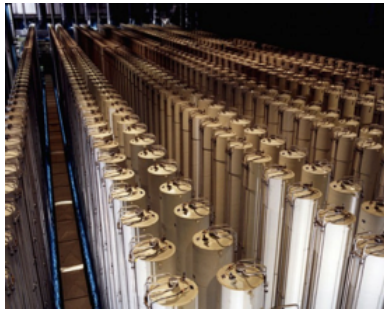
---

**Kathleen Fisher**



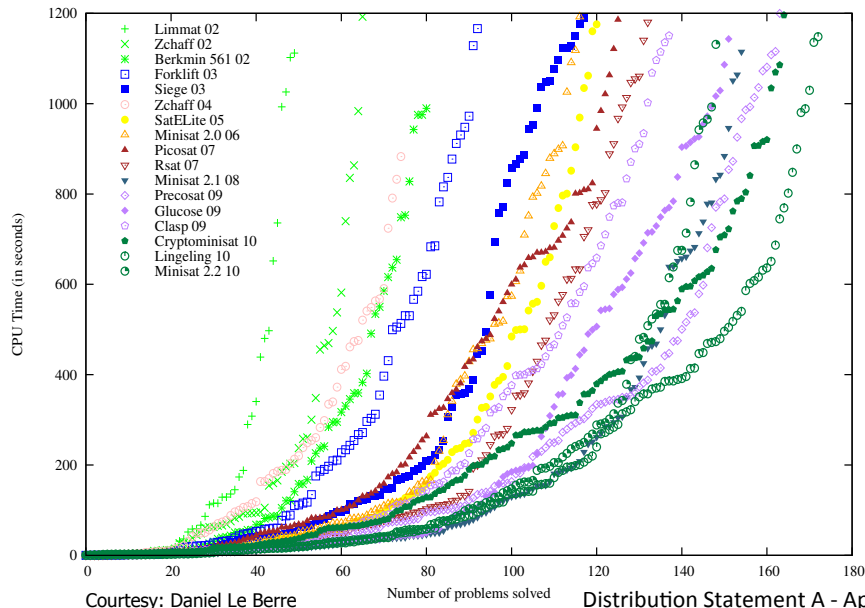
# HACMS: Program Overview

**Problem:** Networked embedded systems vulnerable to cyber attack.

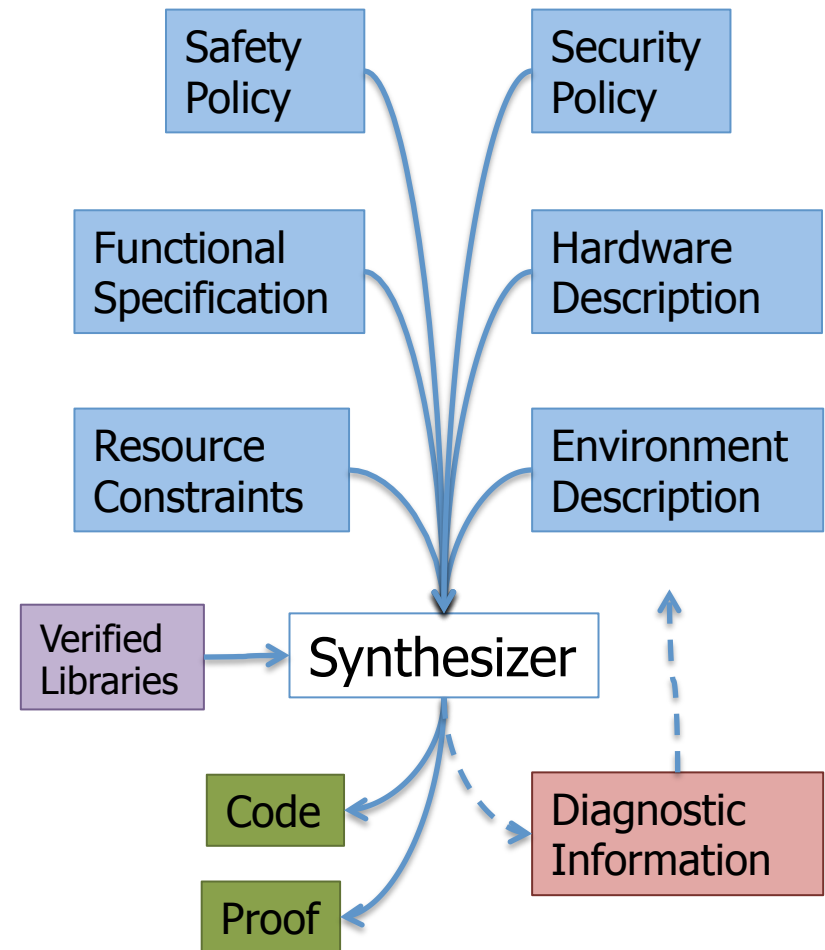


**Opportunity:** Speed of formal methods improved dramatically in past decade:

Results of the SAT competition/race winners on the SAT 2009 application benchmarks, 20mn timeout

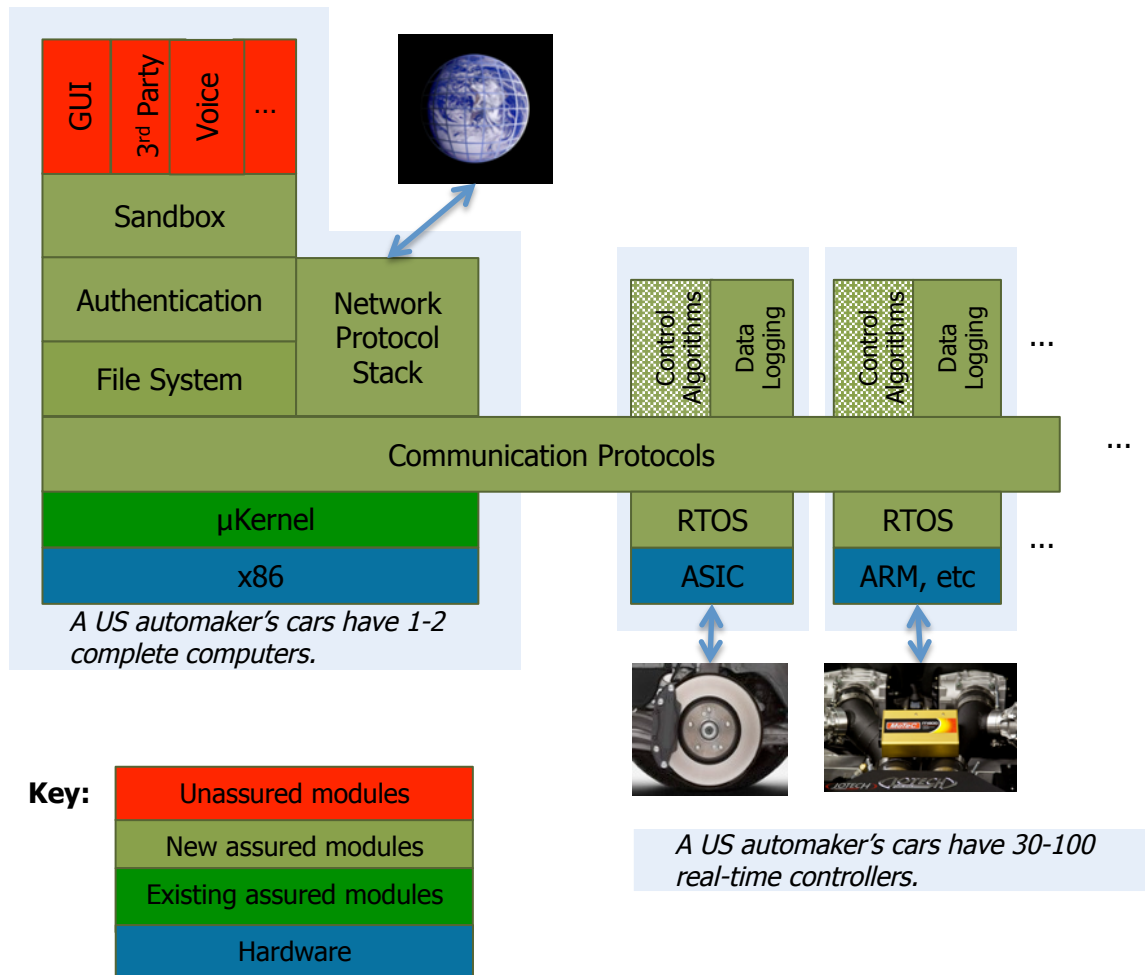


**Program:** Use formal methods to synthesize & verify high assurance vehicles





# High-Assurance Vehicle of the Future: Built from Synthesized Components



## Research Challenges

- Synthesis of attack-resilient control systems
- Synthesis of operating systems code
- Specification languages: function, environment, hardware, resources
- Composition
- Proof engineering
- Scaling
- Attack/fault response
- V&V of complete system
- Managing time: synchrony, asynchrony, concurrency

