

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



From Star Trek to Star Wars: The Force Awakens - The Importance of Hardware and IP Security

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

Carl E. McCants, Ph.D.
Program Manager
5 May 2016

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)



Outline

- Introduction
- What is IARPA?
- Hardware security themes from science fiction
 - Star Trek
 - Star Wars: The Force Awakens
- Hardware and IP security
- Summary



What is IARPA?



Office of the Director of National Intelligence

Central Intelligence Agency

Defense Intelligence Agency

Department of State

National Security Agency

Department of Energy

National Geospatial-Intelligence Agency

Department of the Treasury

National Reconnaissance Office

Drug Enforcement Administration

Army

Federal Bureau of Investigation

Navy

Department of Homeland Security

Air Force

Coast Guard

Marine Corps





IARPA Mission and Method

IARPA's mission is to invest in high-risk/high-payoff research to provide the U.S. with an overwhelming intelligence advantage

- **Bring the best minds to bear on our problems**
 - Full and open competition to the greatest possible extent
 - World-class, rotational Program Managers
- **Define and execute research programs that:**
 - Have goals that are clear, measureable, ambitious and credible
 - Employ independent and rigorous Test & Evaluation
 - Involve IC partners from start to finish
 - Run from three to five years
 - Publish peer-reviewed results and data, to the greatest possible extent



Operations R&D

“Operate effectively in a globally interdependent and networked environment”

Computational Power

Revolutionary advances in science and engineering to solve problems intractable with today’s computers

Trustworthy Components

Gain the benefits of leading-edge hardware and software without compromising security

Safe and Secure Systems

Protecting systems against cyber threats



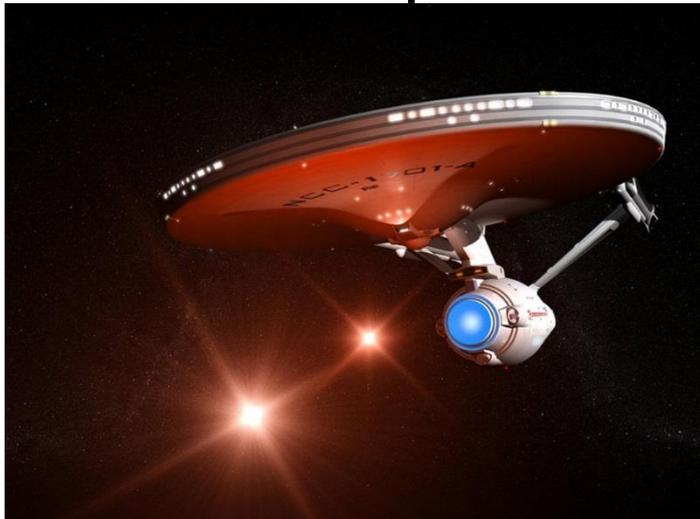
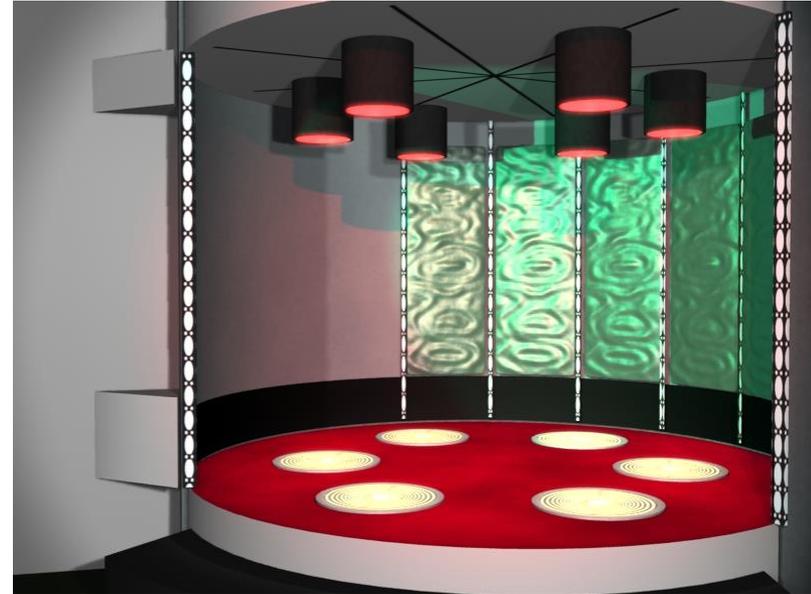
Hardware Security Themes from Science Fiction



