

Cyber Physical System Security (CPSSEC)

Industry Day Briefing

26 June 2014

Dr. Dan Massey

Program Manager

Cyber Security Division

Science and Technology Directorate



**Homeland
Security**

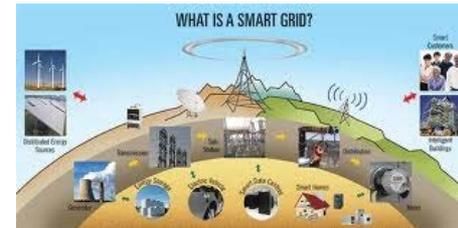
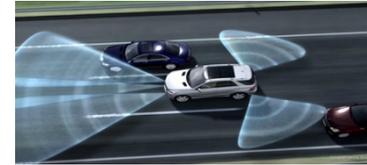
Science and Technology

CPSSEC Overview

Presidential Policy Directive 21 Identifies critical infrastructure as “interdependent functions and systems in both the physical space and cyberspace” and aims to strengthen security and resilience “against both the physical and cyber attacks”

Cyber Physical Systems Are Becoming Ubiquitous:

- Smart cars, smart grids, smart medical devices, smart manufacturing, smart homes, and so on
- You will “bet your life” on many of these systems
- Fast moving field focusing on functionality now and *will bolt on security later...*

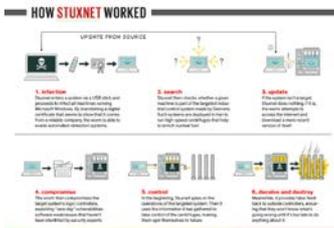


Drones Could Help Tulsa Firefighters During Search, Rescue



Need to ***Build Security In*** at this Early Stage

- Promote security at onset
- Connect research and industry
- Enable security as integral component



Department of Premarket Submission Management of Cybersec in Medical Devices
Guidance for Industry and Drug Administration Staff
DRAFT GUIDANCE Document Issued

Opportunity Now To Build Security Into Emerging Cyber Physical Designs

Problem: Building In Security

Emerging CPS designs haven't identified threats, are full of vulnerabilities, and *lack security as integral part of design*:

- Industry driven by functional requirements and fast moving market
- Research disconnected from market drivers and tangible security problems
- Security concerns cross company and even sector boundaries, requiring shared solutions
- Increasing number of interconnected systems where you bet your life that security can be added later

ARPAnet design goals by Clark in 1988

- Function despite loss of networks/gateways
- Support multiple types of services
- Accommodate a variety of networks
- Distributed management of resources
- Cost effective
- Low level of effort to add a host
- Provide accounting of resources used

Led to today's challenges in accounting (last goal) and lack of security (non-goal)

What you pay for in life, you get. What you don't pay for, you don't get.

From Car and Driver Magazine:

“Just like the internet in its early days, car networks don't employ very much security” says Brad Hein.