Focus on vehicles, but techniques should apply to other domains.



# HACMS Program Architecture

## 1. Military Vehicle Experts

**Boeing**  
Pilot-able Unmanned  
Little Bird Helicopter

**HRL\*/GM**  
GM SUV



## 2. Operating Systems

**NICTA**  
Synthesize OS  
components;  
Verified sel4 kernel;  
Verified RTOS

**SRI\*/UIUC**  
EF-SMT solvers;  
Synthesize monitors  
and wrappers

**Princeton\*/Yale/MIT**  
Build and verify in CoQ  
vehicle-control OS;  
compCERT: concurrent;  
compositional  
integration of verified  
components

**Kestrel\***  
Synthesize protocols:  
refinement of high-  
level spec to low-level  
implementations

## 3. Control Systems

**Galois**  
Embedded DSL;  
Synthesize and verify  
control system code

**SRI\***  
Synthetic sensors;  
Synthesis for  
controllers of hybrid  
systems

**CMU\*/Drexel/  
SpiralGen/UIUC**  
Map high-level  
spec into low-level  
C code; Extend  
Spiral for hybrid  
systems

**UPenn\*/UCLA**  
Synthesize  
attack-resilient  
control systems

## 4. Research Integration

**RC\*/U. Minn**  
Compositional  
verification;  
Integrated workbench

**SRI\***  
Lazy Composition;  
Evidential Tool Bus &  
Kernel of Truth;  
Vehicle Integration

## 5. Red Team

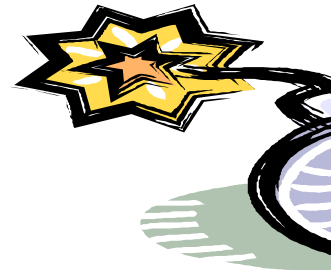
**DRAPER\*/AIS/  
U. Oxford**  
Traditional  
penetration  
testing; novel  
formal methods  
approach

### **Program Timeline:**

- Industry Day: Feb 21
- BAA Release: Feb 23
- Proposals Due: April 10
- Notifications: May 9-11
- Kick-Off: Aug 8-10
- Three 18-month phases

### **Performers:**

- 8 Primes (\*)
- 22 Total



# Active Authentication

---

**Richard Guidorizzi**



## DARPA's Active Authentication Program

---

A yellow sticky note with handwritten text in blue ink. The text lists five examples of passwords: 'Finweb = Jane123', 'DTS = 123Jane', 'PKI = JaneA123', 'DiskCrypt = Jane123A', and 'Gmail = Jane123A'.

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

Passwords will never work as a truly secure identification solution because they:

1. Provide no information about the holder, they are simply data known
2. Are intended as a proxy for person at the keyboard and proxies can be faked



---

How do we move from proxies for you to the actual  
you?

