Cyber Defense

May 2013

Approved for Public Release, Distribution Unlimited

What we hear.

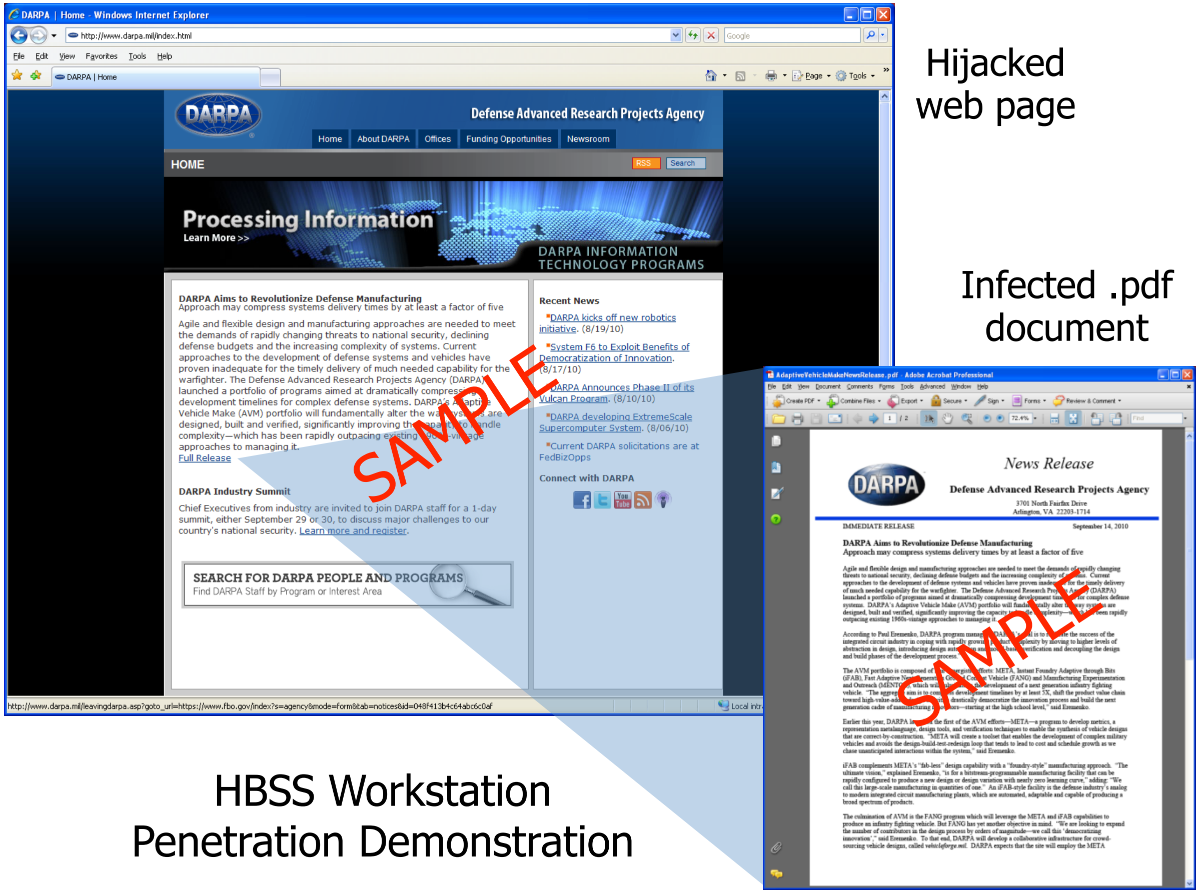
Attackers penetrate the architecture easily…

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.


DARPA | Home - Windows Internet Explorer
http://www.darpa.mil/index.html
Google
File Edit View Favorites Tools Help
DARPA | Home
Page Tools
Home About DARPA Offices Funding Opportunities Newsroom
HOME
RSS
Search
Learn More >>
SAMPLE
AdaptiveVehicleMakeNewsRelease.pdf - Adobe Acrobat Professional
File Edit View Document Comments Forms Tools Advanced Window Help
Create PDF Combine Files Export Secure Sign Forms Review & Comment
1 / 2
72.4%
Find
SAMPLE

DARPA Defense Advanced Research Projects Agency

Processing Information

DARPA INFORMATION TECHNOLOGY PROGRAMS

DARPA Aims to Revolutionize Defense Manufacturing
Approach may compress systems delivery times by at least a factor of five

Agile and flexible design and manufacturing approaches are needed to meet the demands of rapidly changing threats to national security, declining defense budgets and the increasing complexity of systems. Current approaches to the development of defense systems and vehicles have proven inadequate for the timely delivery of much needed capability for the warfighter. The Defense Advanced Research Projects Agency (DARPA) launched a portfolio of programs aimed at dramatically compressing development timelines for complex defense systems. DARPA's Adaptive Vehicle Make (AVM) portfolio will fundamentally alter the way systems are designed, built and verified, significantly improving the capacity to handle complexity—which has been rapidly outpacing existing 1960s-vintage approaches to managing it.
Full Release

DARPA Industry Summit

Chief Executives from industry are invited to join DARPA staff for a 1-day summit, either September 29 or 30, to discuss major challenges to our country's national security. Learn more and register.

