Cyber-Physical Meets Cybertrust

Jeannette M. Wing

President's Professor of Computer Science and Department Head
Carnegie Mellon University

International Symposium on Resilient Control Systems
Salt Lake City, Utah
August 15, 2012

Why We Care

Three-Mile Island

Fukushima

Bushehr (Iran)

INVESTIGATIONS

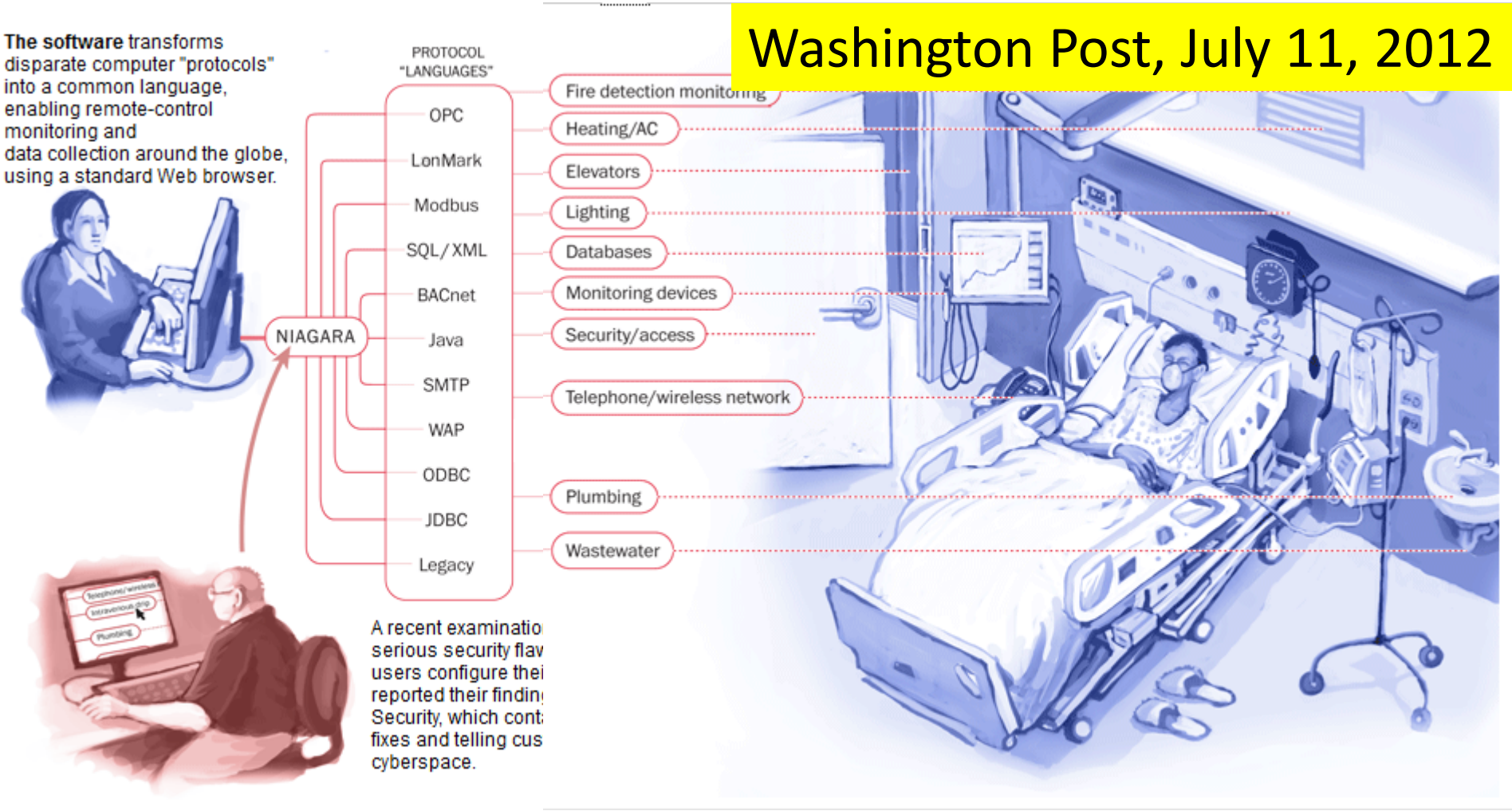
Washington Post, June 3, 2012

Cyber search engine Shodan exposes industrial control systems to new risks

Government and business leaders in the United States and around the world are rushing to build better defenses -- and to prepare for the coming battles in the digital universe. To succeed, they must understand one of the most complex, man-made environments on Earth: cyberspace. (Whitney Shefte, Sohail Al-Jamea and Robert O'Harrow Jr./The Washington Post)

Text Size | Print | E-mail | Reprints

Tridum's Niagara Software Framework



Cyber-Physical Systems

through a CyberTrust lens

Smart Cars

Cars that drive themselves

A BMW is "now actually a network of computers."

[R. Achatz, Seimens, Economist Oct 11, 2007]

Smart parking

Lampson's Grand Challenge:

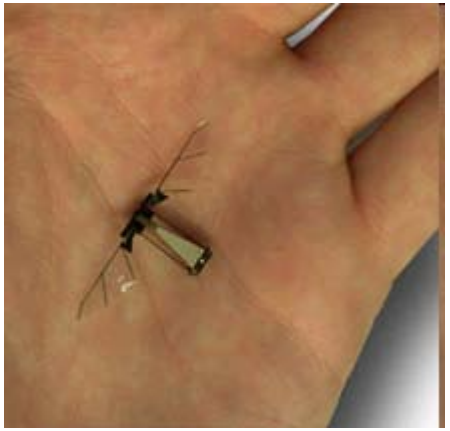
Reduce highway traffic deaths to zero.

[Butler Lampson, Getting Computers to Understand, Microsoft, *J. ACM* 50, 1 (Jan. 2003), pp 70-72.]