Star Trek

Star Trek TOS icons

- Communicator
- Tricorder
- Transporter
- Phaser
- Photon Torpedo



Courtesy Paramount Pictures



Star Trek TOS communicator

- The communicator allowed direct contact between individuals or via a ship's communication system.
- The communicator allowed crew members to contact starships in orbit without relying on a satellite.
- Communicators used subspace transmissions that did not conform to normal rules of physics in that signals typically bypassed EM interference, and allowed instantaneous communication.



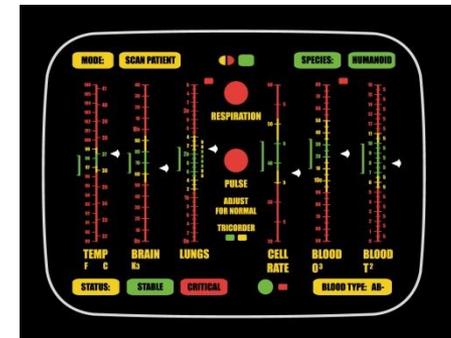
Courtesy Paramount Pictures

Star Trek TOS tricorder

- The tricorder was a multifunction handheld device used for sensor scanning, data analysis, and recording data.
- The standard tricorder was a general-purpose device used primarily to scout unfamiliar areas, make detailed examination of living things, and record and review technical data.
- The medical tricorder was used by doctors to help diagnose diseases and collect bodily information about a patient.
- The engineering tricorder was fine-tuned for starship engineering purposes.



Courtesy Paramount Pictures



Source: <http://en.wikipedia.org/wiki/Tricorder>



What is the theme and security implication?

- Instantaneous, ubiquitous communication
- Unlimited information acquisition
- Instantaneous data analysis and display for actionable intelligence
- Unlimited, instantaneous database access
- Instruments that the Klingons, Romulans, and others could not analyze...



Star Wars: The Force Awakens



Star Wars: The Force Awakens Overview



Source: <http://www.starwars.com/news/star-wars-the-force-awakens-theatrical-poster-first-look-in-theater-exclusives-and-more>



Star Wars: The Force Awakens

Thirty years after the defeat of the Galactic Empire, the galaxy faces a new threat from the evil Kylo Ren (Adam Driver) and the First Order. When a defector named Finn crash-lands on a desert planet, he meets Rey (Daisy Ridley), a tough scavenger whose droid contains a top-secret map. Together, the young duo joins forces with Han Solo (Harrison Ford) to make sure the Resistance receives the intelligence concerning the whereabouts of Luke Skywalker (Mark Hamill), the last of the Jedi Knights.

Source: <https://www.google.com/#q=star+wars+the+force+awakens>



Source: <http://www.forbes.com/sites/jvchamary/2015/12/30/how-bb8-works-star-wars/#539e4ee52ab2>



Hardware and IP Security

What we face...



Source: <http://dilbert.com/strips/comic/2004-10-28/>



Where we were... in 2008

Recognizing this enormous vulnerability, the DOD recently launched its most ambitious program yet to verify the integrity of the electronics that will underpin future additions to its arsenal. In December, the Defense Advanced Research Projects Agency (DARPA), the Pentagon's R&D wing, released details about a three-year initiative it calls the Trust in Integrated Circuits program. The findings from the program could give the military--and defense contractors who make