SEARCH FOR DARPA PEOPLE AND PROGRAMS
Find DARPA Staff by Program or Interest Area

Recent News

- DARPA kicks off new robotics initiative. (8/19/10)
- System F6 to Exploit Benefits of Democratization of Innovation. (8/17/10)
- DARPA Announces Phase II of its Vulcan Program. (8/10/10)
- DARPA developing ExtremeScale Supercomputer System. (8/06/10)
- Current DARPA solicitations are at FedBizOpps

Connect with DARPA

http://www.darpa.mil/leavingdarpa.asp?goto_url=https://www.fbo.gov/index?s=agency&mode=form&tab=notices&id=048f413b4c64abc6c0af

Local intr

News Release

DARPA

Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington, VA 22203-1714

IMMEDIATE RELEASE September 14, 2010

DARPA Aims to Revolutionize Defense Manufacturing
Approach may compress systems delivery times by at least a factor of five

Agile and flexible design and manufacturing approaches are needed to meet the demands of rapidly changing threats to national security, declining defense budgets and the increasing complexity of systems. Current approaches to the development of defense systems and vehicles have proven inadequate for the timely delivery of much needed capability for the warfighter. The Defense Advanced Research Projects Agency (DARPA) launched a portfolio of programs aimed at dramatically compressing development timelines for complex defense systems. DARPA's Adaptive Vehicle Make (AVM) portfolio will fundamentally alter the way systems are designed, built and verified, significantly improving the capacity to handle complexity—which has been rapidly outpacing existing 1960s-vintage approaches to managing it.

According to Paul Eremenko, DARPA program manager, "DARPA's goal is to replicate the success of the integrated circuit industry in coping with rapidly growing product complexity by moving to higher levels of abstraction in design, introducing design automation and model-based verification and decoupling the design and build phases of the development process."

The AVM portfolio is composed of four synergistic efforts: META, Instant Foundry Adaptive through Bits (iFAB), Fast Adaptive Next-Generation Ground Combat Vehicle (FANG) and Manufacturing Experimentation and Outreach (MENTOR), which will culminate in the development of a next generation infantry fighting vehicle. "The aggregate aim is to compress development timelines by at least 5X, shift the product value chain toward high-value-added design activities, drastically democratize the innovation process and build the next generation cadre of manufacturing innovators—starting at the high school level," said Eremenko.

Earlier this year, DARPA launched the first of the AVM efforts—META—a program to develop metrics, a representation metalanguage, design tools, and verification techniques to enable the synthesis of vehicle designs that are correct-by-construction. "META will create a toolset that enables the development of complex military vehicles and avoids the design-build-test-redesign loop that tends to lead to cost and schedule growth as we chase unanticipated interactions within the system," said Eremenko.

iFAB complements META's "fab-less" design capability with a "foundry-style" manufacturing approach. "The ultimate vision," explained Eremenko, "is for a bitstream-programmable manufacturing facility that can be rapidly configured to produce a new design or design variation with nearly zero learning curve," adding: "We call this large-scale manufacturing in quantities of one." An iFAB-style facility is the defense industry's analog to modern integrated circuit manufacturing plants, which are automated, adaptable and capable of producing a broad spectrum of products.

The culmination of AVM is the FANG program which will leverage the META and iFAB capabilities to produce an infantry fighting vehicle. But FANG has yet another objective in mind. "We are looking to expand the number of contributors in the design process by orders of magnitude—we call this 'democratizing innovation'," said Eremenko. To that end, DARPA will develop a collaborative infrastructure for crowd-sourcing vehicle designs, called *vehicleforge.mil*. DARPA expects that the site will employ the META

Hijacked web page

Infected .pdf document

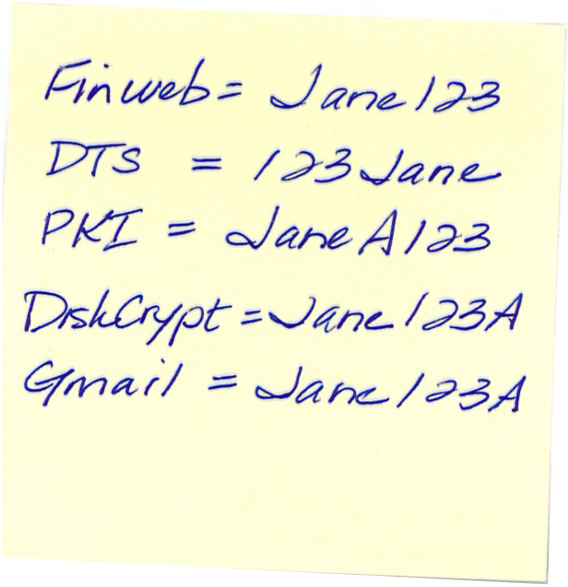
HBSS Workstation Penetration Demonstration

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
DskCrypt = Jane123A
Gmail = Jane123A

http://gizmodo.com/5116607/an-extensive-obsessive-performance-test-of-usb-keys

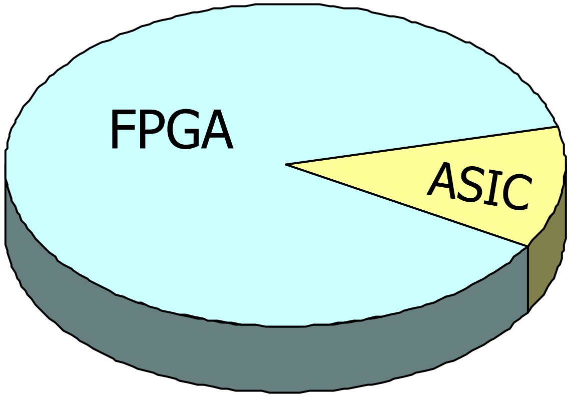
The supply chain is potentially compromised…

Approximately 3500 ICs.