Smart Fliers

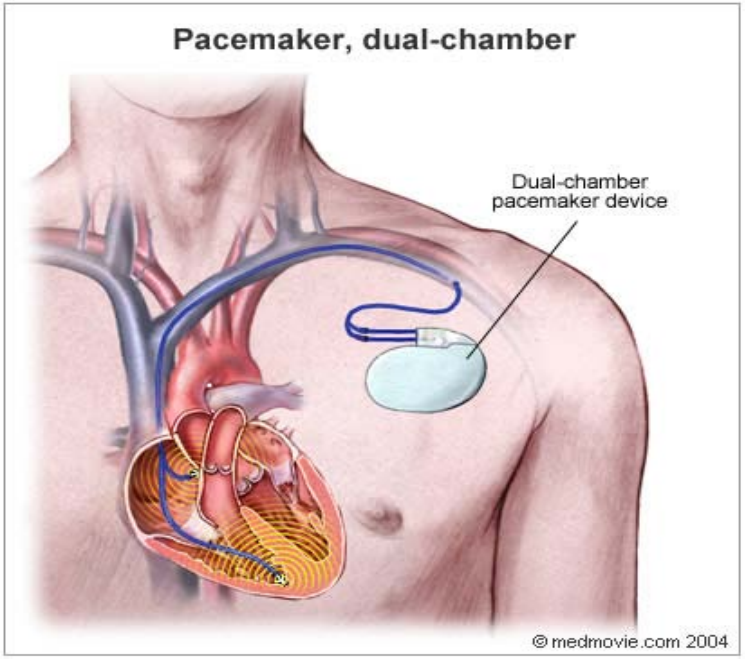
An airplane is a network of computers.

smart helicopters

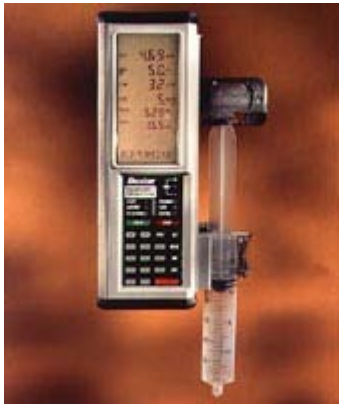


smart insects

Smart Health: Embedded Medical Devices



pacemaker



infusion pump

scanner

Sensors Everywhere

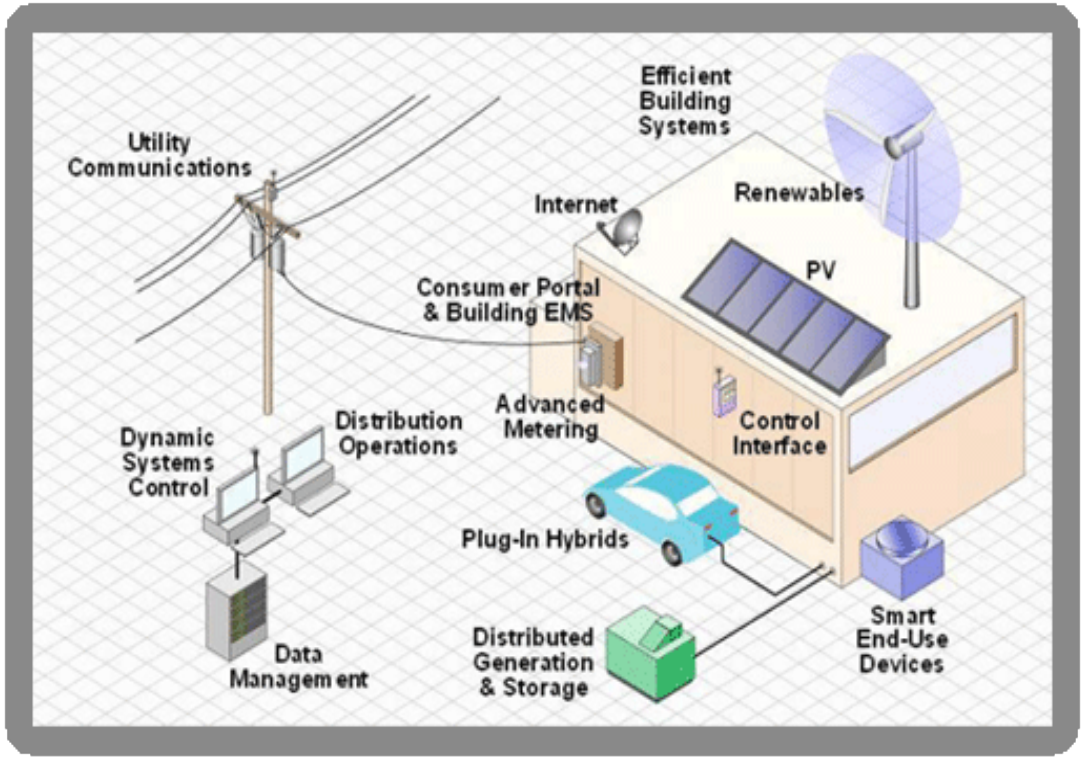
Sonoma Redwood Forest

Hudson River Valley

smart buildings

smart bridges

Smart Energy



smart grid

Robots Everywhere

At work: Two ASIMOs (Japan) working together in coordination to deliver refreshments

At work: Cobot accompanies visitor from meeting to meeting.

At home: iRobot (US) Roomba vacuums your house

At home/clinics: Nursebott provides robotic assistance for the elderly

Assistive Technologies for Everyone

brain-computer interfaces of today

memex of tomorrow

What is Common to These Systems?

