Innovation and Impact in Cyber Security

Farnam Jahanian

Carnegie Mellon University

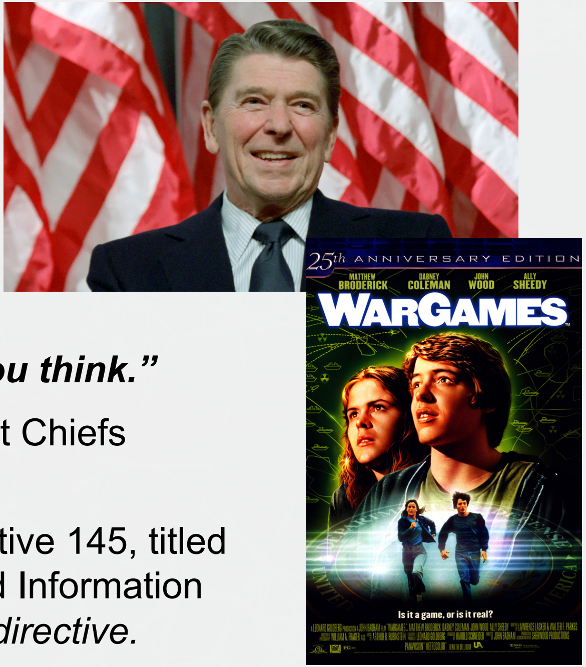
SaTC PI Meeting

January 10, 2017

Reagan, War Games, NSDD145

“Could something like this really happen? Could someone break into our most sensitive computers?”

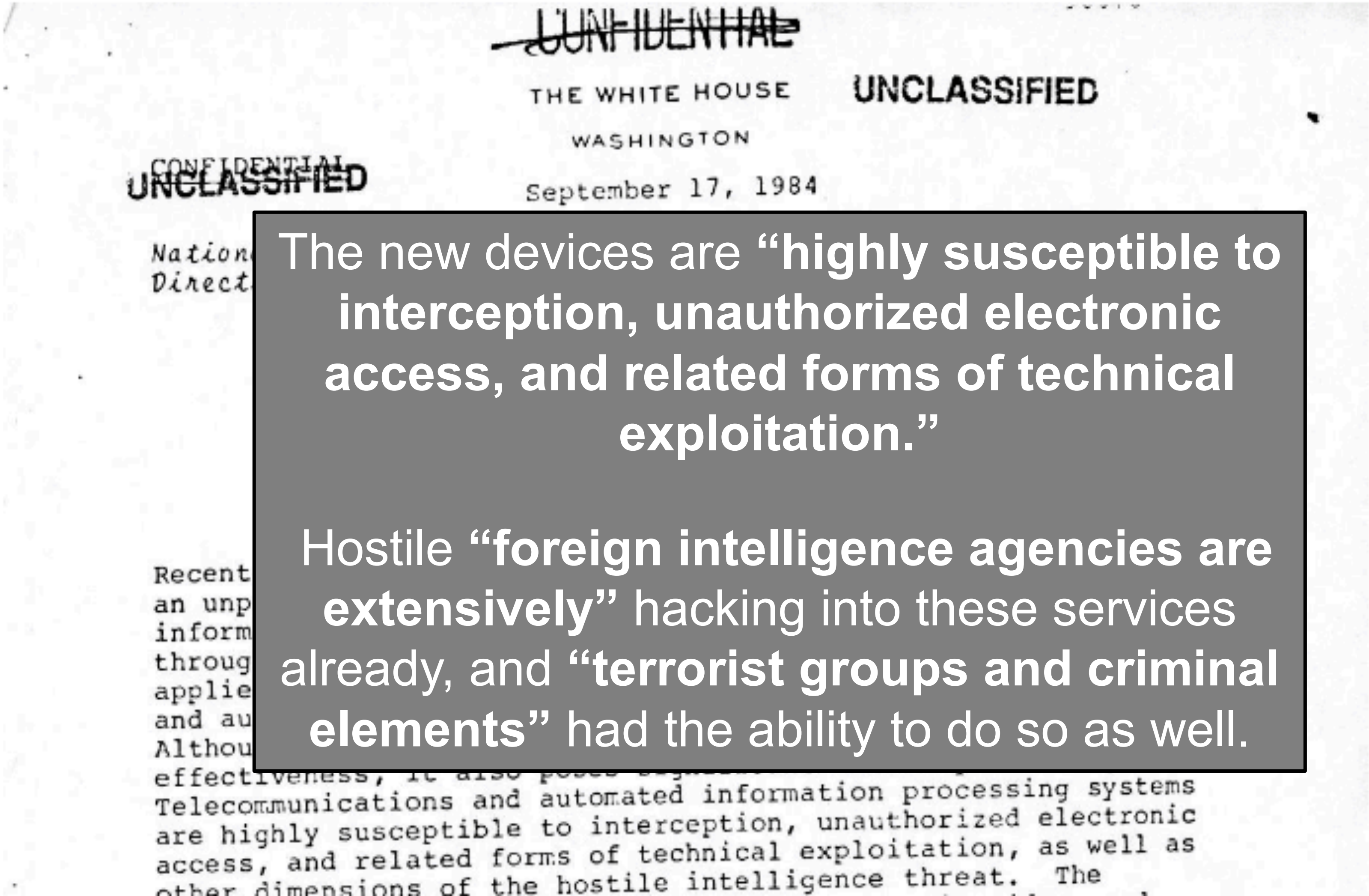
- Ronald Reagan , June 1983



“Mr. President, the problem is much worse than you think.”

- Gen. John Vasey, Chairman of Joint Chiefs

September 17, 1984: National Security Decision Directive 145, titled “National Policy on Telecommunication and Automated Information Systems Security” – Our nation’s *first “cyber warfare” directive.*



~~CONFIDENTIAL~~

THE WHITE HOUSE UNCLASSIFIED

WASHINGTON

~~CONFIDENTIAL~~ UNCLASSIFIED

September 17, 1984

Nation
Direct

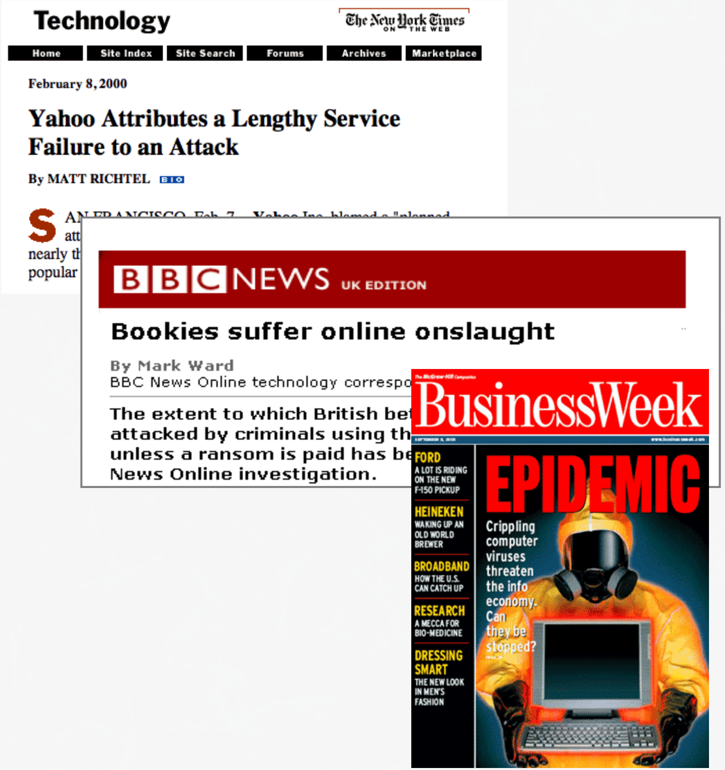
Recent
an unp
inform
throug
applie
and au
Althou
effectiveness, it also poses
Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The

The new devices are **"highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation."**

Hostile **"foreign intelligence agencies are extensively"** hacking into these services already, and **"terrorist groups and criminal elements"** had the ability to do so as well.

Early Years: Cyber Vandalism

- The primary motivation of hackers was **bragging rights.**
- Worms and viruses were intended to simply **wreak havoc** on the infrastructure.
- These were availability attacks that **impacted network access and services**, and often, reputations.



Technology

The New York Times ON THE WEB

Home | Site Index | Site Search | Forums | Archives | Marketplace

February 8, 2000

Yahoo Attributes a Lengthy Service Failure to an Attack

By MATT RICHTEL BIO

SAN FRANCISCO, Feb. 7 -- Yahoo Inc. blamed a "planned
att
nearly th
popular

BBC NEWS UK EDITION

Bookies suffer online onslaught

By Mark Ward
BBC News Online technology correspo

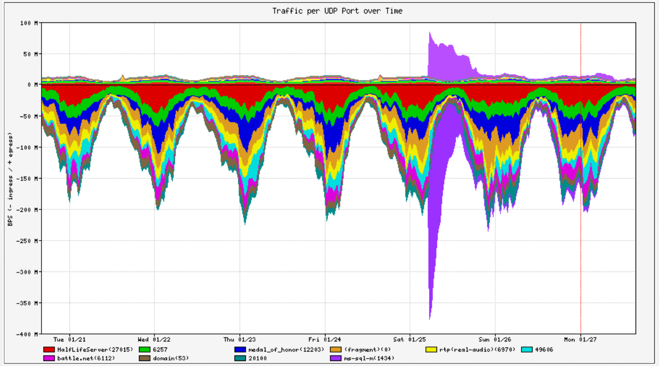
The extent to which British bet
attacked by criminals using th
unless a ransom is paid has be
News Online investigation.