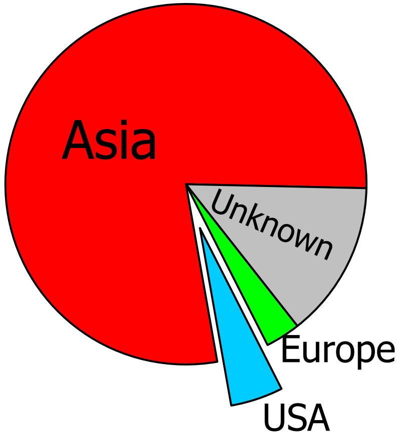
- 200 unique chip types.
- 208 field programmable gate arrays (FPGAs).
- 64 FPGA and 9 ASIC types across 12 subsystems.

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

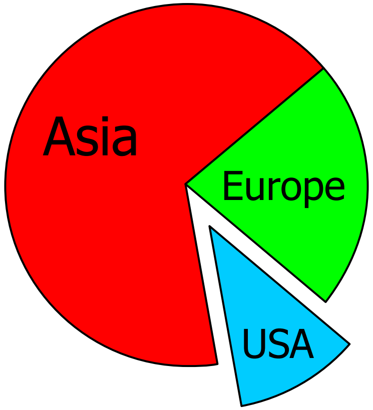
JSF FPGA & ASIC Usage



FPGA Manufacture Location



ASIC Manufacture Location



Approved for Public Release, Distribution Unlimited.

Our physical systems are vulnerable to cyber attacks…

A4 Nation s 219180096 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 i
the con
next w
spokesm
day.

The
"expres

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

ded a
pes of
China.
nent's
with a
n that
Rod-
Thurs-

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 irrita
icans," said James A.
ber and national sec
at the Center for S
International Studi
their favorite child,
Google. The firm's ch
advises President
technology, and its
tions are seen as th
novation that will d
economy.

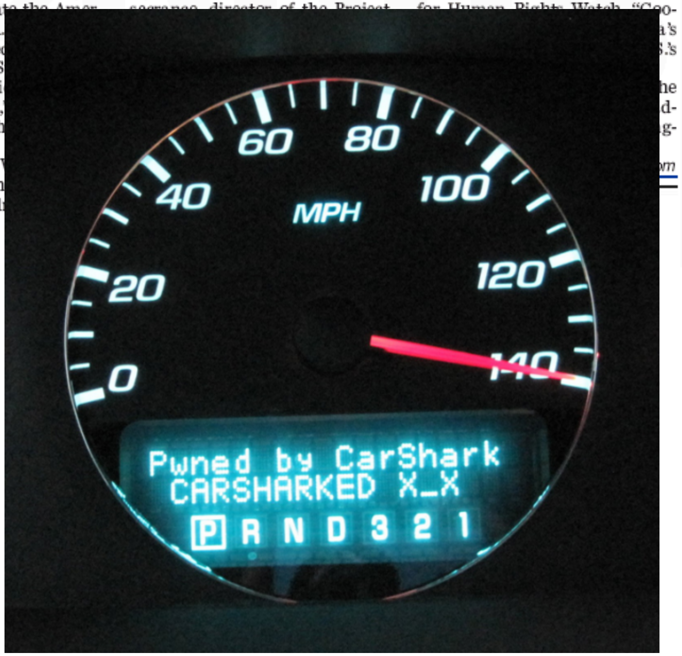
Officials said the administration has raised concerns about cybersecurity and Internet freedom with China before. But by formally protesting to the Chinese, the United States is elevating the issues to a new level, policy experts said. Richard N. Ro-

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
a's
S.'s
he
d-
g-
wn

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]