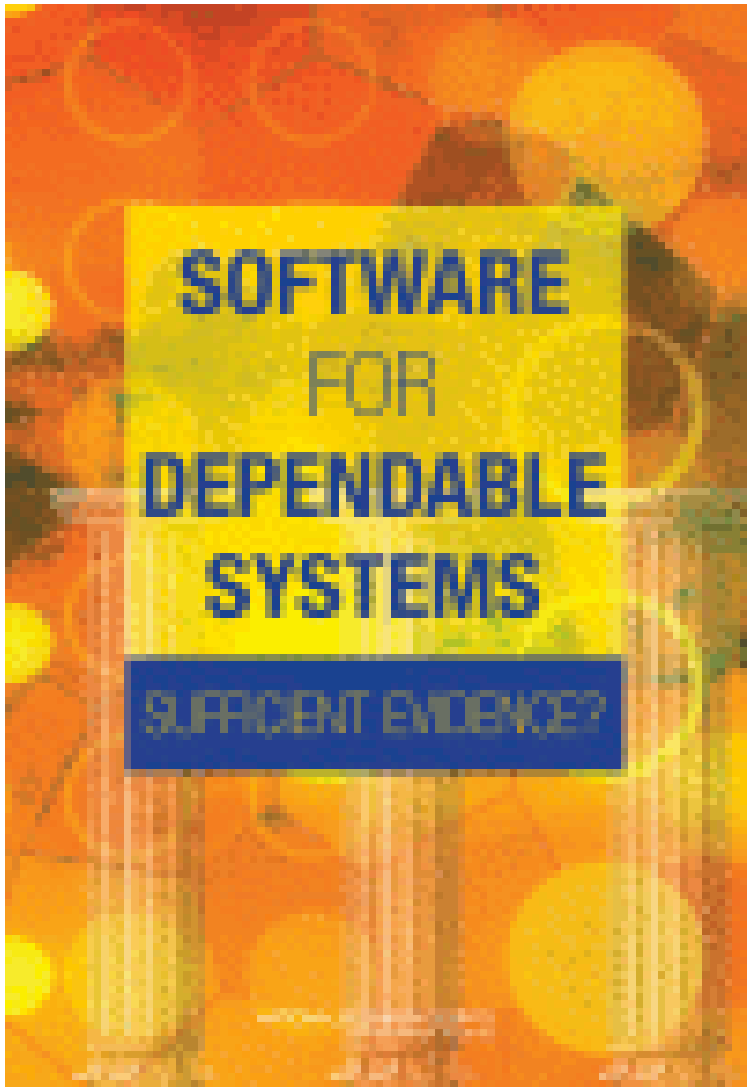
- They have a computational core that interacts with the physical world.

- *Cyber-physical systems are engineered systems that require tight conjoining of and coordination between the computational (discrete) and the physical (continuous).*

- Trends for the future
  - Cyber-physical systems will be smarter and smarter.
  - More and more intelligence will be in software.

CSTB National Academies Study

Software for Dependable Systems: Sufficient Evidence?
Daniel Jackson, Martyn Thomas, and Lynette I. Millett, Editors
May 9, 2007



U.S Broader Research Agenda and Priorities

Dan Reed and George Scalise, editors
August 2007

#1 Priority: Cyber-Physical Systems

Our lives depend on them.

Jeannette M. Wing

Trustworthy Computing

- Trustworthy =
  - + Reliability
    - Does it do the right thing?
  - + Security
    - How vulnerable is it to attack?
  - + Privacy
    - Does it protect a person's identity and data?
  - + Usability
    - Can a human use it easily?

- Computing = hardware + software + people

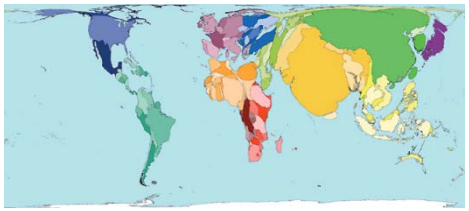
Societal Challenges

- How can we provide people and society with cyber-physical systems they can bet their lives on?

  – Expectations: 24/7 availability, 100% reliability, 100% connectivity, instantaneous response, store anything and everything forever, unintrusive, predictable (or unsurprising), ...

  – Classes: young to old, able and disabled, rich and poor, literate and illiterate, …

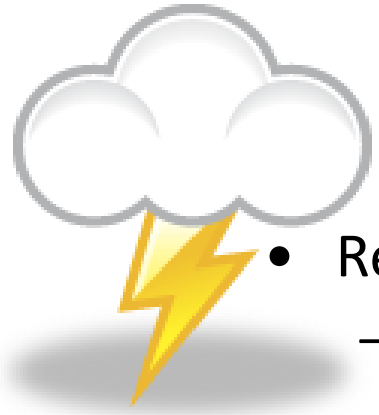
  – Numbers: individual → cliques → acquaintances → social networks → cultures → populations



  – Trustworthiness: reliability, reliability, reliability; privacy, privacy, privacy; usability, usability, usability!

Scientific Challenges

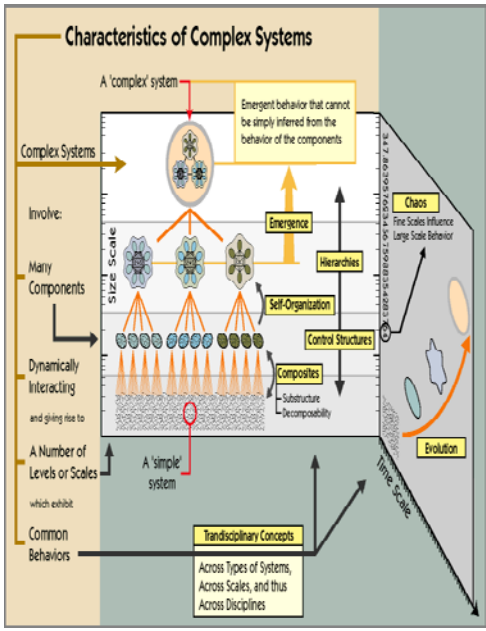
- Co-existence of Booleans and Reals
  - Discrete systems in a continuous world
  - Need for new models (new mathematics?) or extensions of existing continuous and/or hybrid ones



- Reasoning about uncertainty
  - Human, Mother Nature, the Adversary

privacy and usability | reliability | security

- Understanding complex, unpredictable systems
  - Emergent behavior, tipping points, disruptive events…
  - Chaos theory, randomness, …



Technical Challenges

How can we build intelligent and safe digital systems that interact with the physical world?