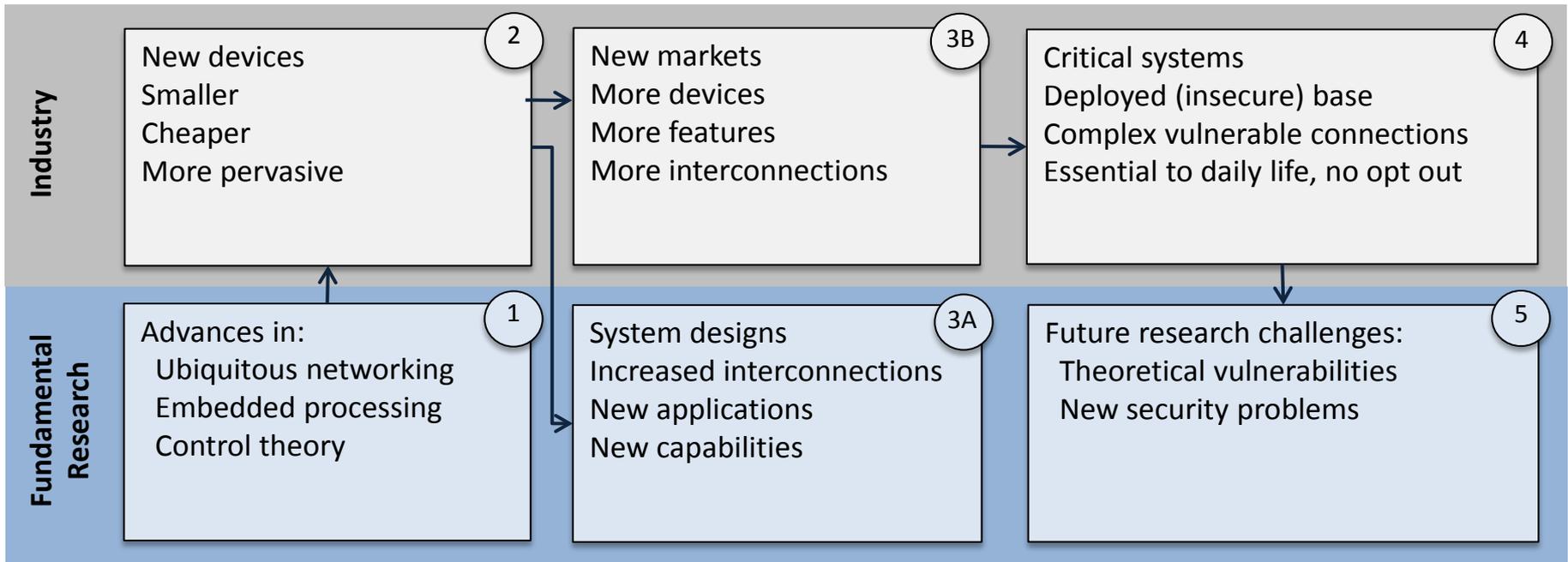
We are setting the CPS design goals now

Security will NOT emerge on its own

Must provide a framework that addresses real threats and real incentives enables collaboration across companies & sectors



Status Quo: CPS Today



1. Rapid advances in theory enable new devices

2. Devices grow smaller, cheaper, more pervasive

3A. Academics envision new system designs

3B. Industry identifies new markets

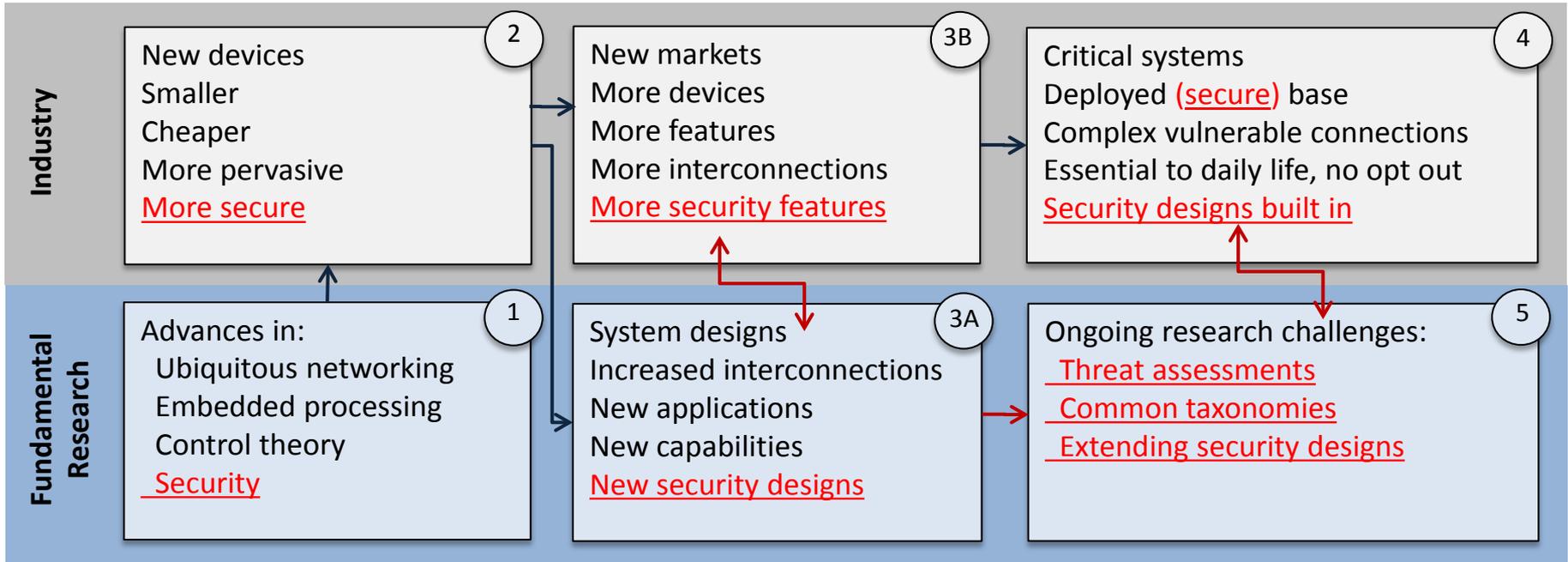
4. Systems become critical to every day life

5. Vulnerable critical systems inspire new security research

Security is not designed in and must be bolted on later – FEMA, CBP, USSS, DOT, NHTSA, and YOU cannot opt out of these systems



Status Quo: With CPSSEC



1. Rapid advances in theory enable new devices

3A. Academics envision new system designs that include security in the design

4. Systems become critical to everyday life

2. Devices grow smaller, cheaper, more pervasive

3B. Industry identifies new markets and also identifies security issues

5. Critical system designs include security and designs evolve to meet threats

Security from early onset Productive research/industry collaboration Security as an integral part of design