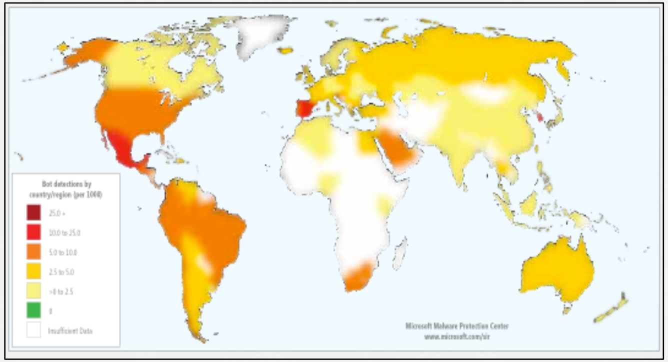
BusinessWeek
FORD
A LOT IS RIDING ON THE NEW F-150 PICKUP
HEINEKEN
WAKING UP AN OLD WORLD BREWER
BROADBAND
HOW THE U.S. CAN CATCH UP
RESEARCH
A MECCA FOR BIO-MEDICINE
DRESSING SMART
THE NEW LOOK IN MEN'S FASHION
EPIDEMIC
Crippling computer viruses threaten the info economy. Can they be stopped?

The Rise of Botnets: Cyber Crime

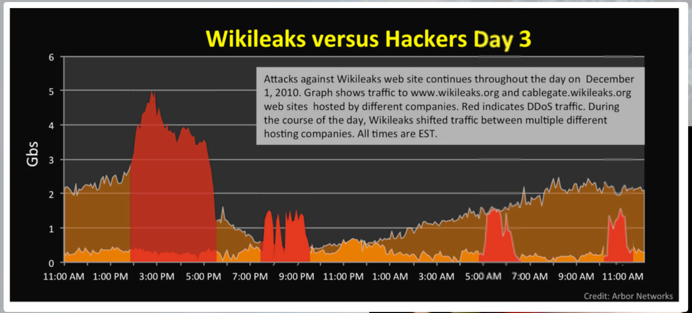
- Dramatic Transformation and Escalation
  - A compromised system is **more useful alive than dead**
  - A compromised system **provides anonymity**
  - A network of compromised hosts provides a **powerful delivery platform**

- Increased sophistication, the targeting of specific applications, and attempts to foil attribution.





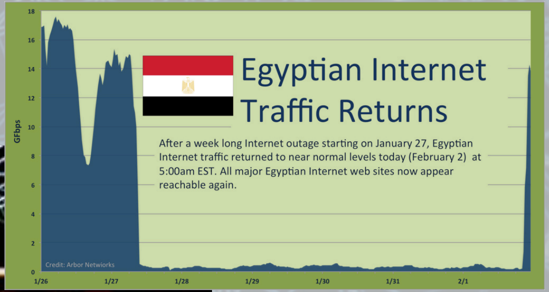
Cyber-War, Censorship, Hack-ivism, and Cyber-Espionage



Wikileaks versus Hackers Day 3

Attacks against Wikileaks web site continues throughout the day on December 1, 2010. Graph shows traffic to www.wikileaks.org and cablegate.wikileaks.org web sites hosted by different companies. Red indicates DDoS traffic. During the course of the day, Wikileaks shifted traffic between multiple different hosting companies. All times are EST.

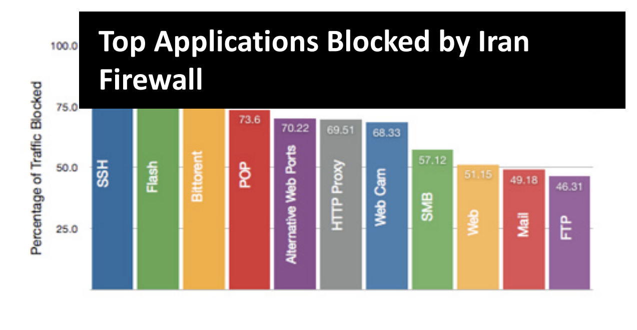
Credit: Arbor Networks



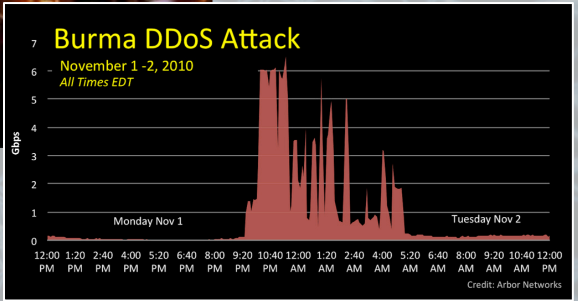
Egyptian Internet Traffic Returns

After a week long Internet outage starting on January 27, Egyptian Internet traffic returned to near normal levels today (February 2) at 5:00am EST. All major Egyptian Internet web sites now appear reachable again.

Credit: Arbor Networks



Top Applications Blocked by Iran Firewall



Burma DDoS Attack

November 1 -2, 2010

All Times EDT

Credit: Arbor Networks

Cyber Security Challenges

- **Attacks and defenses co-evolve**: a system that was secure yesterday might no longer be secure tomorrow.
- As we upgrade functionality, availability, and/or performance, **new systems introduce new vulnerabilities** that need new defenses.
- The **environments** and the functionality of our computing systems are **dynamic**.
- As **automation pervades new platforms**, vulnerabilities will be found in critical infrastructures and systems.
- Both the number and **sophistication** of attackers is increasing as well as the **specificity** of their targets.
- Cyber security is a **multi-dimensional** problem requiring expertise from various disciplines: CS, mathematics, economics, social and behavioral sciences, and policy.

We don’t do the easy stuff well, and the hard stuff is getting harder.

Mobile: Android and iOS

71%

of Android devices out of date

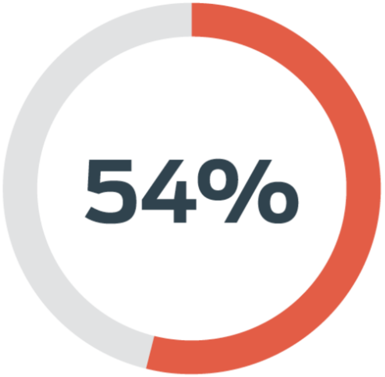
Android < 5.5.1, or < 6.0.1

50%

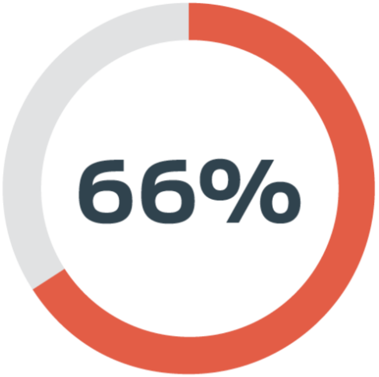
of iOS devices out of date

iOS < 9.2

Operating Systems: OS X



of Macs either run an **unsupported OS**, or are **not fully patched**.



of all Macs are **not running the latest major version**, 10.11.

8% of Apple users are **running unsupported versions of OS X** (10.8 and earlier) that cannot receive security updates.

The New York Times

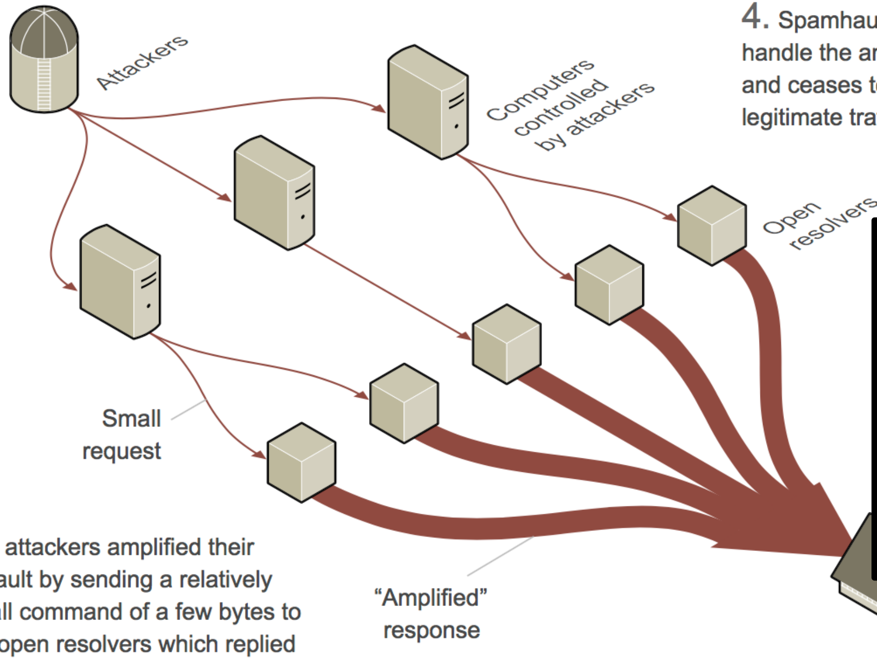
How the amplification attack on Spamhaus Unfolded *[March 2013]*

1. The attackers send commands to about 1,000 computers under their control.

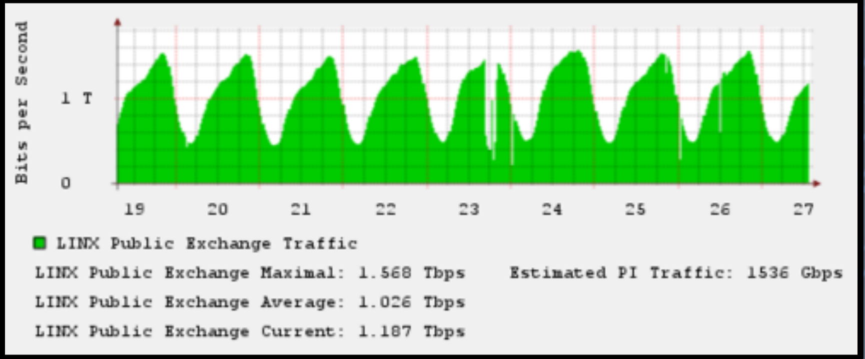
2. Each computer, pretending to be Spamhaus, sends requests for information to a type of Internet server called an open resolver. An estimated 100,000 resolvers are involved in the attack.