- Perception, control, and coordination: continuous and ubiquitous
  - Self-monitoring, real-time learning and adapting

We need to bridge two worlds

security and reliability

Computing side: Computing abstractions currently focus primarily on functionality, and secondarily on aspects of the physical world (e.g., time, space, energy, temperature, human behavior)

privacy and usability

Engineering side: Cautiously over-designed systems preclude flexibility offered by computing's power, especially the intelligence embodied in software.

reliability

- Compositional reasoning may be impossible

especially for security (a global property), …

Cybertrust

through a Cyber-Physical Systems lens

The Setting: Then and Now

We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.

1991 *Computers at Risk*, National Academies CSTB Study, p. 7.

8

networked systems

1999 *Trust in Cyberspace*, CSTB Study.

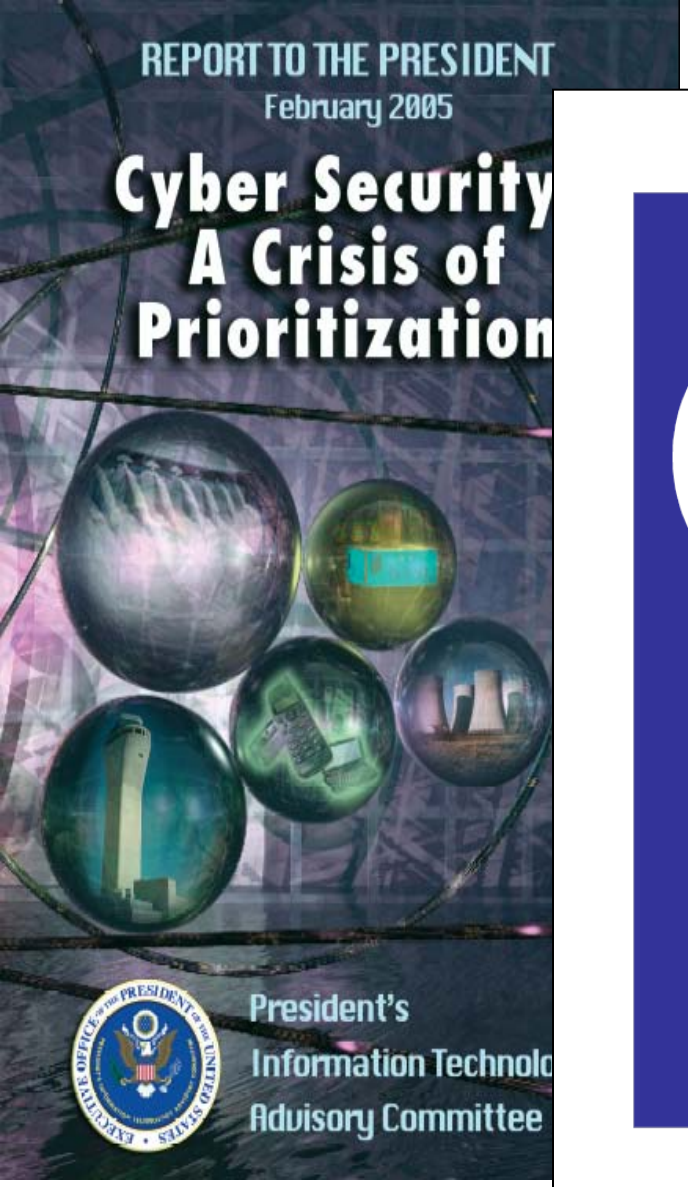
2001 September 11

everywhere, everyone, all the time,
embedded, invisible, visible,
mobile, wearable, handheld, remote,
peta, tera, giga, mini, micro, nano,
good guys, bad guys

8

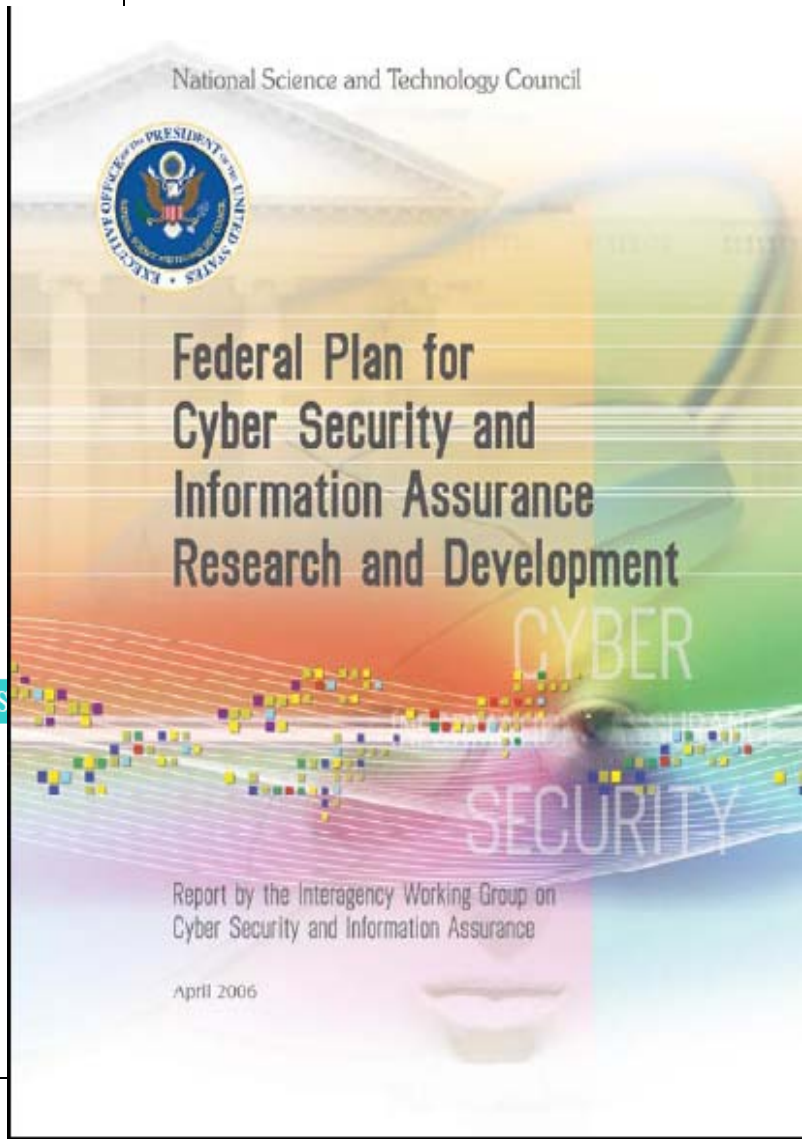
ubiquity

2007 *Improving Cybersecurity for the 21st Century*, CSTB Study.