Cyber Physical System Security Pyramid

OBJECTIVE

APPROACH

Enable tangible progress through cooperation and market-driven requirements

INDUSTRY CONSORTIUM
Develop sector-specific groups

1.
Industry Specific

Demonstrate real vulnerabilities and economically viable mitigations

APPLIED RESEARCH
CPS TTA with stakeholders

2.
Transportation & Emergency Response, Energy, Healthcare

Leverage cross-cutting aspects across general CPS

JOINT RESEARCH
Foundational research
Inter-Agency
NITRD CPS SSG

3.
Transportation, Emergency Response, Energy Healthcare, Building Controls, Manufacturing & Industry, Agriculture, Defense



CPSSEC Program Key Drivers

- Proposals must identify one (and only one) key driver.
- Selected from the NITRD CPS Strategic Vision Statement
 - Transportation
 - Emergency Response
 - Energy
 - Healthcare
 - Building Controls
 - Manufacturing and Industry
 - Agriculture
 - Defense
- Further specialization within a key driver area is encouraged.
 - Sufficiently narrow resource, economic, and security issues
 - No predefined list of specializations
 - Illustrative example: Transportation : *Vehicles*

CPSSEC Program Topic Areas

- CPSSEC Identifies Three Topic Areas:

(1) Security Models and Interactions

Building security into cyber physical system designs requires an understanding of how cyber and physical system components are expected to interact

(2) Secure System Design and Implementation

Provide existing targets more effective tools and techniques for response and mitigation,

(3) Experiments and Pilots

Anticipate new types of attacks before they occur.

- Proposals must identify one (and only one) topic area.

Topic Area 1: Security Models And Interactions

- Understand how cyber and physical system components are expected to interact.
 - Essential to consider that cyber physical systems integrate both cyber and physical in the system
 - “All three words (cyber, physical, system) count”
- Illustrative Issues for Topic Area 1
 - Security models and taxonomies
 - Combining security with safety
 - Metrics and ratings
 - Building Codes for Cyber Physical Systems
 - Model-based Testing and Validation

Topic Area 2: Secure System Design and Implementation

- Build Security Into Cyber Physical System Design.
 - Again “All three words (cyber, physical, system) count”
 - Expected results to include prototype implementation
- Illustrative Issues for Topic Area 2
 - Authentication and Authorization
 - Monitoring and Logging
 - Intrusion Detection, Mitigation, and Tolerance
 - Secure Updates

Topic Area 3: Experiments and Pilot Projects

- Bridge the gap between advances in fundamental science and the cyber physical systems being deployed today.
- Focus on cyber physical systems in use today
- Experiment and Pilot Project Requirements
 - Clearly identify proposed system technical readiness level
 - Identify safety concerns and appropriate risk mitigations
 - Clearly explain how attacks are introduced and analyzed

Program Impact: CPS Community

PROGRAM COMPONENT

IMPACT

CYBERSECURITY
INDUSTRY
CONSORTIUM

1.
Transportation
Automotive

- Pre-competitive research efforts
 - Priorities connected to market driven challenges

APPLIED
RESEARCH

2.
Transportation &
Emergency Response

- Results from CPSSEC Technical Topic Area efforts

JOINT
RESEARCH

3.
Transportation, Emergency Response
Energy Healthcare

- Priorities connected to academic research community

Program Impact: CPSSEC TTA

- Not Possible to “Opt Out” of CPS, with or without CPSSEC
 - First Responders will rely on these CPS advances
 - Critical infrastructure are being built on CPS designs
 - Must identify requirements and promote desired solutions
 - *Legacy of current designs will guide next several decades*
 - *EO/PPD adds concrete requirements*
- DHS and Federal Government impact
 - Meet EO/PPD objectives for inter-agency coordination on CPS
 - DHS component concerns reflected in industry and research
 - Pilot projects with DHS component agencies

Schedule and Milestones

Year 1

Year 2

Year 3

Year 4

1

TTA #01: Security Models and Interactions

1

TTA #01: Model and Interactions Pilots

KEY

- 6 month project reassessment point
- ◆ Travel (PI/Program Meetings)
- ◆ Evaluation and Transition Plan
- ◆ Demonstration of Capabilities (1 per year)
- ◆ Final Demonstration

2

TTA #02: Secure System Design and Implementation

2

TTA #02: Secure System Design Pilots

3

TTA #03: Experiments and Pilots Projects

References

- 2014 NITRD Cyber Physical Systems Vision Statement;
http://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf
- Executive Order 13636, Improving Critical Infrastructure Cyber Security;
<http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- Presidential Policy Directive 21, Critical Infrastructure Security and Resilience;
<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>
- Carl E. Landwehr, "A building code for building code: putting what we know works to work", Annual Computer Security Applications Conference, ACSAC '13, New Orleans, LA, USA, December 9-13, 2013; <http://dx.doi.org/10.1145/2523649.2530278>
- DHS Cyber Security Division Broad Agency Announcement HSHQDC-14-R-B005;
<https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html>
- DHS Software Assurance Marketplace (SWAMP); <https://www.dhs.gov/csd-swamp>
- DHS Homeland Open Security Technologies (HOST); <https://www.dhs.gov/csd-host>
- DHS Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT);
<https://www.predict.org>



Homeland Security

Science and Technology