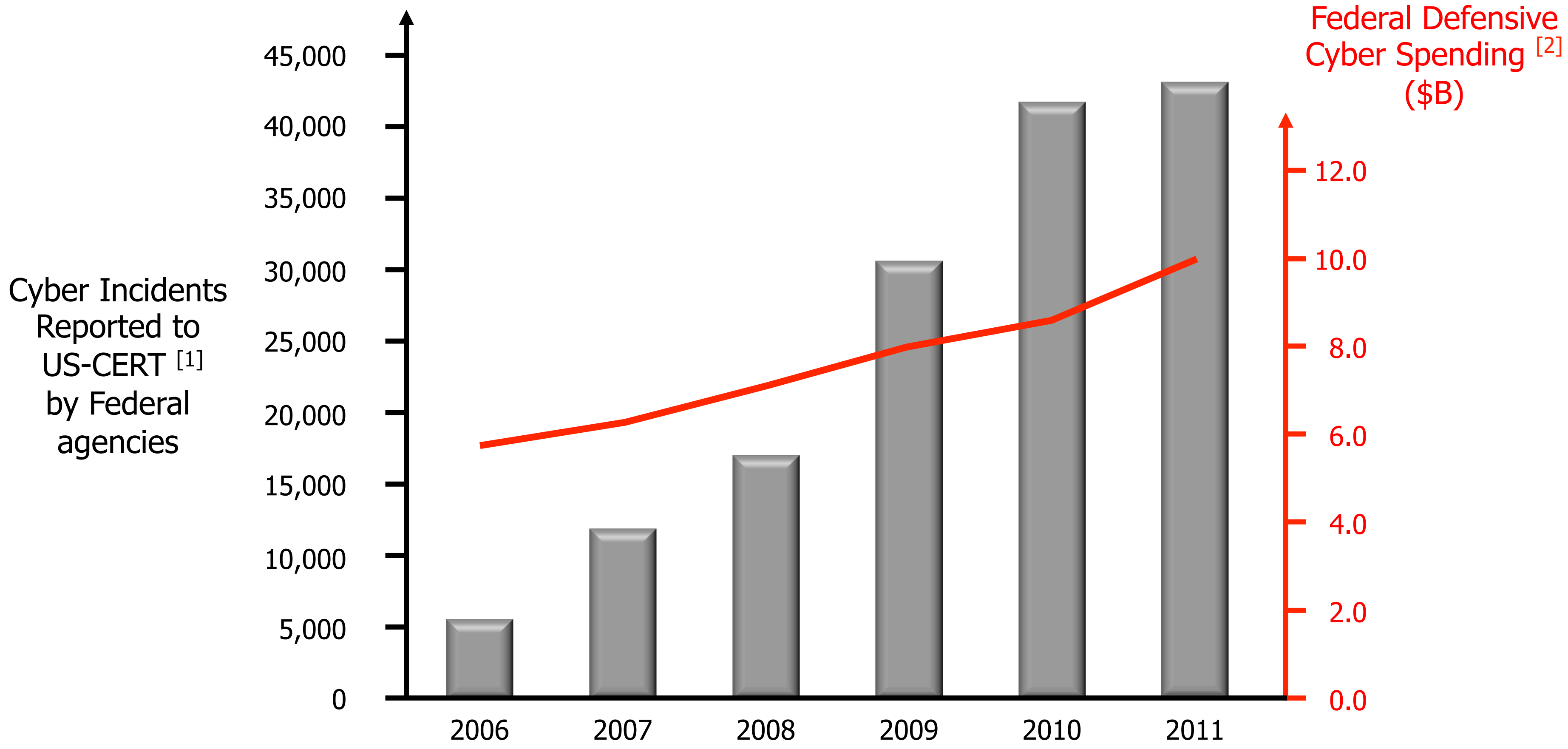


False speedometer reading
Note that the car is in park…

[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…



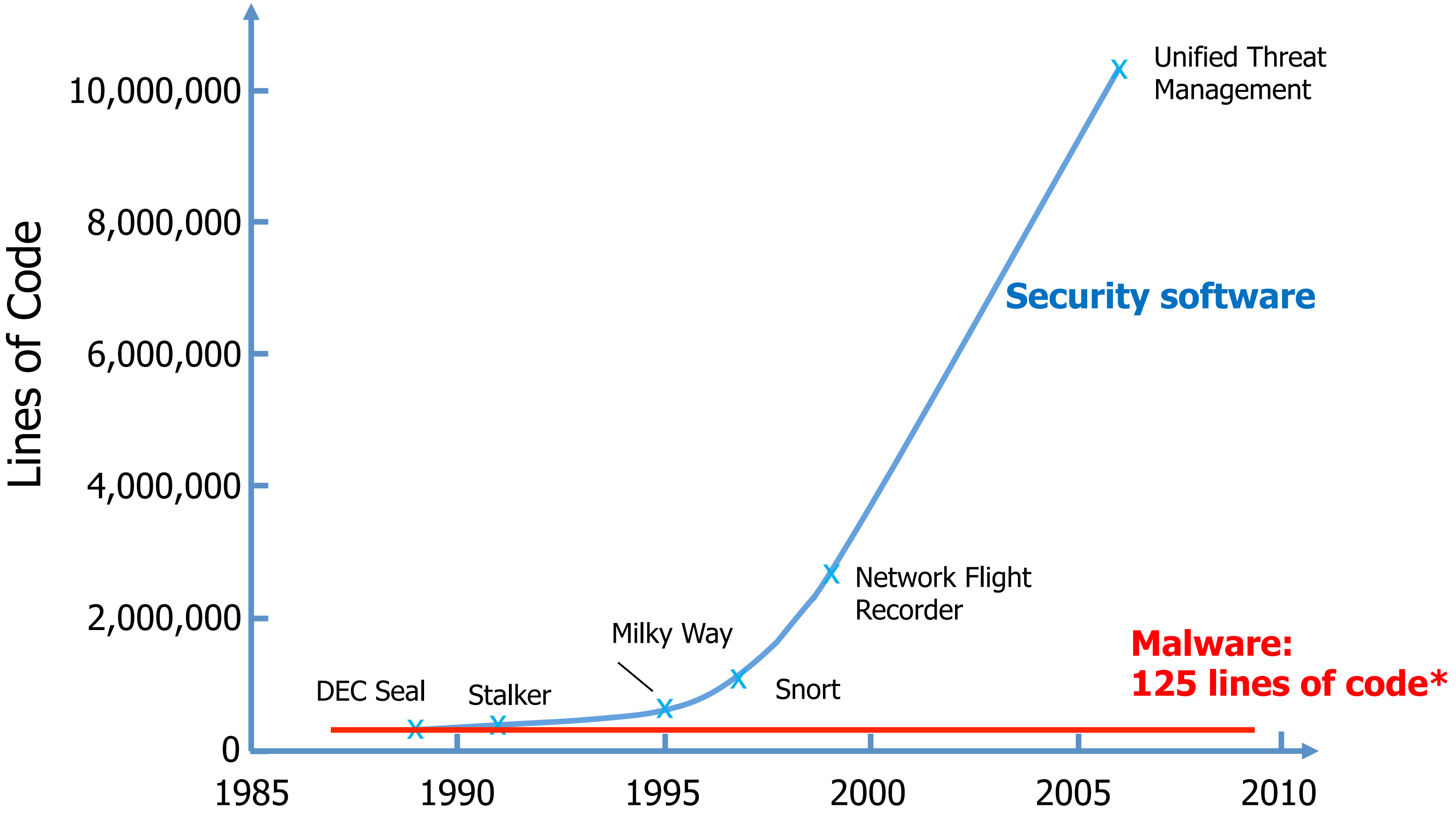
Federal Cyber Incidents and Defensive Cyber Spending
fiscal years 2006 – 2011