3. The resolvers respond with a much larger message than the initial request, amplifying the size of the attack.

4. Spamhaus cannot handle the amount of traffic and ceases to respond to legitimate traffic.



The attackers amplified their assault by sending a relatively small command of a few bytes to the open resolvers which replied with a message that was 100 times larger than the initial request.

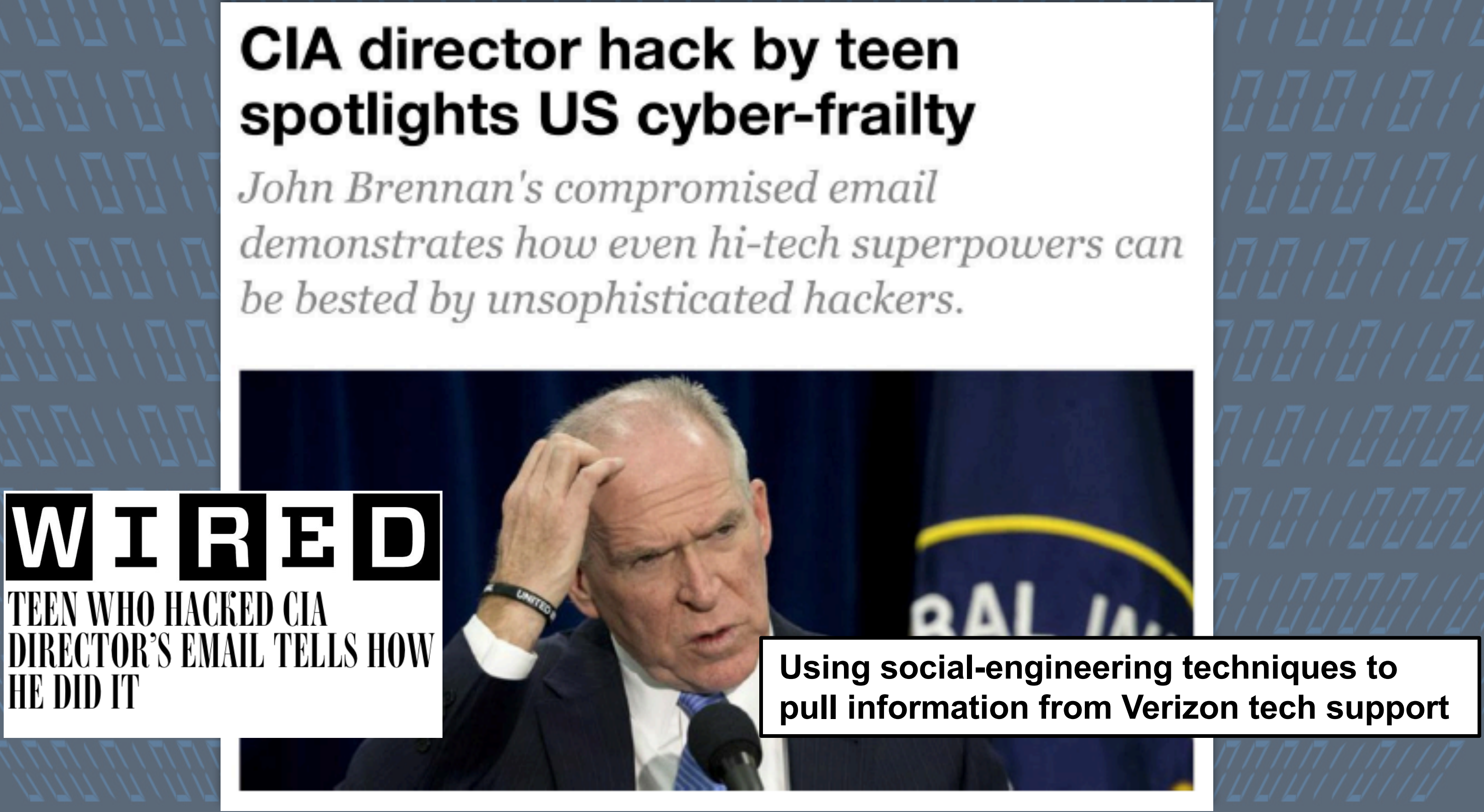


🟩 LINX Public Exchange Traffic

```
LINX Public Exchange Maximal:  1.568 Tbps     Estimated PI Traffic: 1536 Gbps
LINX Public Exchange Average:  1.026 Tbps
LINX Public Exchange Current:  1.187 Tbps
```

- Open DNS Resolvers
- Lack of egress filtering

Source: New York Times



CIA director hack by teen spotlights US cyber-frailty

John Brennan's compromised email demonstrates how even hi-tech superpowers can be bested by unsophisticated hackers.

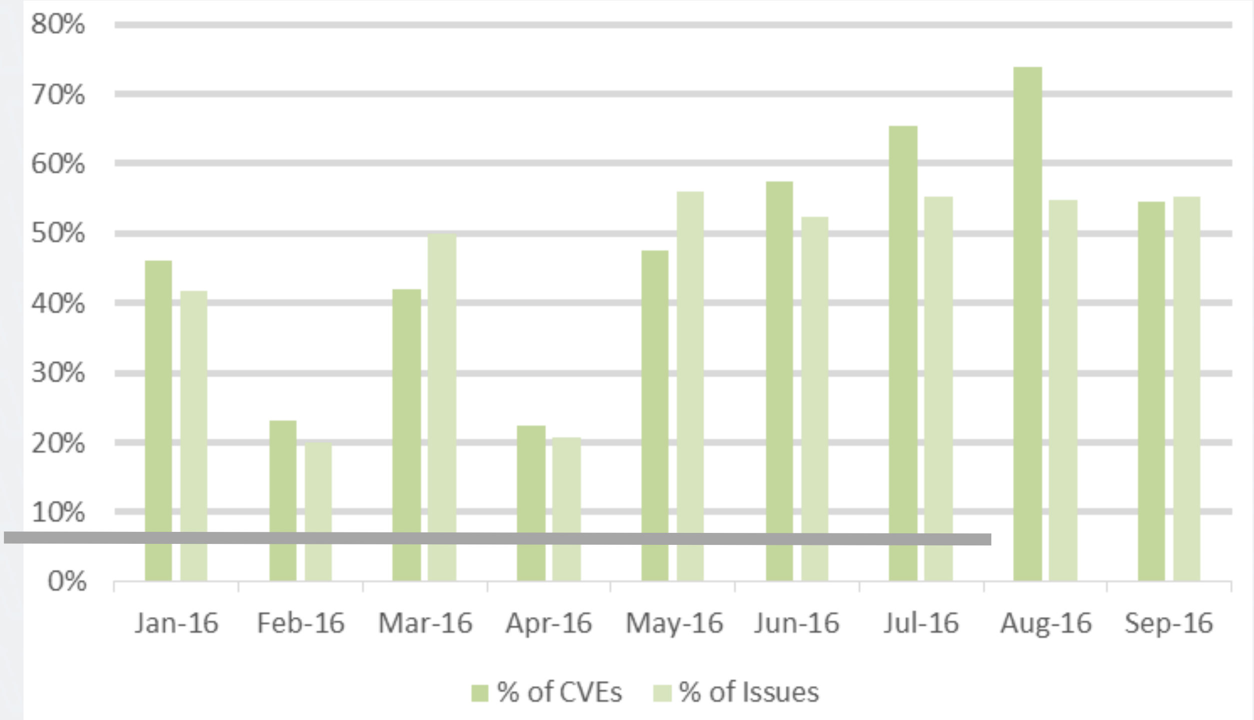
WIRED

TEEN WHO HACKED CIA DIRECTOR'S EMAIL TELLS HOW HE DID IT

Using social-engineering techniques to pull information from Verizon tech support

Software is Composed, Not Written

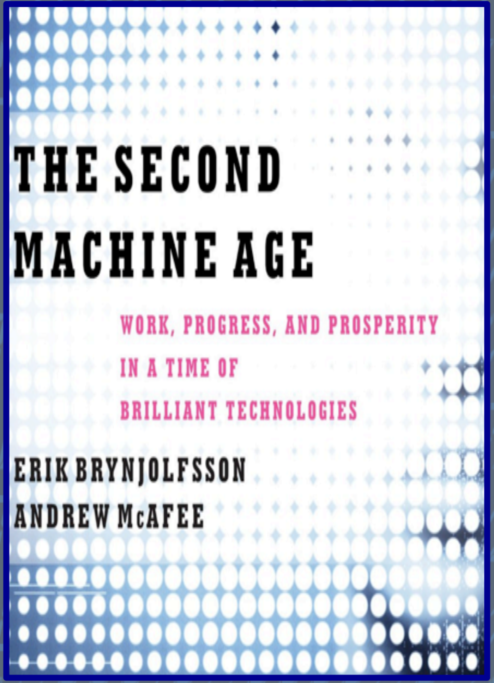
Proportion of Security Patches addressing Vulnerabilities in External Libraries and Drivers on the Google Android Platforms



Are We at an Inflection Point?