SEMICONDUCTORS / DESIGN

FEATURE

The Hunt for the Kill Switch

Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out

By SALLY ADEE / MAY 2008

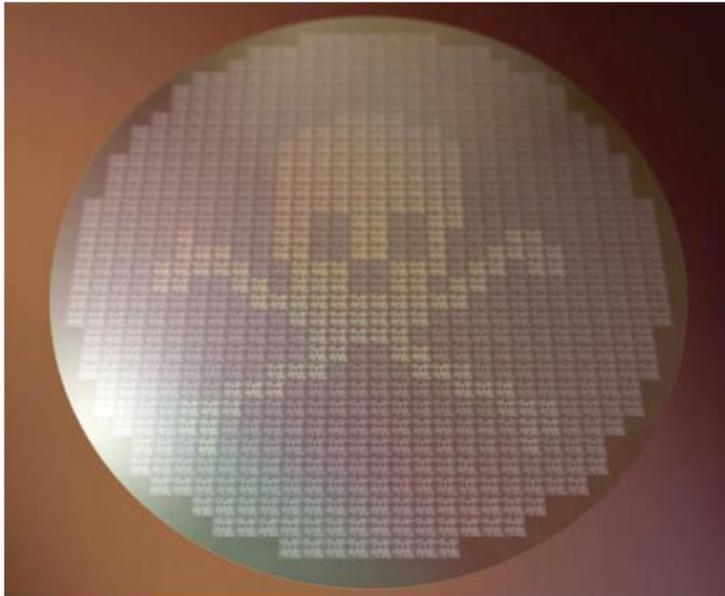


Photo: James Archer/AnatomyBlue

Last September, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar--supposedly state-of-the-art--to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare--and not just any kind.

Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the

The Hunt for the Kill Switch - IEEE Spectrum

<http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the->

Where we were... in 2010

A Survey of Hardware Trojan Taxonomy and Detection

Mohammad Tehranipoor
University of Connecticut

Farinaz Koushanfar
Rice University

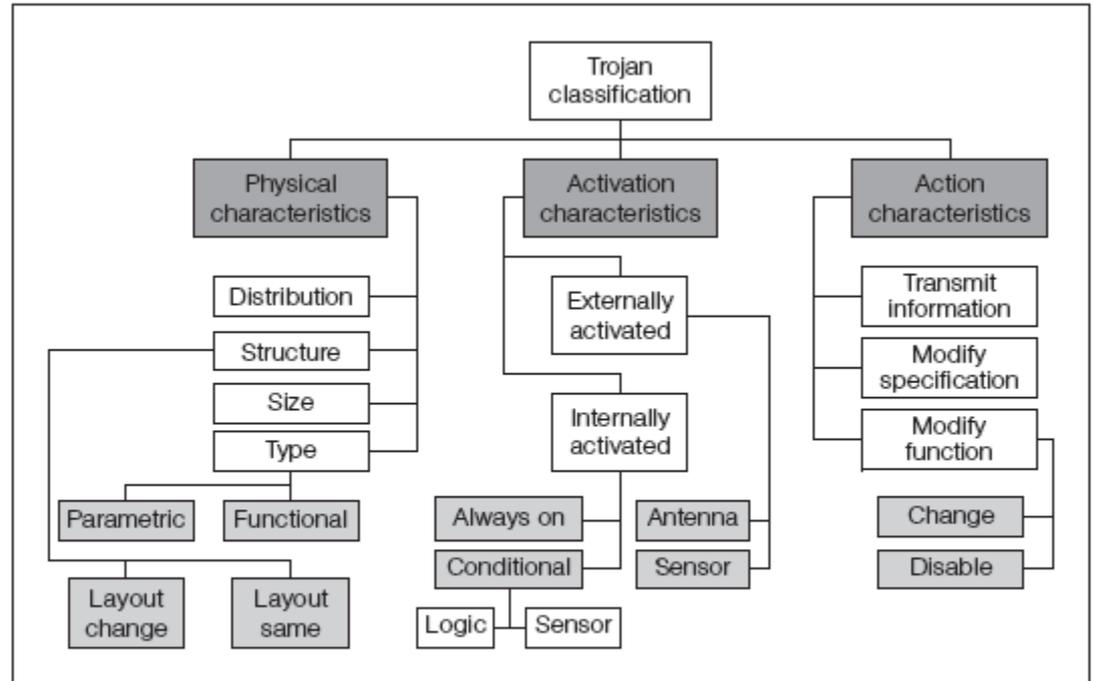


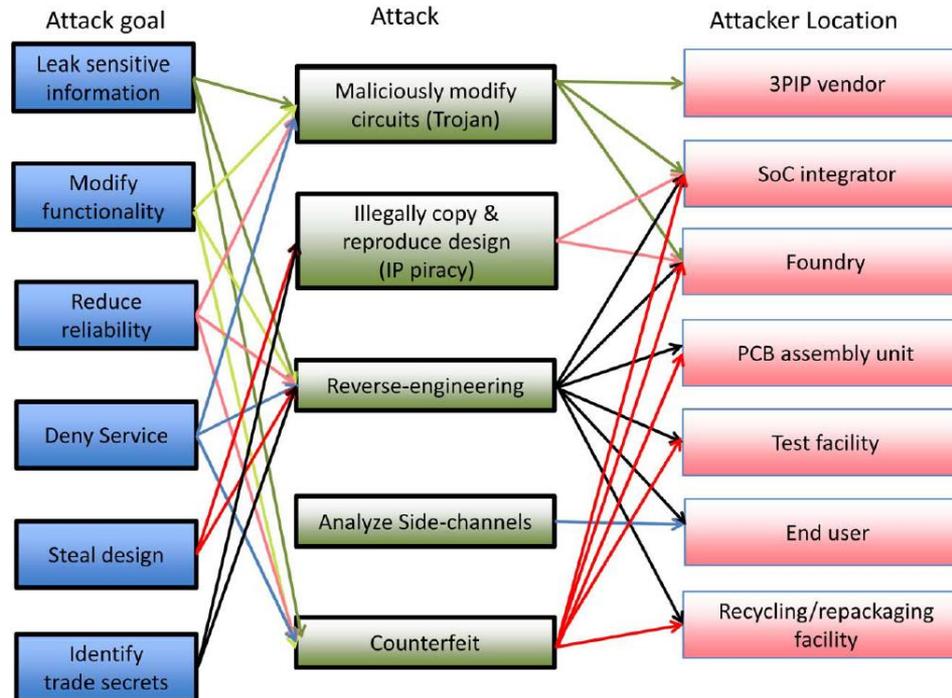
Figure 1. Detailed taxonomy showing physical, activation, and action characteristics of Trojans. (Source: Wang et al.⁵)

Where we were... in 2014

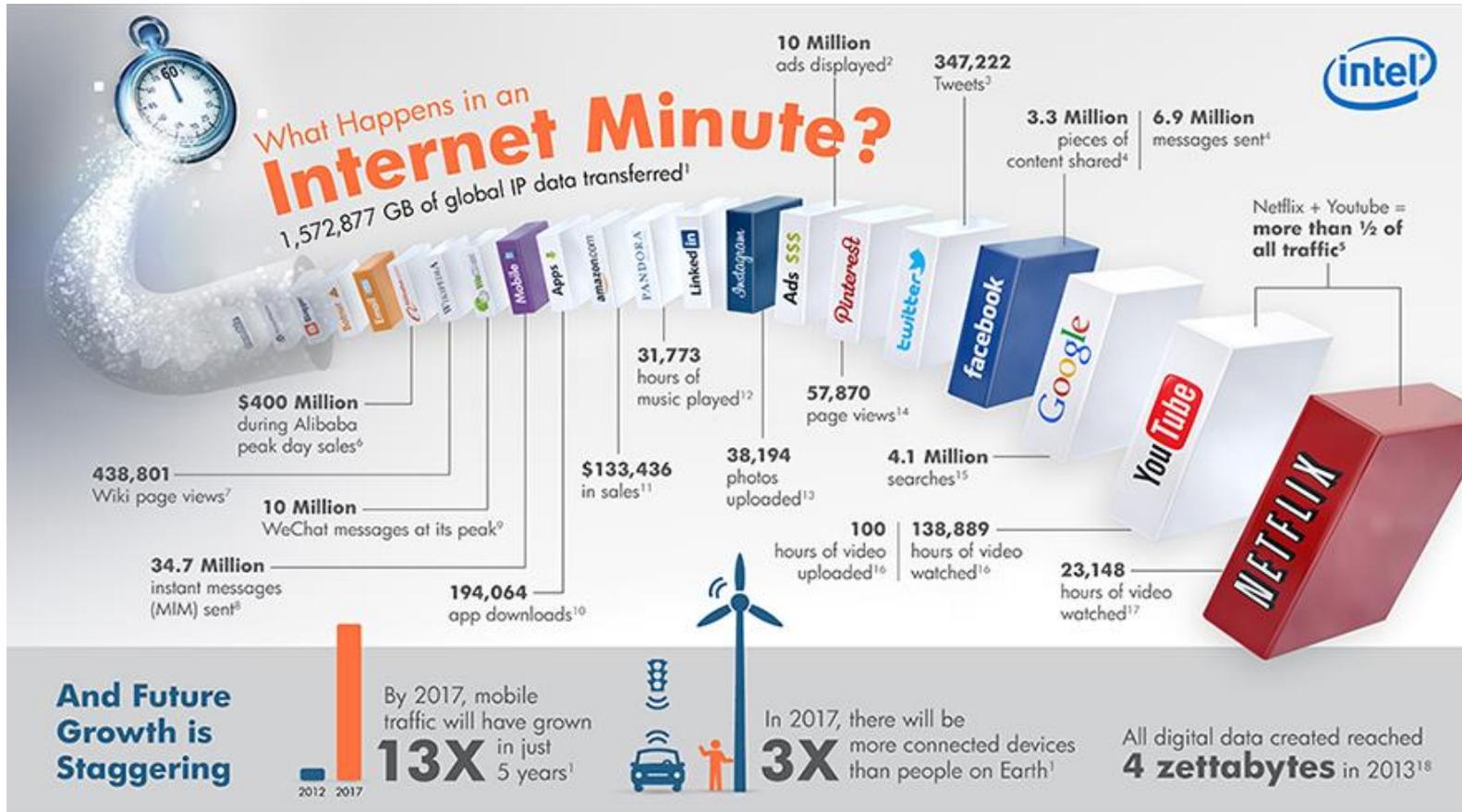
A Primer on Hardware Security: Models, Methods, and Metrics