[1] GAO Testimony. GAO-12-166T CYBERSECURITY Threats Impacting the Nation

[2] INPUT reports 2006 – 2011

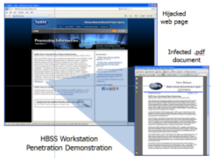
Why?

We are divergent with the threat…

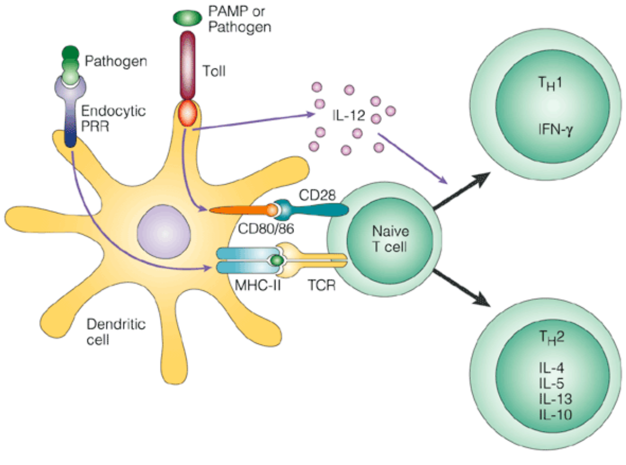


* Public sources of malware averaged over 9,000 samples
(collection of exploits, worms, botnets, viruses, DoS tools)

Getting convergent:
Manageable diversity (CRASH[‡])



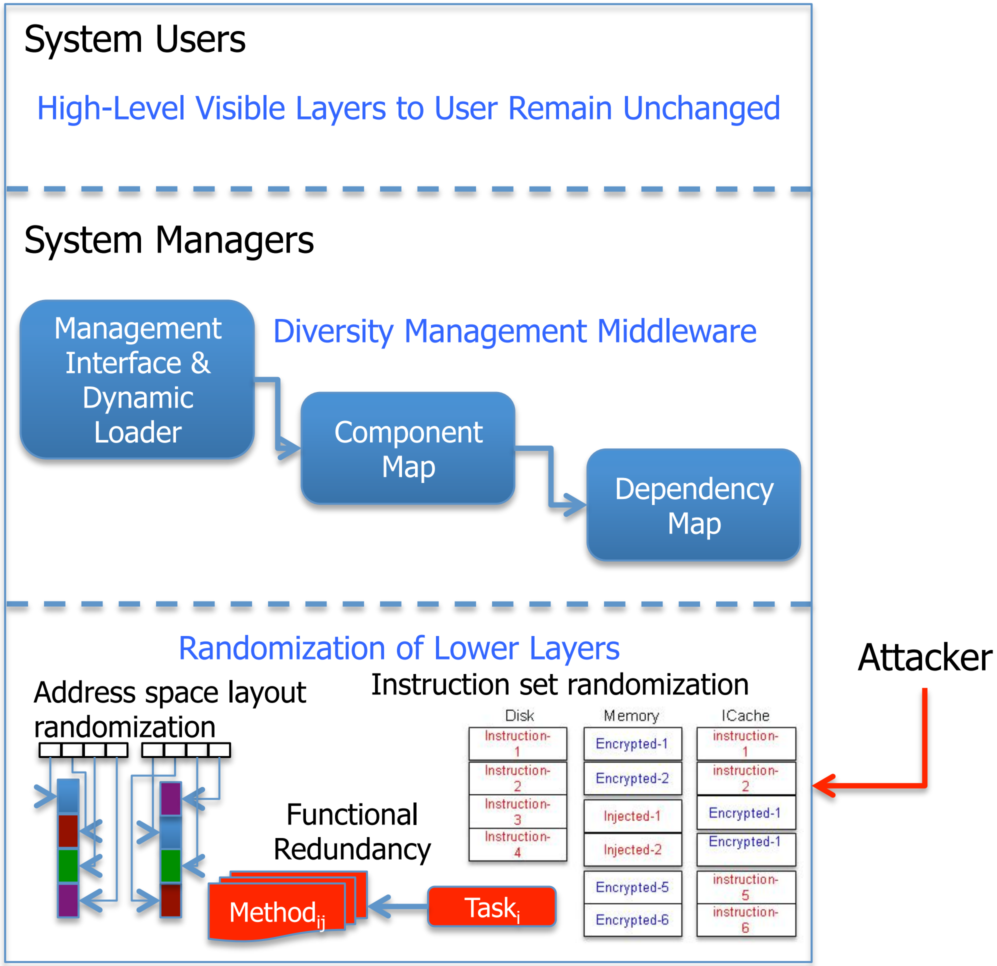
New architectures guided by biology



Nature Reviews | Immunology

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

Make all systems look the **same** to the system users and managers, but **different** to the attackers.