In the last 10 years alone, we have seen extraordinary advances …

- Self-driving cars
- Complex communication
- Natural language understanding
- Face recognition
- Language translation
- Watson and Jeopardy
- 3D printing and additive manufacturing
- Advanced robotics . . .


THE SECOND MACHINE AGE
WORK, PROGRESS, AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES
ERIK BRYNJOLFSSON
ANDREW McAFEE

Disruption of Markets and Industries

Technological innovations have always **disrupted the status quo** and underpinned dynamic economic change. *e.g., the steam engine, the printing press, electricity*

Today’s advances are catalyzing:

○ Disruption across many markets

○ Adoption at breathtaking speed and scale

○ Acceleration of economic impact

Power of digital innovation is that it is a “recombinant in its purest form.”

“Possibilities do not merely add up, they multiply.”

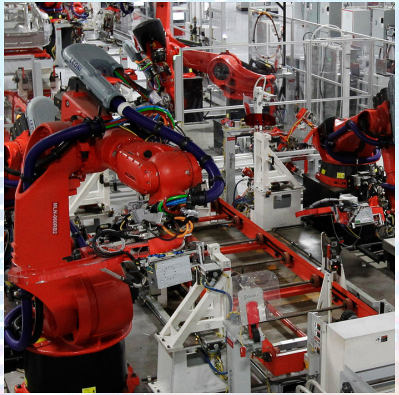
Paul Romer, Economist

Future security challenges will continue to follow technology trends and Internet adoption patterns.

Three Emerging Trends

Smart Systems
and IOT

Data Explosion and
Analytics

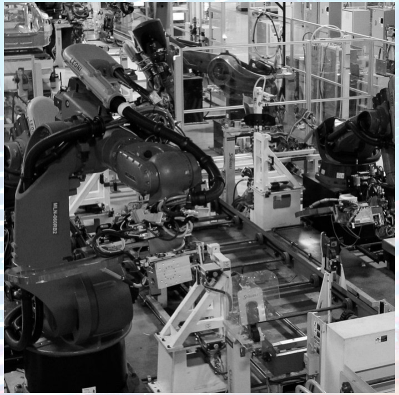


Autonomy and
Robotics

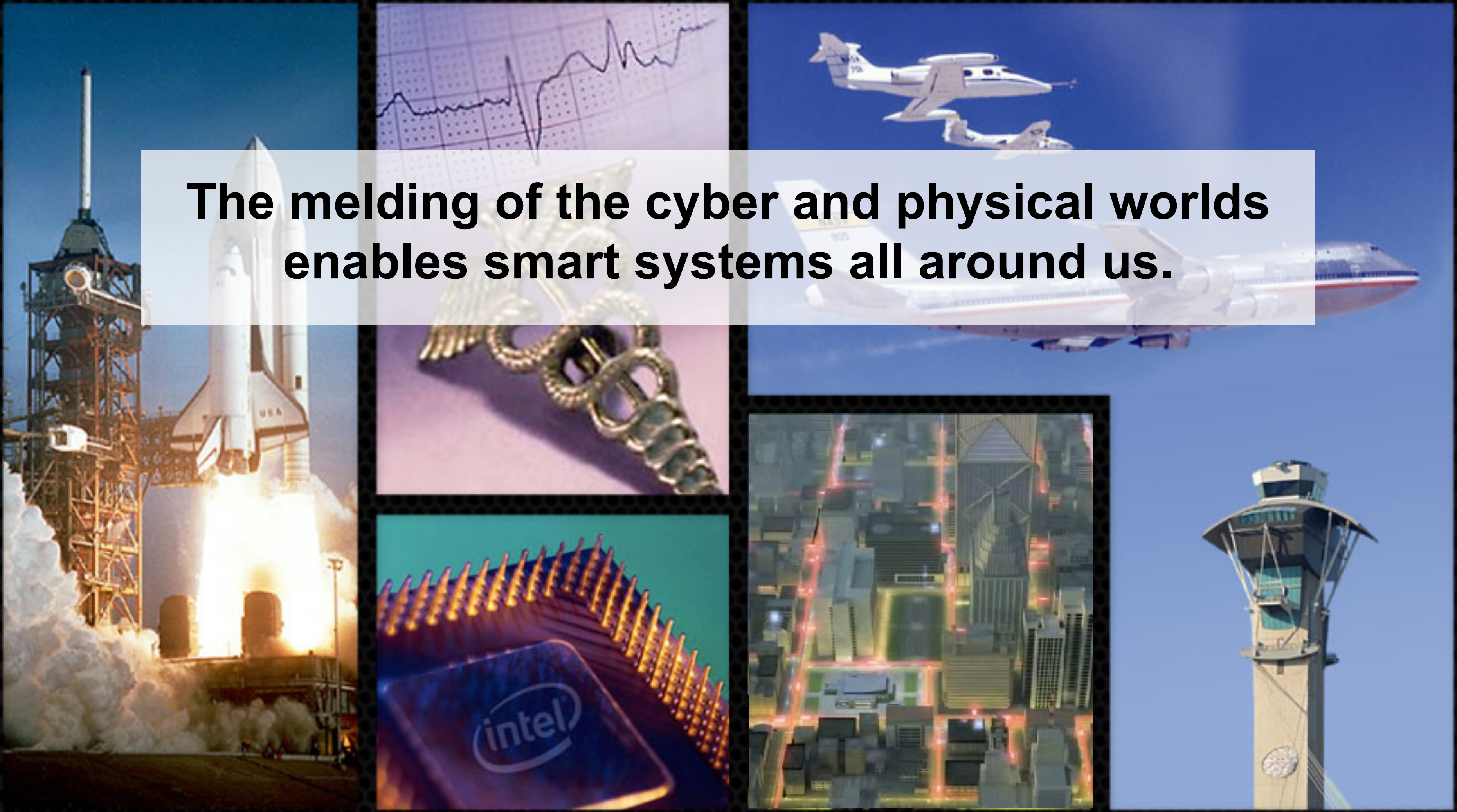
Three Emerging Trends

Smart Systems and IOT

Data Explosion and Analytics

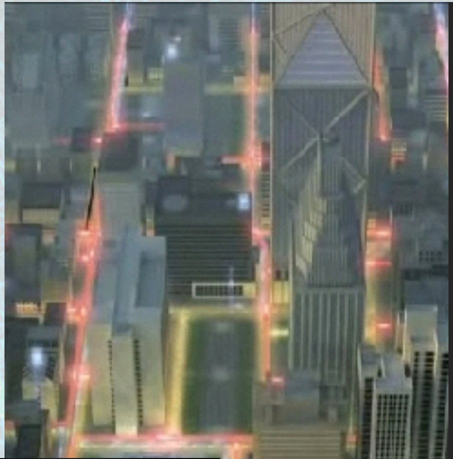


Autonomy and Robotics



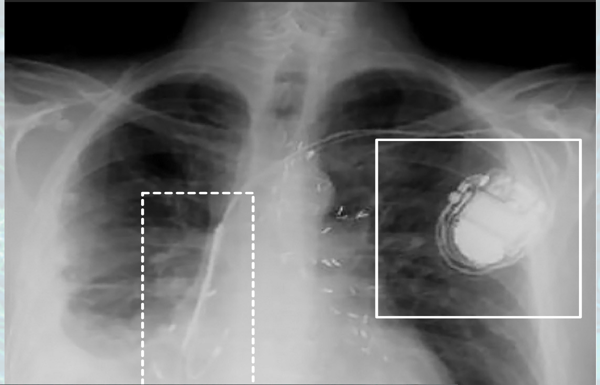
The melding of the cyber and physical worlds enables smart systems all around us.

Security of Cyber Physical Systems



Smart Grids

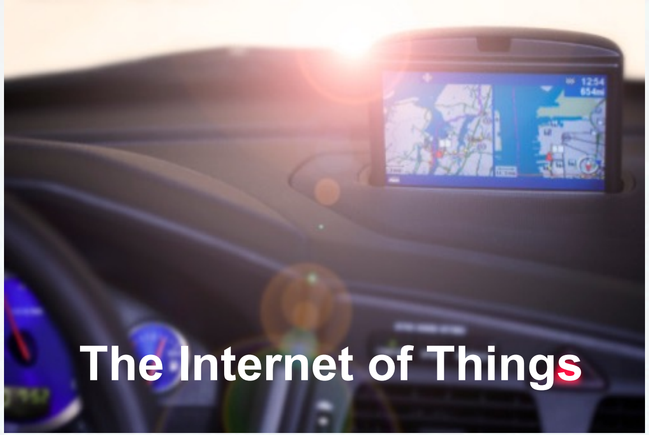
Embedded Medical Devices



Automobiles

Industrial Control

The Internet of Things

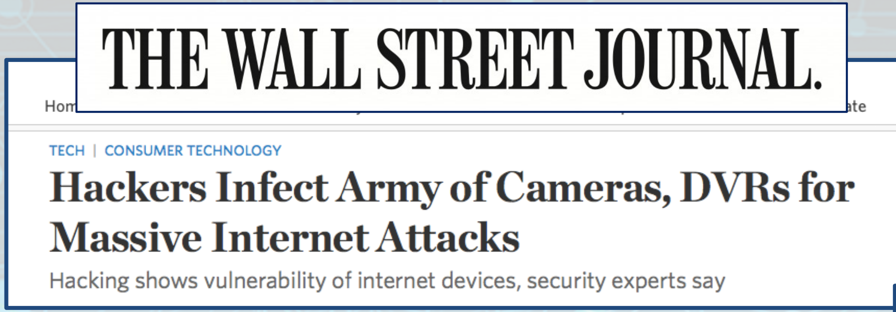


Digital Makeover of Physical Things: The Internet of *(Unsafe)* Things

Estimated **6.5B devices growing to 21B** by 2020, according to Gartner Research.