Credit: NCO/NITRD

Credit: U.S. Department of Homeland Security



Credit: NCO/NITRD

What's Missing in Our Thinking

- Be proactive, not reactive.
  - We are using yesterday's solutions to address today's threats.
  - We should be ready today for tomorrow's threats.
  - We are not.

- Anticipate the future.
  - Long-term outlook
  - Big picture view
  - Foundational research

Long-Term Outlook: Who and Why

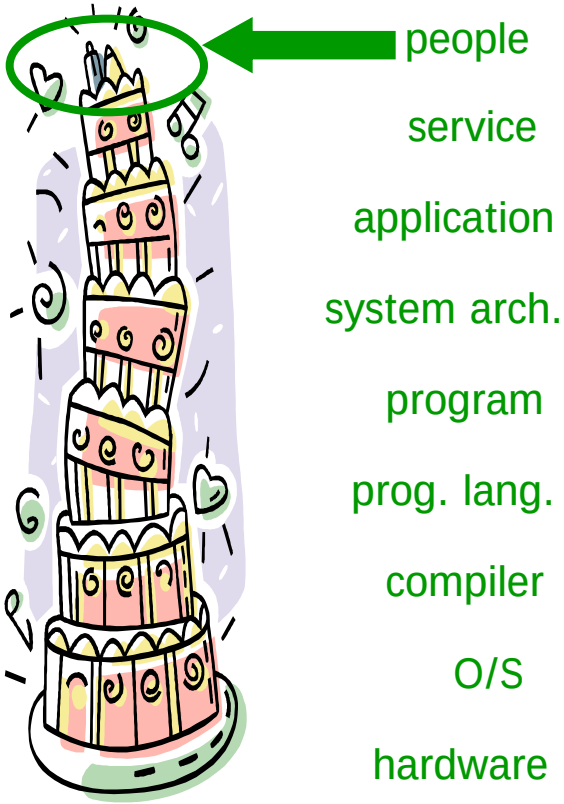
- Threats
  - Yesterday: hackers, criminals
  - ~~Tomorrow~~: organized crime, terrorists, nation-state, enemy state

    Yesterday: 2007 (Estonia), 2010 (Stuxnet)
- Motivation
  - Yesterday: fame, money
  - Tomorrow: power, control

- Attacks
  - Use cyberattack as an amplifier of a physical attack
    - Cyberspace is an enabler
  - Attack the Internet
    - More likely as we put more key functionality on-line
  - Use cyberspace to hide

Big Picture: It's Not Just About Security

- **Trustworthy** systems
  - Reliability
  - Security
  - Privacy
  - Usability



- **Holistic** view
  - Technical: The whole stack
  - Non-Technical

    Psychology and human behavior

    - Usable security - Social engineering attacks - Privacy
    - Insider threat - Attacker's motivation

    Economics, risk management, law, politics

Reliability: Highlights of Progress

70s

Floyd, Dijkstra, Hoare
- program correctness
- program verification
- theorem provers

80s

advanced programming languages
- type checking

database transactions
Byzantine failure model
process algebras
specifications for design
model checking

90s

maturation, scaling, and application of 80s technologies
- hardware verification using model checkers

00s

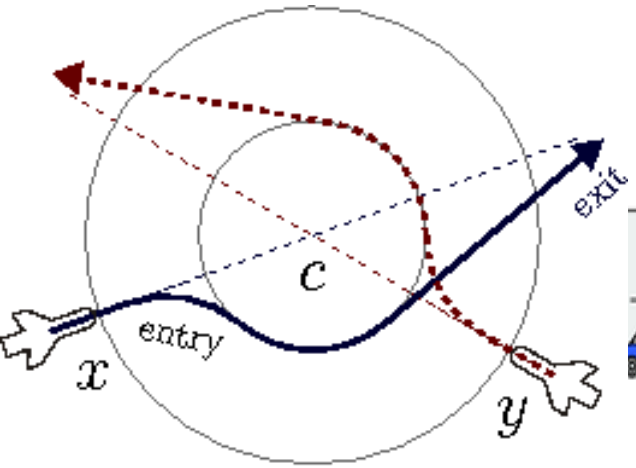
software model checking
sophisticated type systems
static analysis tools for debugging

tomorrow

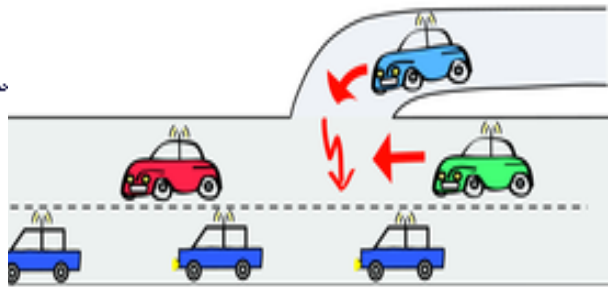
cyber-physical systems verification
component-level reasoning
complexity management
…

Jeannette M. Wing

Research Challenge: Cyber-Physical Systems



$$\frac{\mathrm{d}\varphi_t(x)}{\mathrm{d}t} = f(\varphi_t(x)) \quad (t \in \mathbb{R})$$
$$\varphi_0(x) = x$$



Challenge 1: Reasoning about Reals and Booleans

Challenge 2: Reasoning about Uncertainty in Environment
- stochasticity, non-determinism

Challenge 3: Reasoning about Malicious Adversaries

Computable Reals: A Fundamentally Hard Problem

"A real number is computable if its digit sequence can be produced by some algorithm or Turing machine. The algorithm takes an integer $n \geq 1$ as input and produces the n-th digit of the real number's decimal expansion as output. " [Turing 1936]

Fact: While the set of real numbers is uncountable, the set of computable numbers is only countable and thus almost all real numbers are not computable.