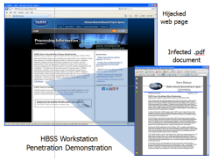


System Users
High-Level Visible Layers to User Remain Unchanged
System Managers
Management Interface & Dynamic Loader
Diversity Management Middleware
Component Map
Dependency Map
Randomization of Lower Layers
Address space layout randomization
Instruction set randomization
Functional Redundancy
$Method_{ij}$
$Task_i$
Attacker

Disk	Memory	ICache
Instruction-1	Encrypted-1	instruction-1
Instruction-2	Encrypted-2	instruction-2
Instruction-3	Injected-1	Encrypted-1
Instruction-4	Injected-2	Encrypted-1
	Encrypted-5	instruction-5
	Encrypted-6	instruction-6

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

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.

Active Authentication

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

Objective

Validate the individual at the keyboard by those unique factors that make up the individual.

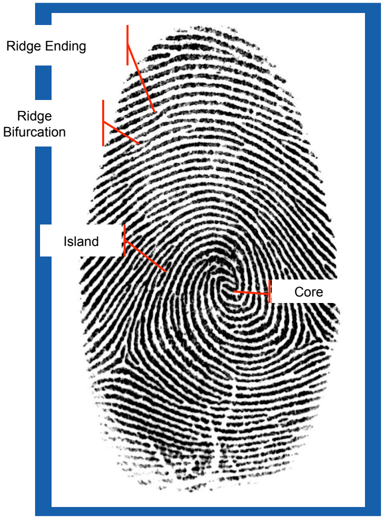
Approach

Focus on software biometrics (those without hardware sensors).

Rotate many different biometrics as the human at the keyboard is working, resulting in an invisible authentication method.

Beyond passwords

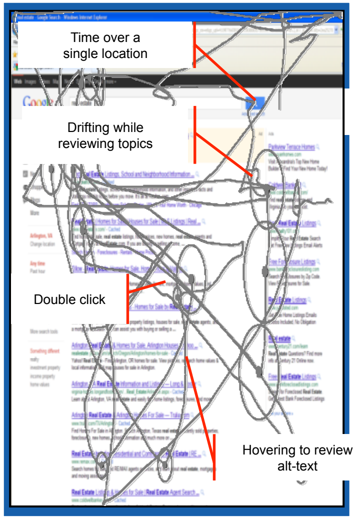
Fingerprint



Source: epdeatonville.org\wp-content uploads\2011 04\fingerprint.jpg

Existing Technology

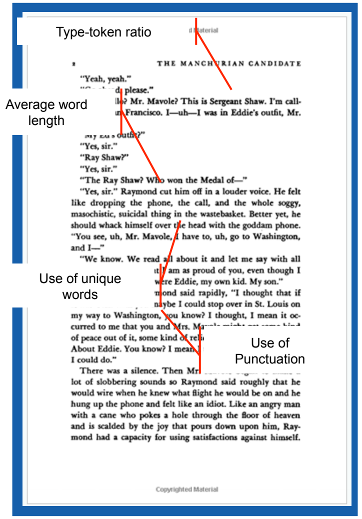
Mouse tracking


Time over a single location
Drifting while reviewing topics
Double click
Hovering to review alt-text

Source: google search for "real estate" with mouse tracking provided by IOGraph

Repurposed Technology

Forensic authorship


Type-token ratio
Average word length
Use of unique words
Use of Punctuation

d Material

2 THE MANCHURIAN CANDIDATE

"Yeah, yeah."

d, please."

llo? Mr. Mavole? This is Sergeant Shaw. I'm call-
n Francisco. I—uh—I was in Eddie's outfit, Mr.

outfit?"

"Yes, sir."

"Ray Shaw?"

"Yes, sir."

"The Ray Shaw? Who won the Medal of—"

"Yes, sir." Raymond cut him off in a louder voice. He felt like dropping the phone, the call, and the whole soggy, masochistic, suicidal thing in the wastebasket. Better yet, he should whack himself over the head with the goddam phone. "You see, uh, Mr. Mavole, I have to, uh, go to Washington, and I—"

"We know. We read all about it and let me say with all it I am as proud of you, even though I were Eddie, my own kid. My son."

mond said rapidly, "I thought that if maybe I could stop over in St. Louis on my way to Washington, you know? I thought, I mean it occurred to me that you and Mrs. Ma of peace out of it, some kind of rel About Eddie. You know? I mean I could do."

There was a silence. Then Mr lot of slobbering sounds so Raymond said roughly that he would wire when he knew what flight he would be on and he hung up the phone and felt like an idiot. Like an angry man with a cane who pokes a hole through the floor of heaven and is scalded by the joy that pours down upon him, Raymond had a capacity for using satisfactions against himself.

Copyrighted Material

Source: The Mancurian Candidate, Robert Graves, P2, Amazon Preview

New Technology

Biometric Identity Modalities

Approved for Public Release, Distribution Unlimited.