- Proliferation of devices designed to be controlled over the network
- Significant expansion of attack surface for exploitable vulnerabilities
- Consumer expectation: patch my thermostat and rice cooker?
- Market pressures on companies with limited secure software experience
- Memory and power issues to support heavy-weight security solutions
- Lack of standards and common interfaces

Mirai Malware

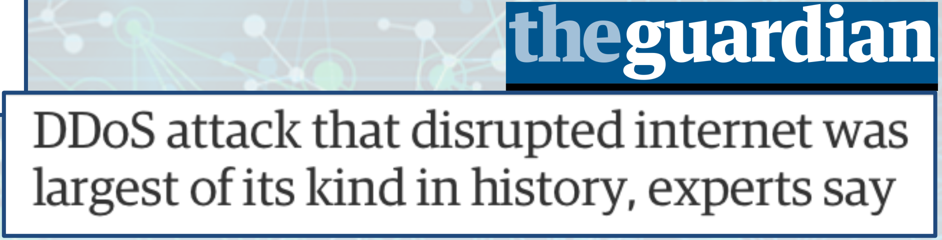


THE WALL STREET JOURNAL.

TECH | CONSUMER TECHNOLOGY

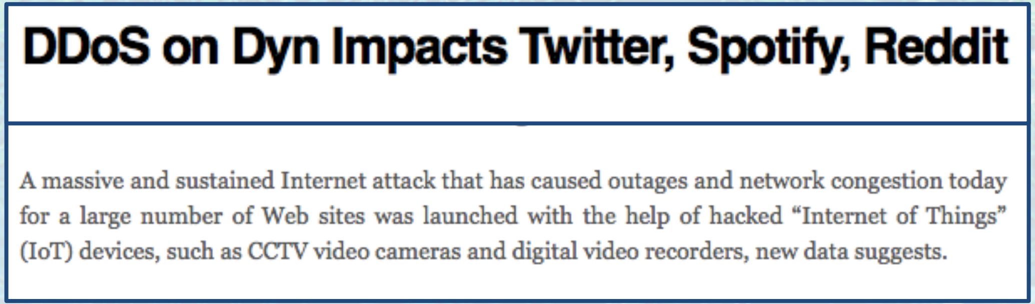
Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks

Hacking shows vulnerability of internet devices, security experts say



theguardian

DDoS attack that disrupted internet was largest of its kind in history, experts say

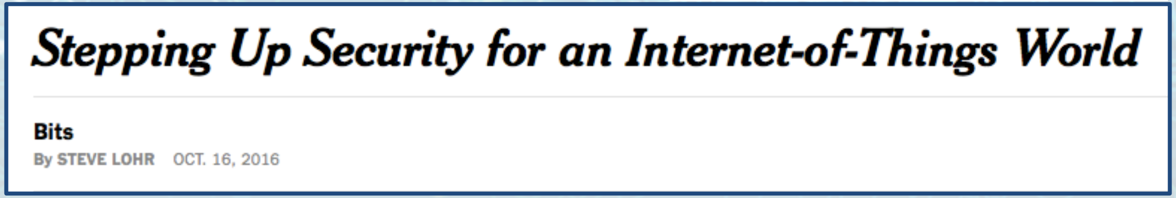


DDoS on Dyn Impacts Twitter, Spotify, Reddit

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

KrebsonSecurity
In-depth security news and investigation

The New York Times
NYTIMES.COM

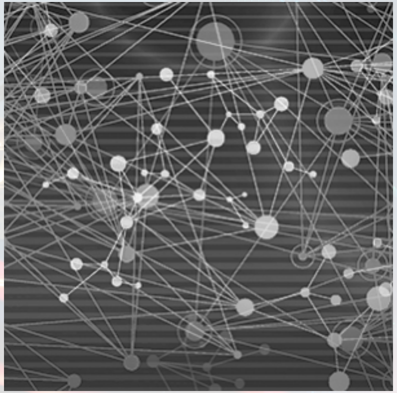


Stepping Up Security for an Internet-of-Things World

Bits

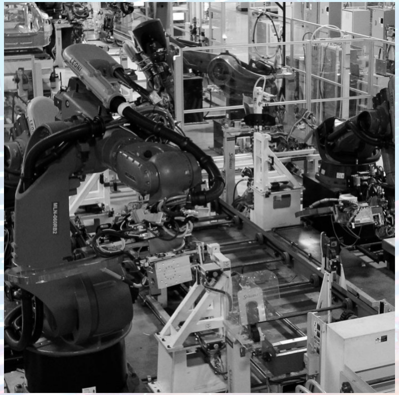
By STEVE LOHR OCT. 16, 2016

Three Emerging Trends



Smart Systems and IOT

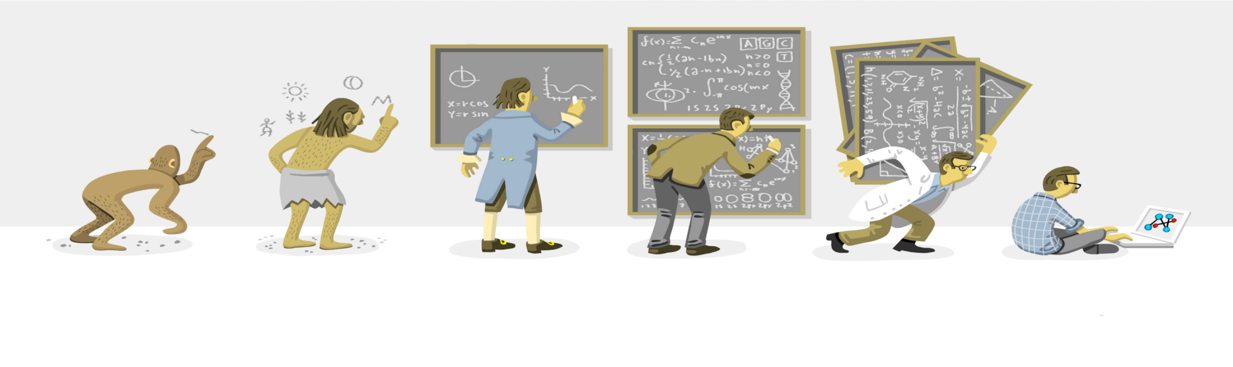
Data Explosion and Analytics



Autonomy and Robotics

Seizing the Big Data Revolution

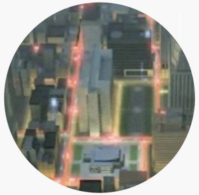
- Data Tsunami: **Explosive Growth** in Size, Complexity and Data Rates
  - Enabled by mobile phones, social media, email, videos, images, click streams, Internet transactions…and sensors everywhere!
- The Age of Data: **From Data to Knowledge to Action**
  - Widespread use of data to create actionable information leads to timely and more informed decisions and actions.



Extracting Knowledge from Data

Classifying Breast Cancers via Image Analysis

Energy Savings in the Homes and Buildings

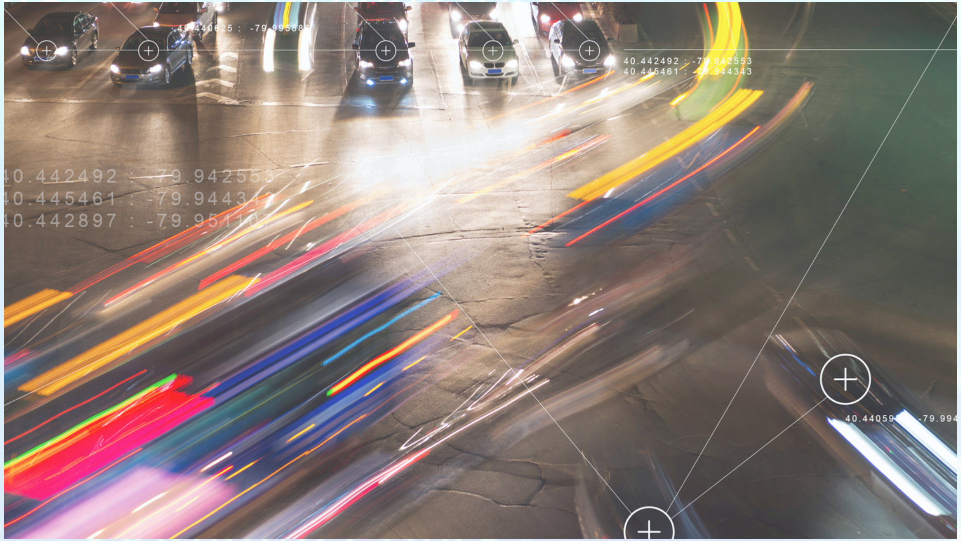


Reducing Traffic Congestion in Urban Areas

Machine Learning and Predictive Analytics

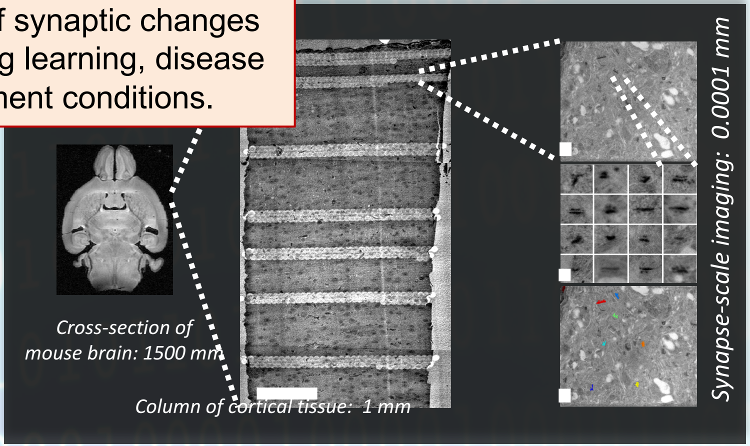
- How can one construct computer systems that **automatically learn** and **improve** through **experience**?