The paper is a primer on hardware security threat models, metrics, and remedies.

By MASOUD ROSTAMI, FARINAZ KOUSHANFAR, AND RAMESH KARRI



Where we were... in 2014

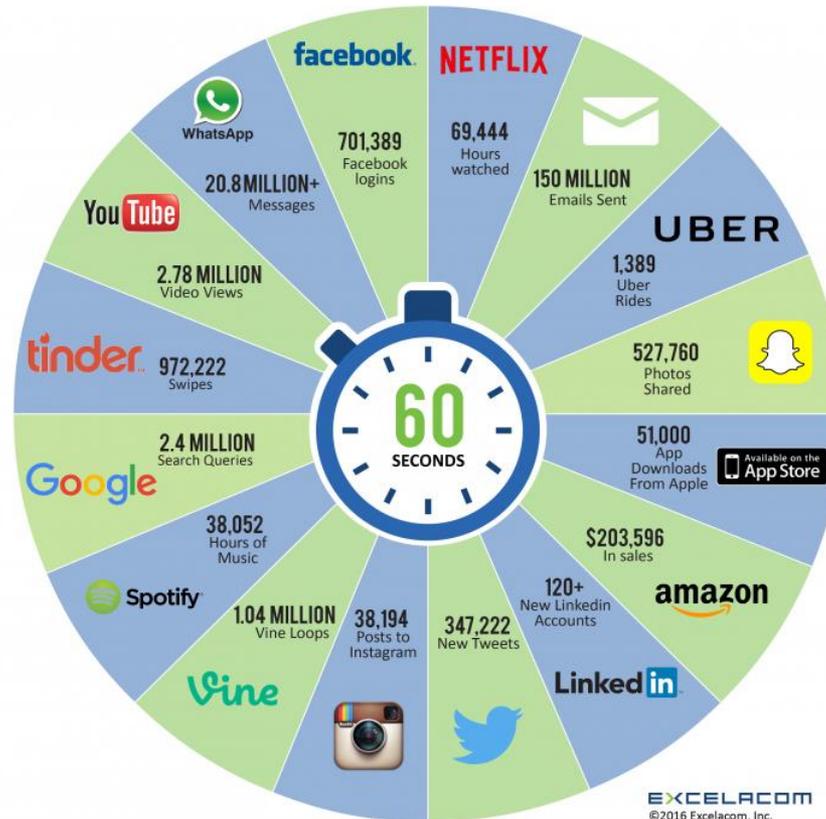


Source: <http://www.intel.com/content/www/us/en/communications/internet-minute-infographic.html>



Where we are now...

2016 What happens in an INTERNET MINUTE?



EXCELACOM
©2016 Excelacm, Inc.

Source: <http://www.excelacom.com/resources/blog/2016-update-what-happens-in-one-internet-minute>



Where we are now...