Computable Reals: Verification Challenge

On the one hand:

- A real number *a* is said to be **computable** if it can be approximated by some computable function in the following manner: given any integer $n \geq 1$, the function produces an integer *k* such that:

$$\frac{k-1}{n} \leq a \leq \frac{k+1}{n}$$

On the other:

- The computable numbers include many of the specific real numbers which appear in practice, including all real algebraic numbers, as well as *e*, π, and many other transcendental numbers.

Security: Highlights of Progress

70s

Computer security
- Protect the Box

O/S: kernel vs. user, virtual machines
files: access control
Orange Book (theorem provers again)

80s

Morris worm (anti-progress)
Crypto
- Needham-Schroeder, Diffie-Hellman, RSA
- zero-knowledge proof ('89)

90s

Network security
- firewalls, packet filters, intrusion detection
- standards, e.g., IPSEC, SSL, IPv6

Foundations, e.g., "provable security", authentication logics

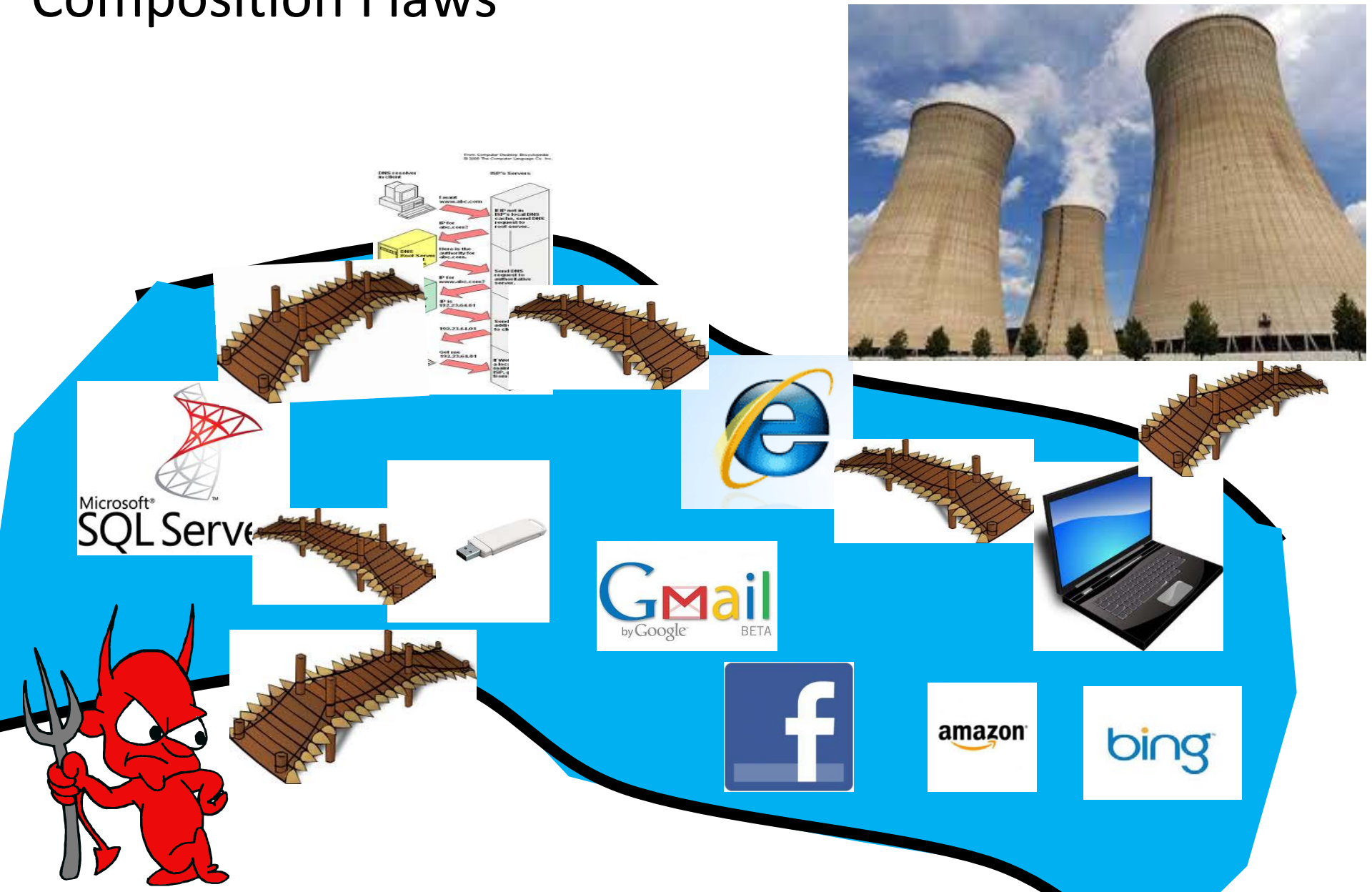
00s

Security w/o perimeters
- remote code, worms, viruses (CRA Grand Challenge #1)
- code-level security: buffer overruns, format string vuln's