- **Evidence-based decision making** and policy formulation in healthcare, education, public safety, urban services, and marketing.

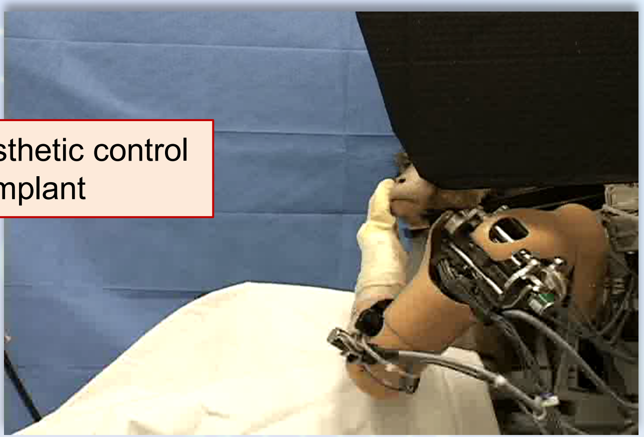


Analysis of social media and Google searches to track flu epidemics and potential spread of infectious diseases in near real-time.

Identifying new brain areas and specific types of synaptic changes that occur during learning, disease states, or treatment conditions.


Cross-section of mouse brain: 1500 mm
Column of cortical tissue: 1 mm
Synapse-scale imaging: 0.0001 mm

Learning to extract information from text and answer questions.



Learning prosthetic control from neural implant

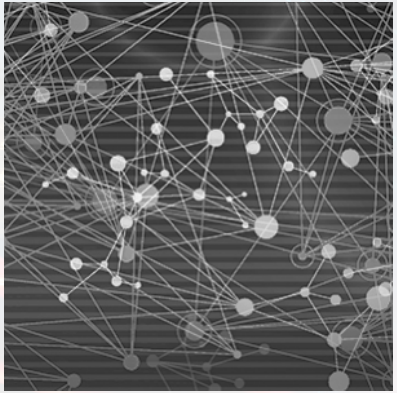
Big Data and Security

- Big data is a **big security target**:
  - Apple has **500+ million** customer credit cards on file
  - Facebook has over **1.75 billion users** sharing 1+ billion pieces of content every day (2016)
- No longer about protecting internal data
- Impact of platforms and ecosystems:
  - More than 2 million apps in the AppStore
  - **How secure are partner platforms and third-party apps**?

Machine Learning and Security

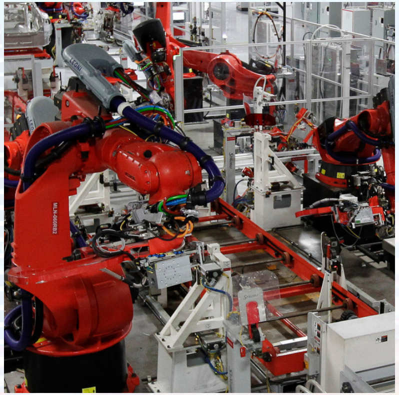
- The **need for research** on the adversarial machine learning problem
- Data or analysis may be manipulated directly or indirectly (e.g. impact of fake news in changing public opinion)
- Data provenance
- An adversary can “game” the system to **evade detection** or **create false alarms**
- Can machine learning techniques be applied to cyber security problems?
- **Not a silver bullet**, but may help to provide context for better decision making

Three Emerging Trends



Smart Systems and IOT

Data Explosion and Analytics



Autonomy and Robotics

Emerging Frontiers

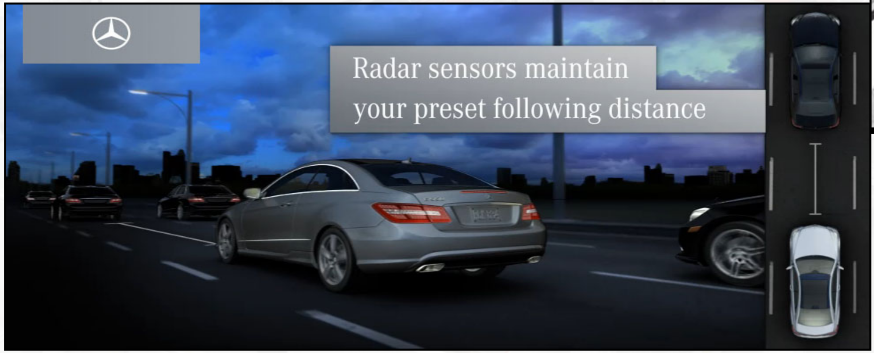
Robotics and Automation

- Increasingly capable robots with **enhanced senses, dexterity and intelligence** used to automate tasks, augment human capabilities or work beside and cooperatively with people
- **Autonomous vehicles** that can navigate and operate with reduced or no human intervention
- Applications extend beyond industrial automation to **services**, **personal safety**, **surgery**, **emergency response** and even **human augmentation**

The Future is Here

Lane departure warning

Self-parking

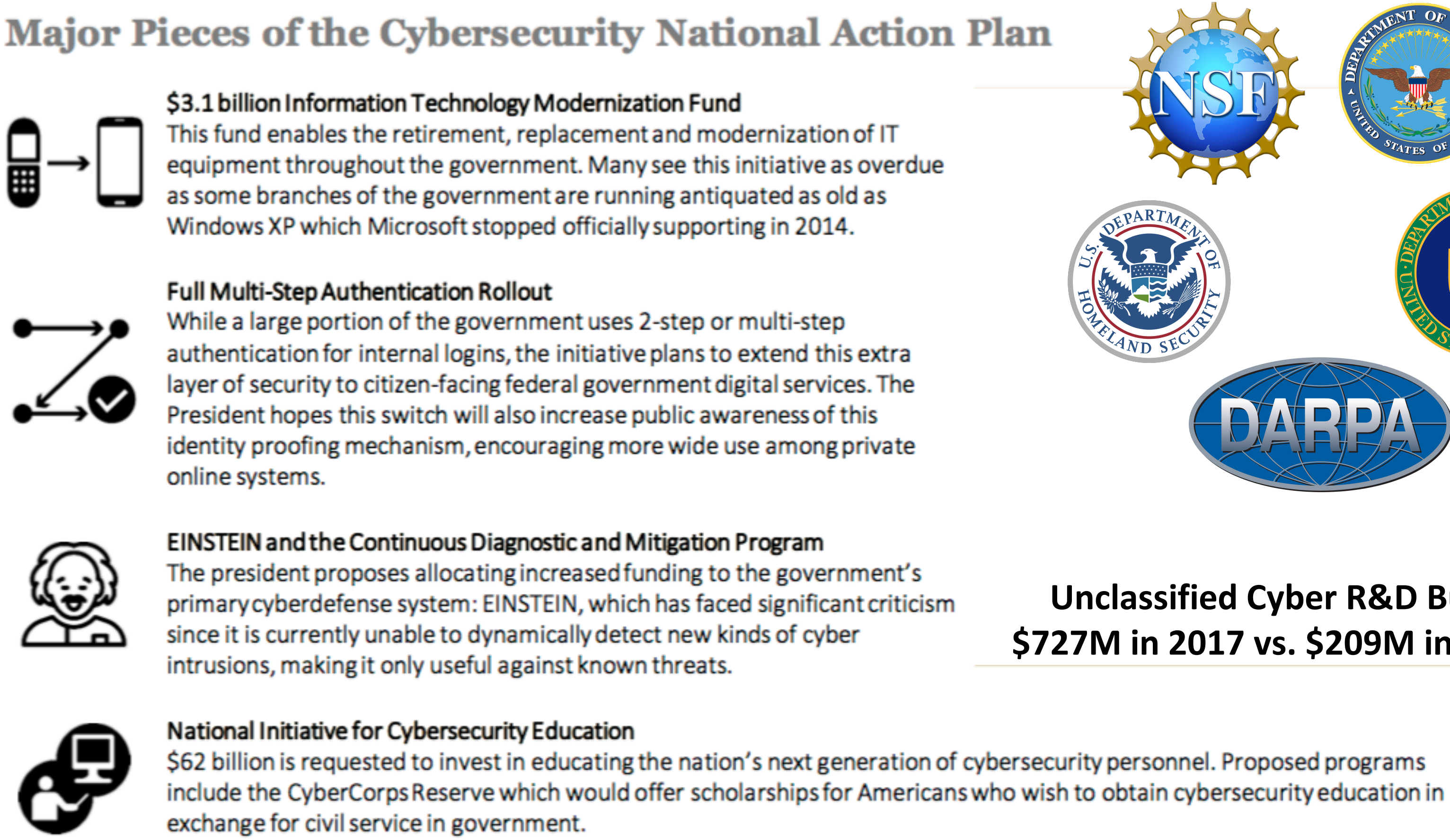


Adaptive cruise control

Where Do We Go From Here?