IARPA Trusted Integrated Chips (TIC) Program

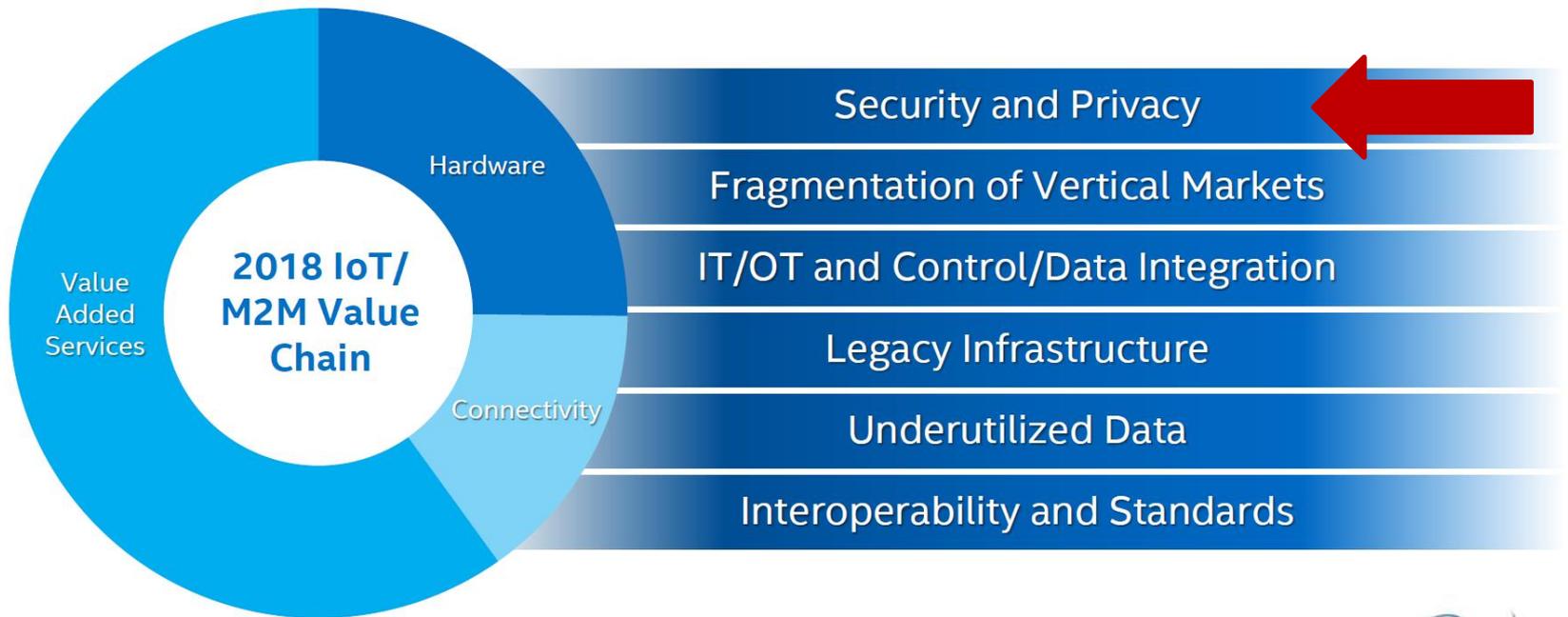
Vision

- Ensure the U.S. Government can obtain the highest performance possible in integrated circuits which are often derived from commercial foundries, not just through U.S. trusted foundries.
- Obtain assurance that designs are safe and secure – not compromised with malicious circuitry.
- Ensure security of designs, capability, and performance while simultaneously protecting intellectual property.
- Realize secure systems combining advanced CMOS with higher value chips.



Where we are headed...

IoT Growth - Challenges and Opportunities



Intel Technology Conference 2014

Intel Confidential

Source: ABI Research*

*Other names and brands may be claimed as the property of others.





Summary



Summary

- Hardware security research has made significant advances to the state-of-the-art and state-of-the-practice over the past 8 years
- The “Internet of Things” with its increased connectivity and analytics capabilities will require new approaches to hardware security.
- IARPA is interested in relevant research ideas and program managers to implement and execute these ideas...



The ultimate goal...



Source: <http://cloudtweaks.com/2016/03/att-achieving-security-internet-things/>



Questions?



"We'd now like to open the floor to shorter speeches disguised as questions."

Source: <http://www.newyorker.com/cartoons/a15376>