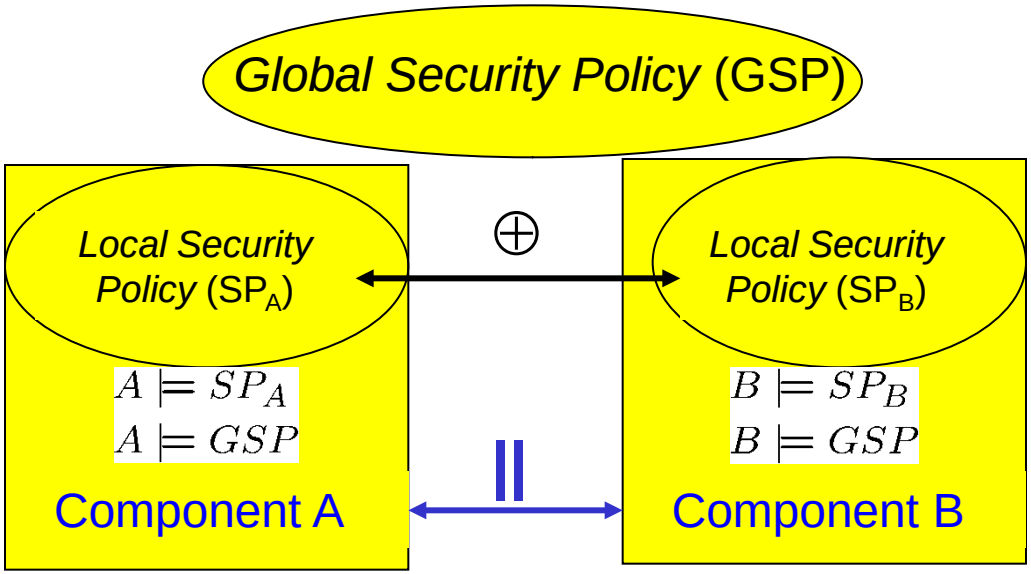
tomorrow

security composition
security metrics (CRA Grand Challenge #3)
security tradeoffs with R, P, and U
…

Composition Flaws



Composition of Components and of Security Policies



Consider the composition **A || B**:

$$\mathbf{A \,||\, B} \overset{?}{\models} \mathbf{GSP}$$

$$\mathbf{A \,||\, B} \overset{?}{\models} \mathbf{SP_A} \text{ and } \mathbf{A \,||\, B} \overset{?}{\models} \mathbf{SP_B}$$

Consider more simply, $SP_A \oplus SP_B$:

$$\mathbf{SP_A} \oplus \mathbf{SP_B} \overset{?}{\Rightarrow} \mathbf{GSP}$$

$$\mathbf{SP_A} \oplus \mathbf{SP_B} \overset{?}{\Rightarrow} \mathbf{SP_A} \text{ and } \mathbf{SP_A} \oplus \mathbf{SP_B} \overset{?}{\Rightarrow} \mathbf{SP_B}$$

Netscape and Domain Name Server

Names to IP addresses mapping

```
user.foo.com [1.2.3.4,
              1.2.3.5,
              1.2.3.6]
user.bar.com [1.2.3.5,
              1.2.3.7]
```

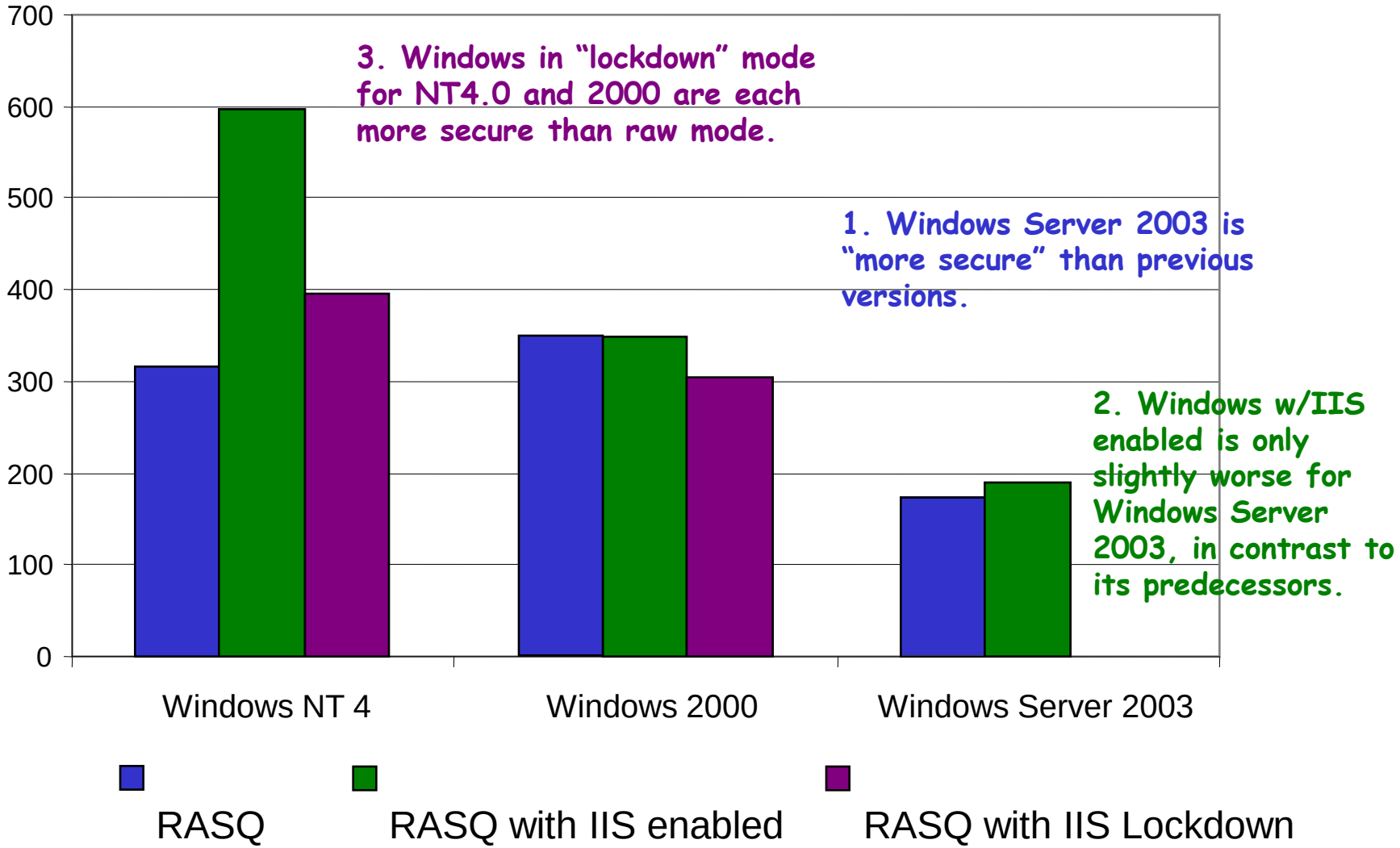
Security Metrics

Computing Research Associates Grand Challenges on Trustworthy Computing, November 16-18, 2003
http://www.cra.org/grand.challenges