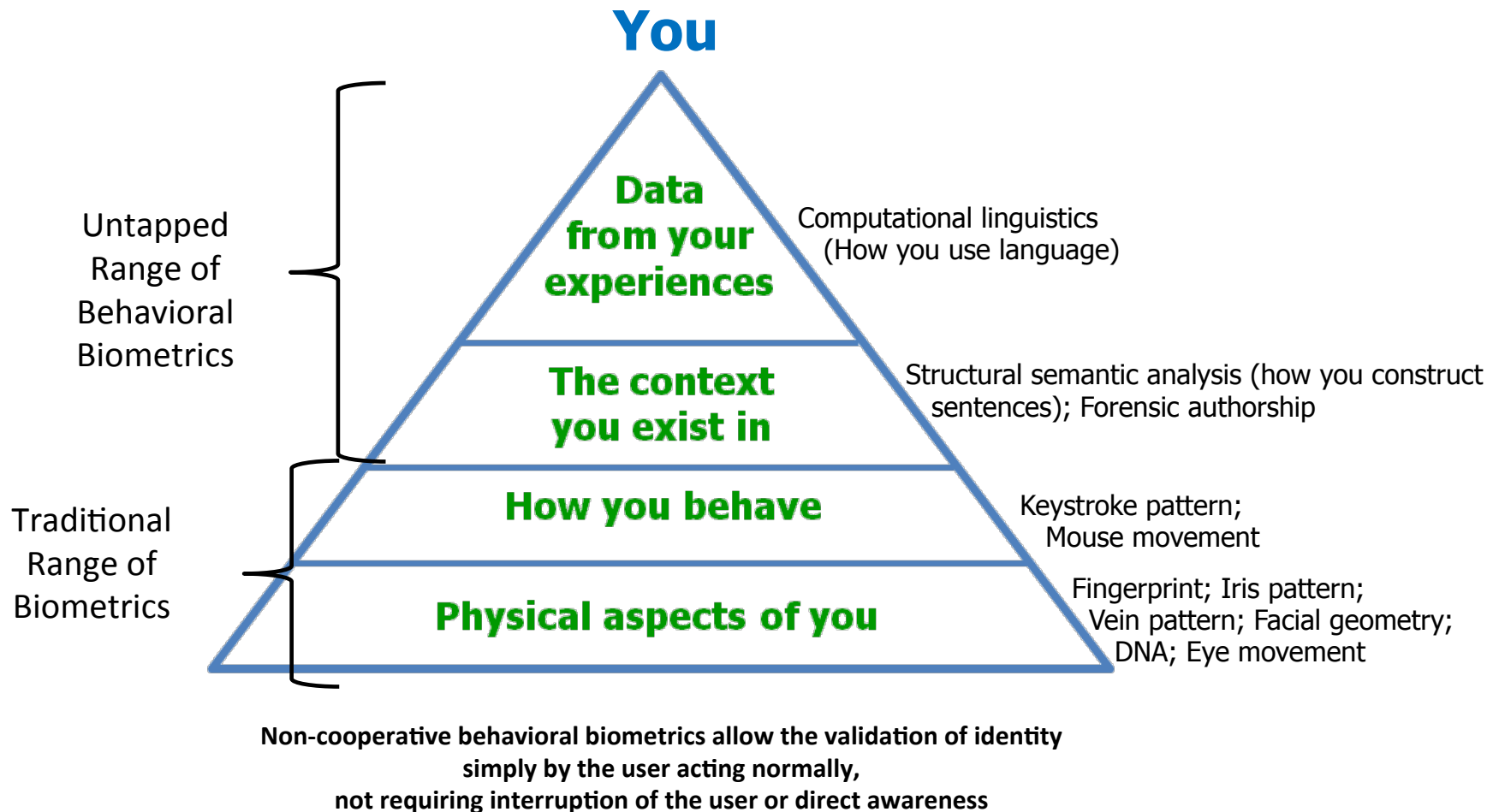
- Non-Cooperative Biometric don't require the  
deployment of sensors

We can turn data (biometric features) into information  
(validation of identity) without the direct cooperation of  
the user



# The Active Authentication Program

A continuous authentication solution that takes the data available on a DoD computer system and makes an informed decision on the identity of the user of the computer





# What new biometrics are we working on in the Active Authentication Program?

## **Neuro-cognitive patterns – Naval Post Graduate School**

Developing digital “cognitive fingerprints” from various biometric sources; potentially developing a framework for identification of other behavioral biometrics. Also able to provide behavioral forensics of the user to ascertain shifts in thought process, social programming, belief structure, etc.

## **User Search Patterns – Allure Security Technology, Inc**

Using the user’s patterns for searching for information on the computer, verified by high volumes of decoy document touches placed in the file system.

## **Keystroke and Mouse Dynamics – BehavioSec**

Enhancing keystroke & mouse behavioral biometrics with large scale user trials including research into the areas of continuous trust models & application usage patterns.

## **User Behavior Patterns as seen from the Operating System – Coveros**

Using traditional computer based IDS algorithms on user behavior (as seen in OS interactions) to determine when someone other than the authorized user is accessing the system.