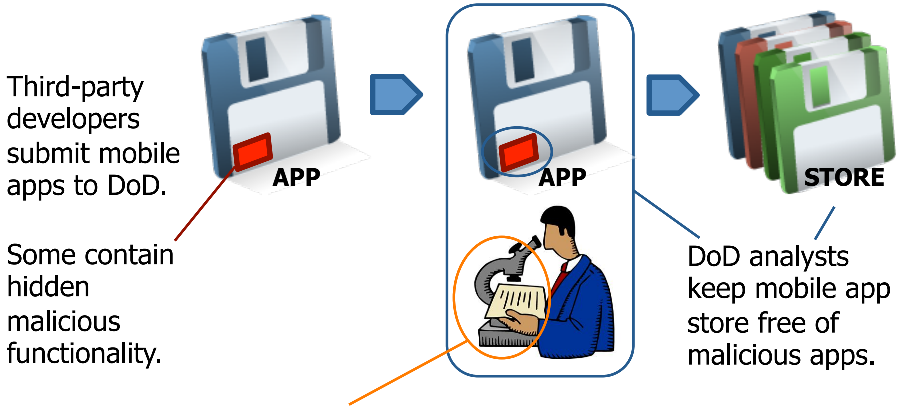
Automated Program Analysis for Cybersecurity (APAC)

Objective

- Develop new program analysis tools and techniques for detecting malicious functionality in mobile applications.
- Seek fundamental advances in program analysis that might enable DoD to vet other kinds of software, too.

Approach

- Produce practical automated analysis tools designed to keep malicious code out of DoD mobile application marketplaces.
- Translate goal of keeping malicious code out of DoD mobile application marketplaces into lower-level properties that can be proven with automated program analysis tools.



Third-party developers submit mobile apps to DoD.

Some contain hidden malicious functionality.

DoD analysts keep mobile app store free of malicious apps.

Develop new tools and techniques for vetting mobile apps.

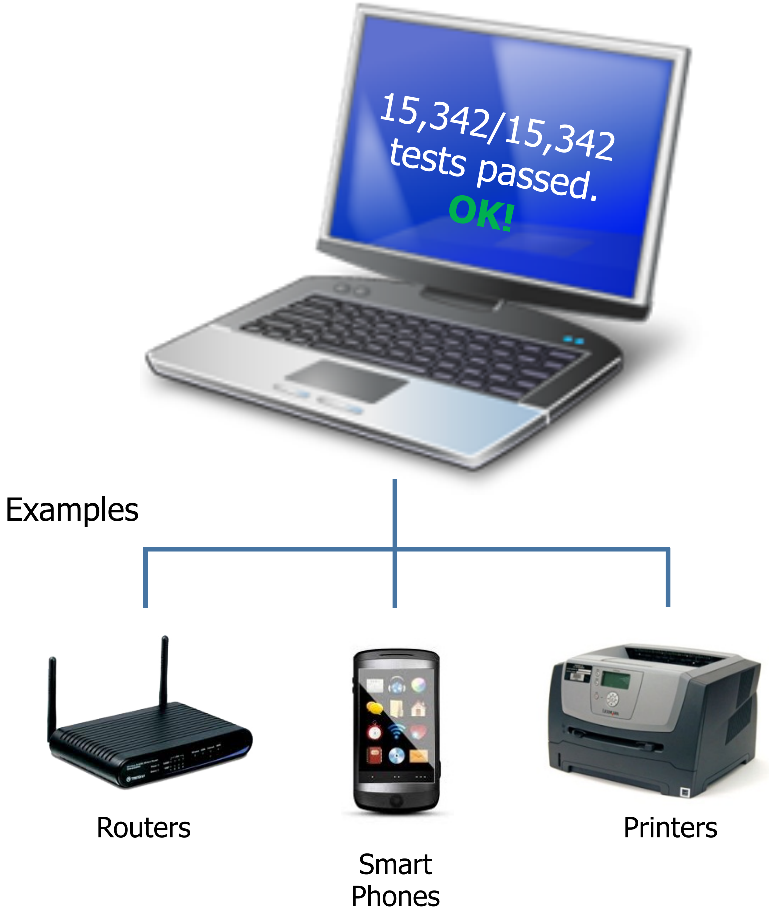
VET: Vetting Commodity IT Software and Firmware

Objective

- Fully-automated checks for broad classes of malicious features and dangerous flaws in software and firmware

Approach

- Detect attacks we have never seen before that are not based on signatures
  - Define malice:
    - Determine broad classes of hidden malicious functionality to rule out
  - Confirm the absence of malice:
    - Demonstrate the absence of those broad classes of hidden malicious functionality
  - Examine equipment at scale:
    - Scale to non-specialist technicians who must vet every individual new device used by DoD prior to deployment



Images of specific hardware are for illustration only and should not be interpreted as implying vulnerabilities

http://www.dtic.mil/whs/esd/cmd/index.htm
http://broadband.mt.gov/providers.aspx
http://www.benning.army.mil/library/content/MCoELibrariesEResources/mcoelibrarieseresources.htm
http://www.mc4.army.mil/hardware/Printers