Federal R&D Budget: “Cyber Security and Privacy” is a National Priority

President Obama's $19 Billion Cybersecurity Proposal Calls for 35% Increase Over 2016 Enacted Level



Major Pieces of the Cybersecurity National Action Plan

$3.1 billion Information Technology Modernization Fund

This fund enables the retirement, replacement and modernization of IT equipment throughout the government. Many see this initiative as overdue as some branches of the government are running antiquated as old as Windows XP which Microsoft stopped officially supporting in 2014.

Full Multi-Step Authentication Rollout

While a large portion of the government uses 2-step or multi-step authentication for internal logins, the initiative plans to extend this extra layer of security to citizen-facing federal government digital services. The President hopes this switch will also increase public awareness of this identity proofing mechanism, encouraging more wide use among private online systems.

EINSTEIN and the Continuous Diagnostic and Mitigation Program

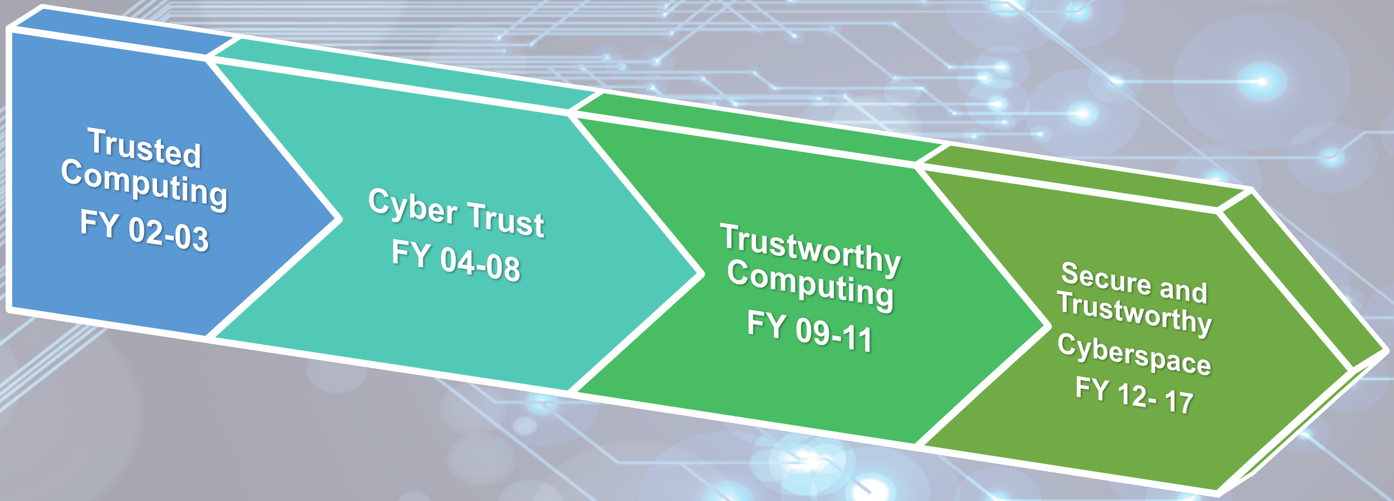
The president proposes allocating increased funding to the government's primary cyberdefense system: EINSTEIN, which has faced significant criticism since it is currently unable to dynamically detect new kinds of cyber intrusions, making it only useful against known threats.

National Initiative for Cybersecurity Education

$62 billion is requested to invest in educating the nation's next generation of cybersecurity personnel. Proposed programs include the CyberCorps Reserve which would offer scholarships for Americans who wish to obtain cybersecurity education in exchange for civil service in government.

Unclassified Cyber R&D Budget
$727M in 2017 vs. $209M in FY2008

NSF Cyber Security Programs Over Time



Trusted Computing
FY 02-03

Cyber Trust
FY 04-08

Trustworthy Computing
FY 09-11

Secure and Trustworthy Cyberspace
FY 12- 17

Secure and Trustworthy Cyberspace Program

Securing Cyberspace and Critical Infrastructure

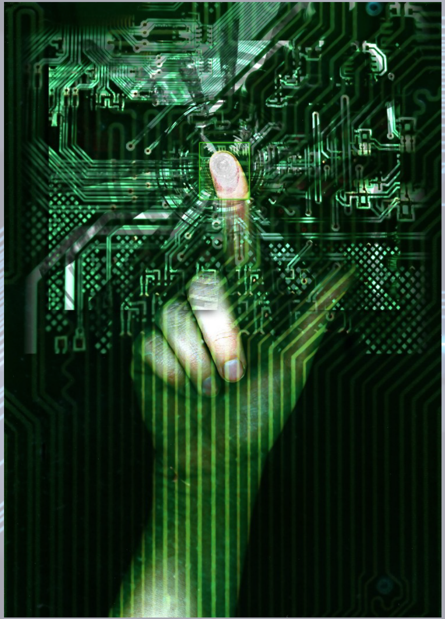


Image Credit: *ThinkStock*

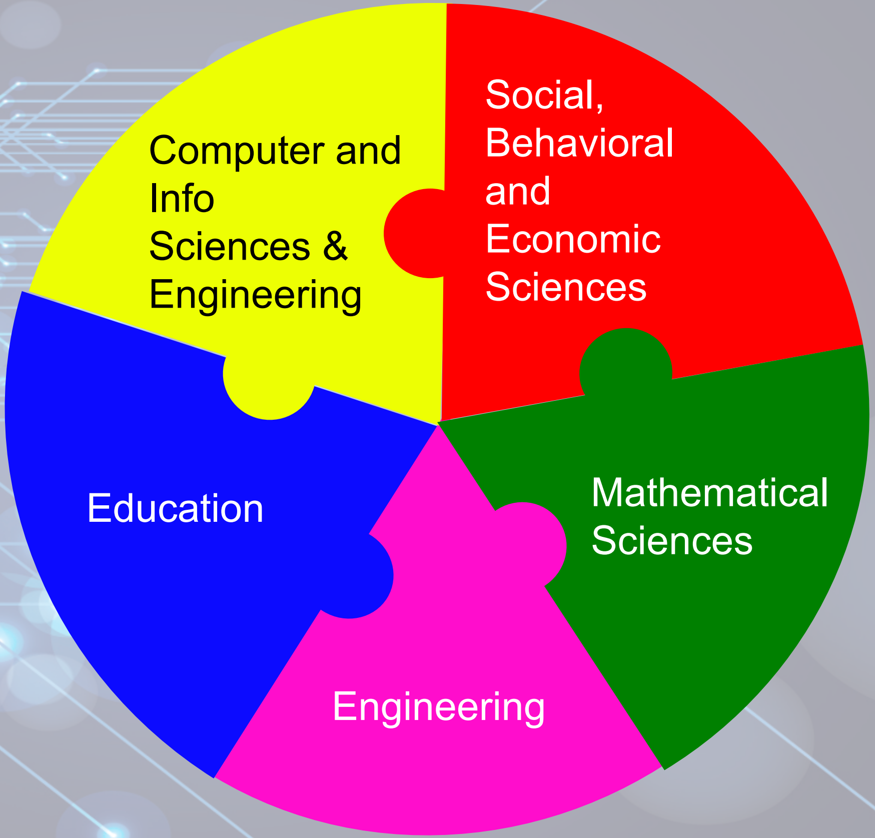
NSF program aims to support fundamental scientific advances and technologies to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability.

SaTC Program:	$ 80M
Scholarship for Service (SFS):	$ 50M
NSF 2016 total investment:	$160M

Secure and Trustworthy Cyberspace Program

Cross-directorate interdisciplinary community of security and privacy researchers and practitioners:

- Core foundational research in S&P
- Transition to Practice (TTP)
- Cybersecurity Education
- *Frontiers* support center-scale activities
- Joint programs with Intel and SRC


Computer and Info Sciences & Engineering
Social, Behavioral and Economic Sciences
Education
Mathematical Sciences
Engineering