## **Stylometry – Drexel University**

Using traditional stylometric methods to validate a user based on what they are typing. Also researching how to detect adversaries who attempt to impersonate users through mimicking typing methods.

## **Stylometry focused on Cognitive Processing Time –Iowa State University**

Using stylometric methods to validate the user based on natural pauses in the way they type.

## **Stylometry focused on Cognitive Rhythms – NYIT**

Using text productivity, pause, and revision behaviors to validate users based on how they type (includes content/language).

## **Covert Games - Southwest Research Institute**

Determine the user’s pattern of behavior by introducing patterned system aberrations that the user intuitively learns, i.e. hidden games in the computer interface.

## **Screen Interface – University of Maryland**

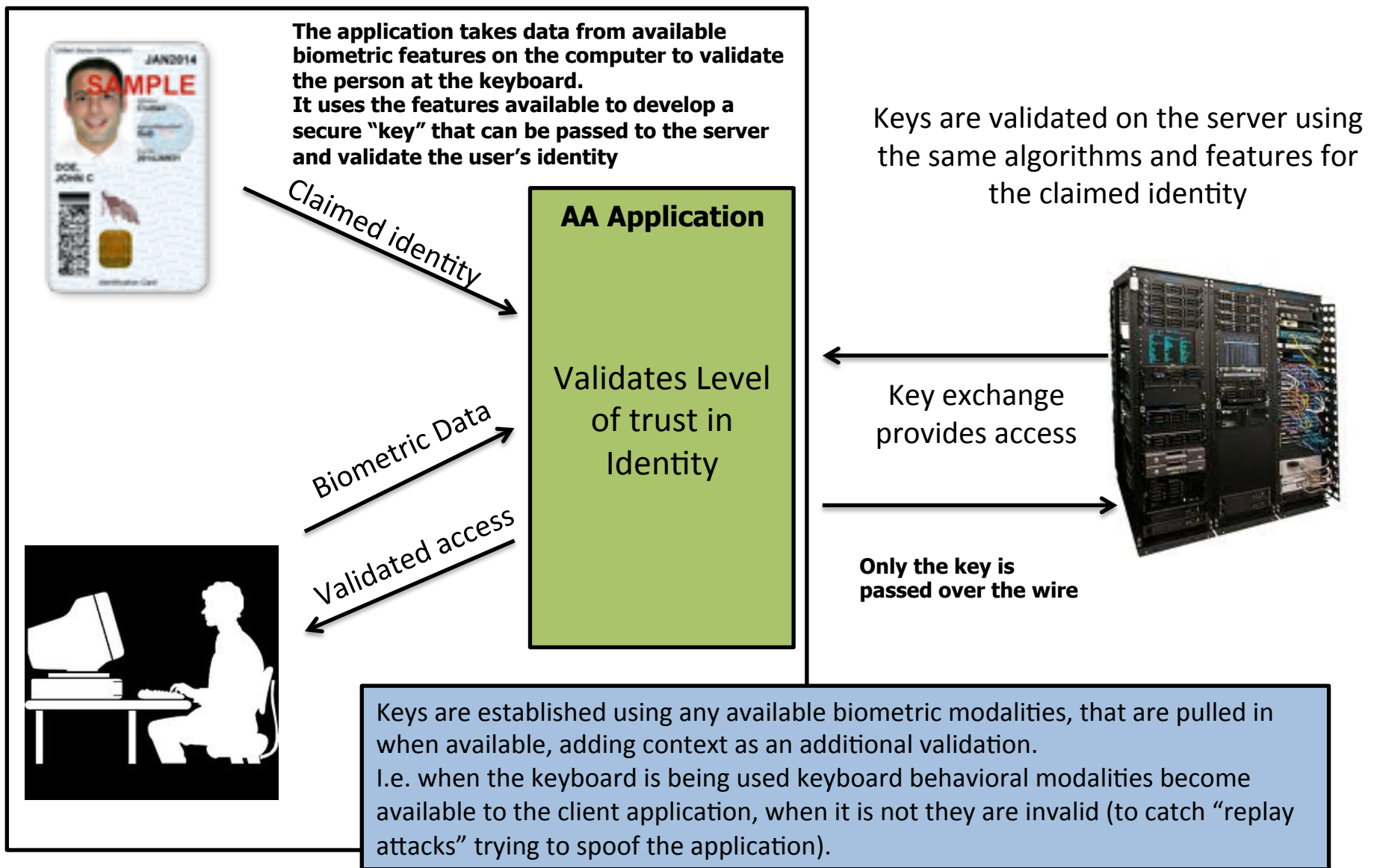
Using spatio-temporal screen fingerprints to identify the user for authentication.