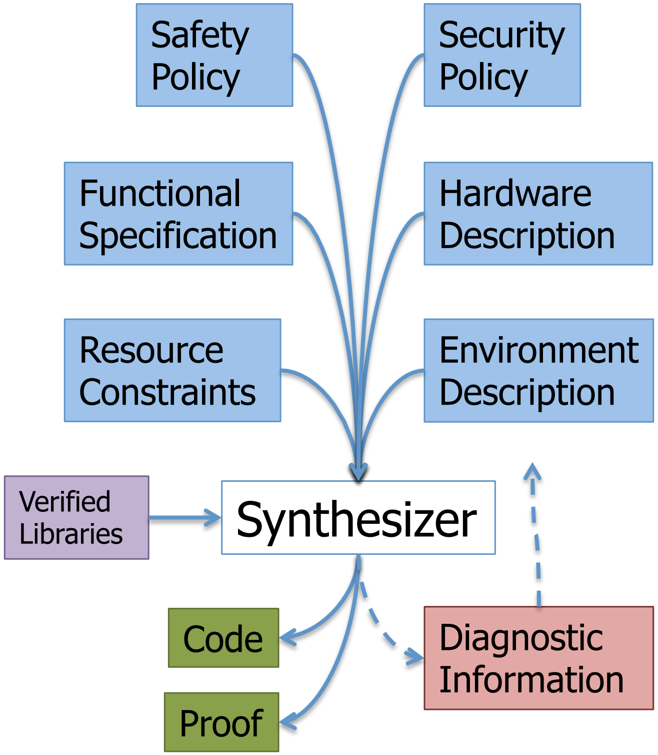
High Assurance Cyber Military Systems

Objective:

- Cost-effective construction of high-assurance cyber-physical systems.
    - Functionally correct.
    - Satisfy appropriate safety and security properties.

Approach:

- Use clean-slate formal methods
- Produce high-assurance operating system components and control systems.
- Develop a suite of program synthesizers and formal-methods tools.
- Generate an integration workbench containing all HACMS tools and assured components.


Safety Policy

Security Policy

Functional Specification

Hardware Description

Resource Constraints

Environment Description

Verified Libraries

Synthesizer

Code

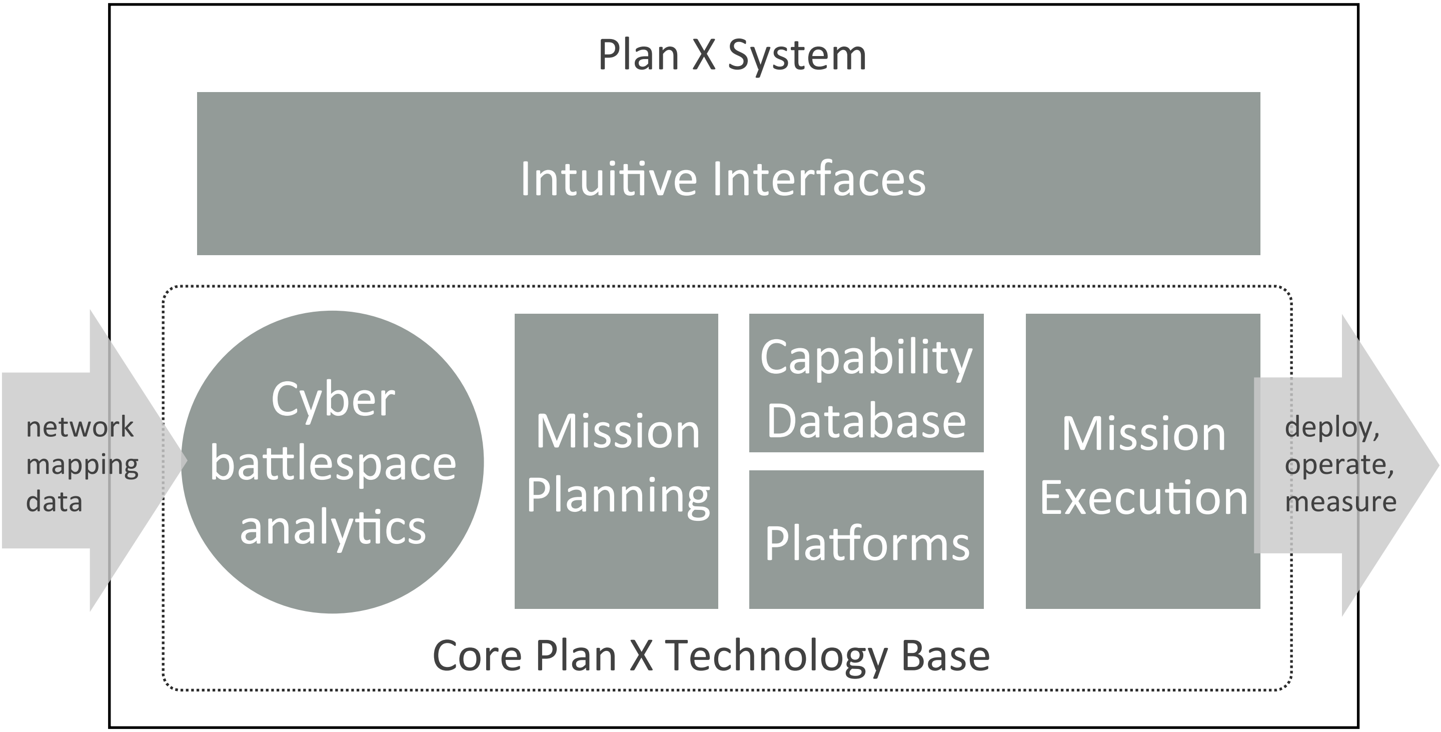
Proof

Diagnostic Information

Clean-slate formal-methods-based approach

Plan X

A single view of the cyber battlespace for planning, operation and situational awareness



- Real-time cyberspace analytics
- Intuitive views and interactions
- Single fused situational awareness
- Machine execution
- Assured and integrated battle damage assessment
- Work with range of skill sets, novice to expert

www.darpa.mil