The Need for Large-Scale Integration, Experimentation and Evaluation

DARPA AV Grand Challenges

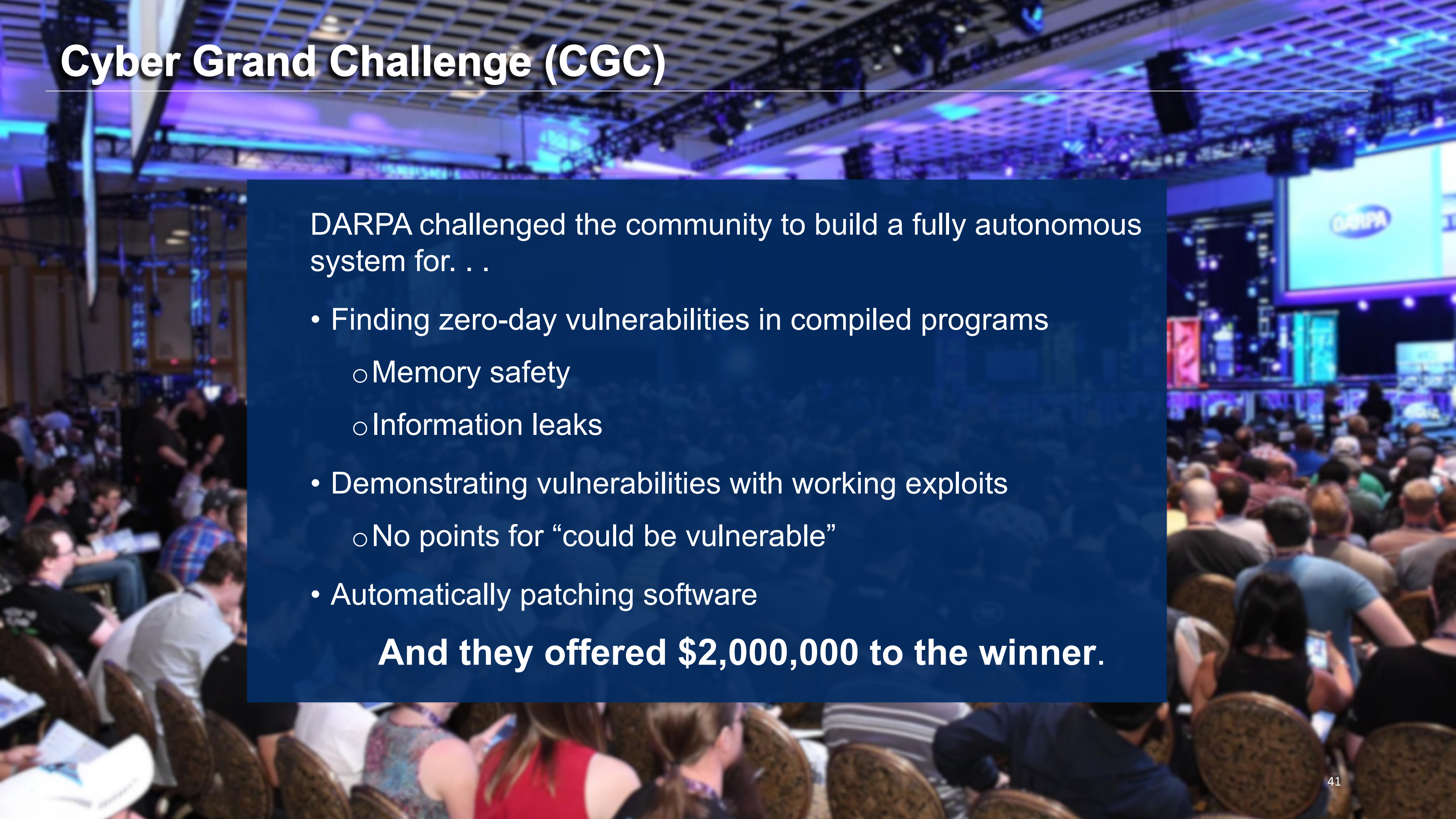
2004 Sandstorm

Today's Uber

2007 Boss

2011 Cadillac SRX

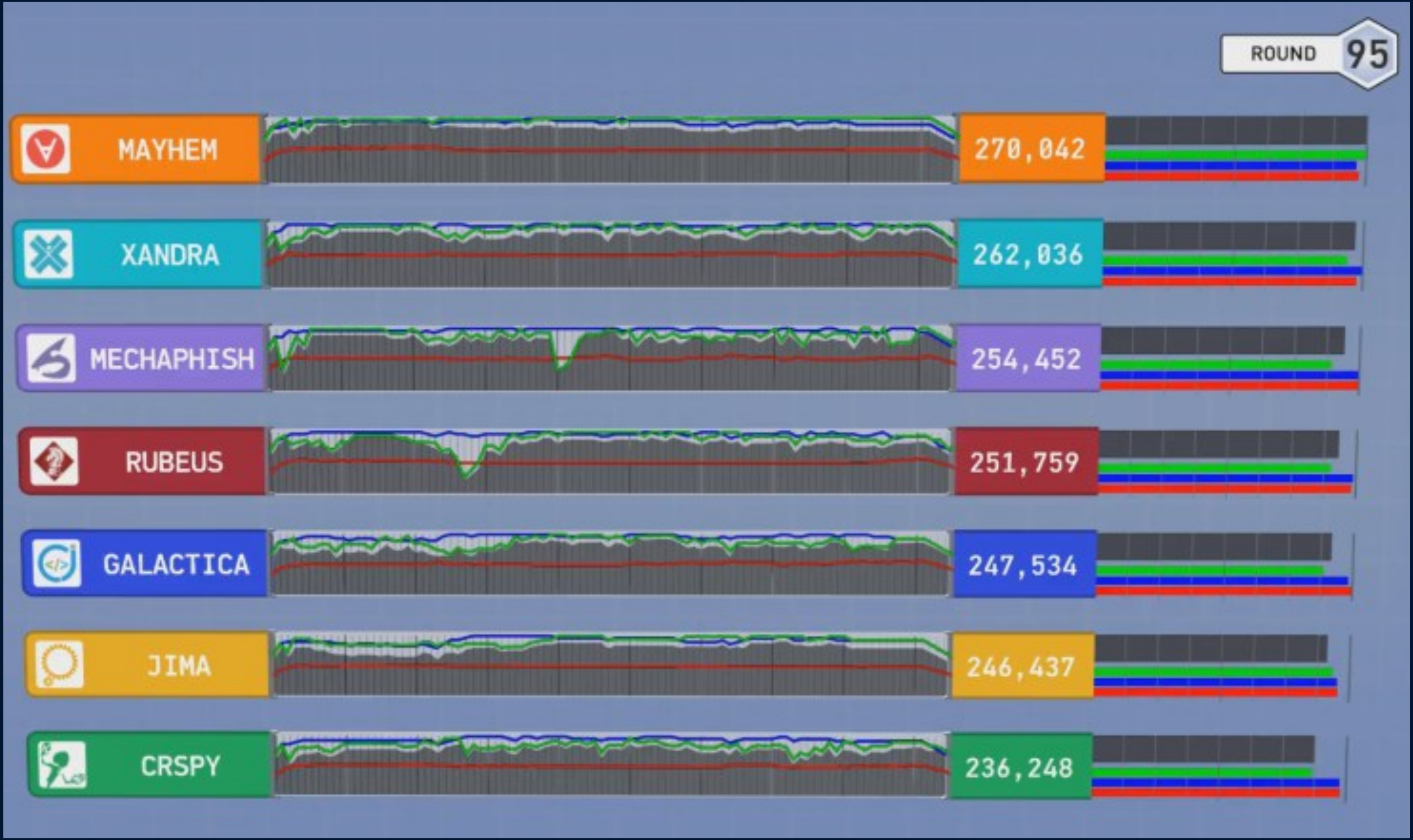
Cyber Grand Challenge (CGC)



DARPA challenged the community to build a fully autonomous system for. . .

- Finding zero-day vulnerabilities in compiled programs
    - Memory safety
    - Information leaks
- Demonstrating vulnerabilities with working exploits
    - No points for “could be vulnerable”
- Automatically patching software

And they offered $2,000,000 to the winner.



ROUND 95

MAYHEM	270,042
XANDRA	262,036
MECHAPHISH	254,452
RUBEUS	251,759
GALACTICA	247,534
JIMA	246,437
CRSPY	236,248

Security Hygiene, Best Practices, and Technology Transfer

In theory, there is no difference between theory and practice. In practice, there is.

- Yogi Berra

Countless Vulnerable and Mismanaged Assets

Open recursive DNS resolver	***27 million*** open recursive resolver
DNS source port randomization	***226,976 (4.8%)*** DNS resolvers without using source port randomization
Consistent A and PTR records	***27.4 million (23.4%)*** A records that do not have matching PTR records
BGP misconfiguration	***42.4 million (7.8%)*** short-lived BGP routes
Lack of Egress Filtering	***35.6%*** tested netblocks that have not implemented egress filtering
Untrusted HTTPS Certificates	***10.2 million (52%)*** HTTPS servers using untrusted certificates
Open SMTP mail relays	***22,284 (2%)*** SMTP servers that allow open mail relays
Publicly available IPMI cards	***98,274*** public accessible IPMI cards

There is wide-spread realization that single factor authentication (i.e., password) is not secure enough!

? *Why isn’t two-factor authentication more pervasively deployed?*

Gap between Research, Innovation and Practice

- Growing R&D Investments in universities, research labs and commercial vendors … significant scientific progress and egineering advances
- What are the disincentives for technology adoption?
- Why is practicing security hygiene so hard?
- What are the barriers to technology transfer?
- Social, behavioral, economic and policy factors?
- Push vs. Pull Model: Incentives for push vs. Demand creation for pull

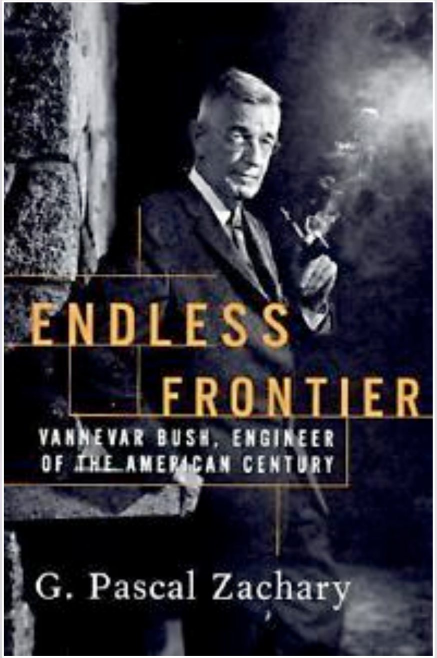
Concluding Remarks

- We don’t do the easy stuff well, and the hard stuff is getting harder.
- The hard stuff, future security challenges, will continue to follow technology trends and Internet adoption patterns.
- These challenges call for:
    - Continued investments in cyber security and privacy
    - Large-Scale Integration, Experimentation and Evaluation
    - Bridge the gap between research, innovation and practice

Lessons from the Past

Vannevar Bush’s vision of the endless frontier:

> Basic research is “the pacemaker of technological progress” and “[n]ew products and new processes do not appear full-grown. They are founded on new principles and new conceptions, which in turn are painstakingly developed by research in the purest realms of science!”



Thank You!