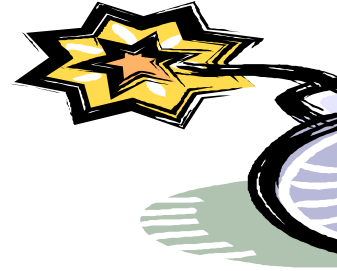
## **Behavioral Web Analytics -Naval Research Labs (NRL funded)**

Identification of the user from Web browsing activities to include semantic (what kind of webpages are visited) and syntactic session features



# How will the AA system validate identity?





PROCEED

---

**Drew Dean**



# Do you trust the cloud?

---



*Secure communications...*

Solution: Encrypt data in flight



*Secure storage...*

Solution: Encrypt data on disk

Solution: Compute on Encrypted Data  
(Fully Homomorphic Encryption)



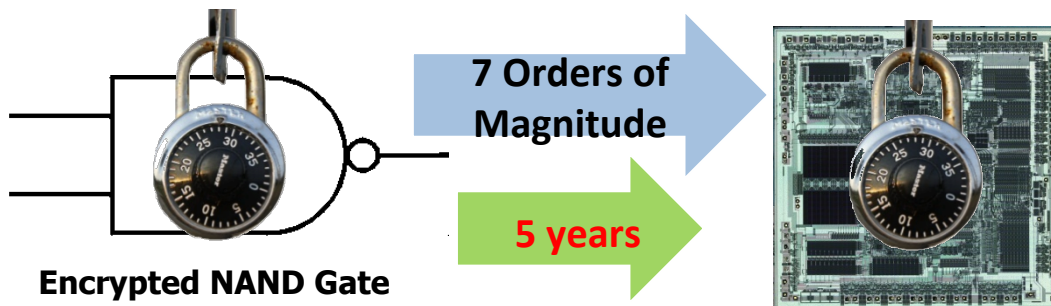
*Secure computation?*



## PROgramming Computation on Encrypted Data (PROCEED)

**Goal:** *practical computation on encrypted data without decrypting*

- In 1978, formally stated as fully homomorphic cryptosystem.
- An open problem for 31 years
- 2009 publication of Craig Gentry's construction of the first FH cryptosystem.
- Gentry's prototype ran 14 orders of magnitude slower than computation in the clear
- Fractions of a nanosecond (e.g an NAND) become half an hour.



### Potential Applications:

- Email content-filtering guard between networks with different classification levels
- Privacy-preserving cloud-based voice over IP service
- Secure cloud-based mapping service that cannot determine your location, route, or destination

### Research Thrusts

- Fundamental Mathematics
- Implementation/Measurement/Optimization
- Programming Model
- Algorithms and Data Structures



## PROCEED First Year Accomplishments

### Programmatics and Program Structure

- Kickoff: February 2011
- Three Technology Areas: Fully and Somewhat Homomorphic Encryption (FHE & SWHE), Secure Multiparty Computation (SMPC), Secret Sharing
- Technology characteristics
  - Different security models, very different performance
  - Theory develops faster than implementation
- Theory and Implementation efforts funded for each Technology Area

### Y1 Results - Highlights

|                | Theory                                                                                                                             | Implementation                                                                                                       |
|----------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| FHE / SWHE     | 16 new FHE and SWHE schemes                                                                                                        | 10x-100x performance improvement                                                                                     |
| SMPC           | Resolved open question from 1988 on SMPC communication complexity in malicious vs. honest-but-curious threat models: it's the same | 20x reduction in memory used to compute set intersection                                                             |
| Secret Sharing | First algorithms for floating-point arithmetic                                                                                     | Implemented/tested AES-128 block cipher on data protected using secret sharing. New performance record: 30KB/second. |