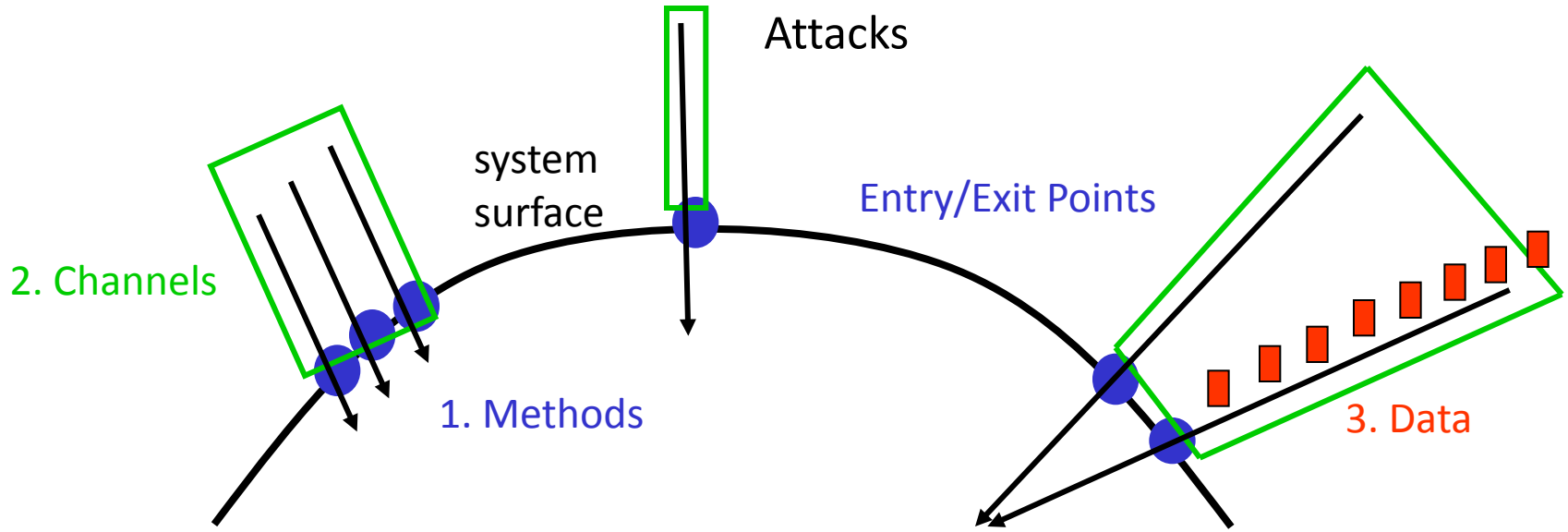
Challenge #3:

Within 10 years, develop quantitative information-systems risk management that is at least as good as quantitative financial risk management.

Measuring the Relative Attack Surface



Attack Surface



The *attack surface* of a system is the ways in which an adversary can enter the system and potentially cause damage.

Reduce the attack surface $\Longrightarrow$ Increase system's security

Privacy: Do You Read These? What Are They Saying?

Each privacy statement goes on for tens of screenfuls!

Windows

Sign In | United States | All Microsoft Sites

Search this website

Home | Explore Windows | Products | Shop | Downloads | Help & How-to

Windows 7 Help home | Getting started | Top solutions | How-to videos

Microsoft Windows Media Player 12 privacy statement

Applies to these editio

Last updated: July

Microsoft is comm
you the performar
This privacy staten
Windows Media P
that communicate
sites, products, or

Windows Media P
Internet, both on y
players. Windows
Internet-based onl
companies. This p
these online store

Collection ar

Google | Policies & Principles

Overview | Privacy | Terms of Service

Privacy Policy | Advertising | Principles

Current version

Past versions

Self Regulatory Frameworks

Key terms

Privacy Policy

Last modified: March 1, 20

There are many different wa
new content. When you sh
show you more relevant sea
use our services, we want y

Our Privacy Policy explains

- What information we c
- How we use that infor
- The choices we offer, i

We've tried to keep it as si
read about these key terms
time to get to know our pra

Information we collect

We collect information to p

facebook

Sign Up

Facebook helps you connect and share with the people in your life.

Data Use Policy

Date of Last Revision: June 8,

Information we receive and h
- Information we receive abo
- Public information
- Usernames and User IDs
- How we use the informatior
- Deleting and deactivating y

Sharing and finding you on Fa
- Control each time you post
- Control over your timeline
- Finding you on Facebook
- Access on phones and othe
- Activity log
- What your friends share ab
- About Pages

amazon

Jeannette's Amazon.com | Today's Deals | Gift Cards

Shop by Department

Search All

Help > Privacy, Security & Accessibility > Privacy Notice

Topics

Privacy, Security & Accessibility

Privacy Notice

Amazon Accessibility Resources

Safety and Security Tips

Our Efforts to Stop Spoofing

Is This E-mail from Amazon?

E-mail Account Verification

Security Researchers and Professionals

Amazon Consumer Survey E-mails

Search Help:

Amazon.com Privacy Notice

Last updated: April 6, 2012. To se

Amazon.com knows that you care ho
that we will do so carefully and sens
you are accepting the practices d

- What Personal Information Abo
- What About Cookies?
- Does Amazon.com Share the In
- How Secure Is Information Abo

Privacy: Questions to Ponder

1. What does privacy mean?

2. How do you state a privacy policy? How can you prove your software satisfies it? How can you determine whether an organization complies with it?

3. How do you reason about privacy? How do you resolve conflicts among different privacy policies?

4. Are there things that are impossible to achieve wrt some definition of privacy? What is possible, even without giving up security?

5. How do you implement practical mechanisms to enforce different privacy policies? As they change over time?

6. How do you measure privacy? What are the tradeoffs between privacy and utility?

New Challenges

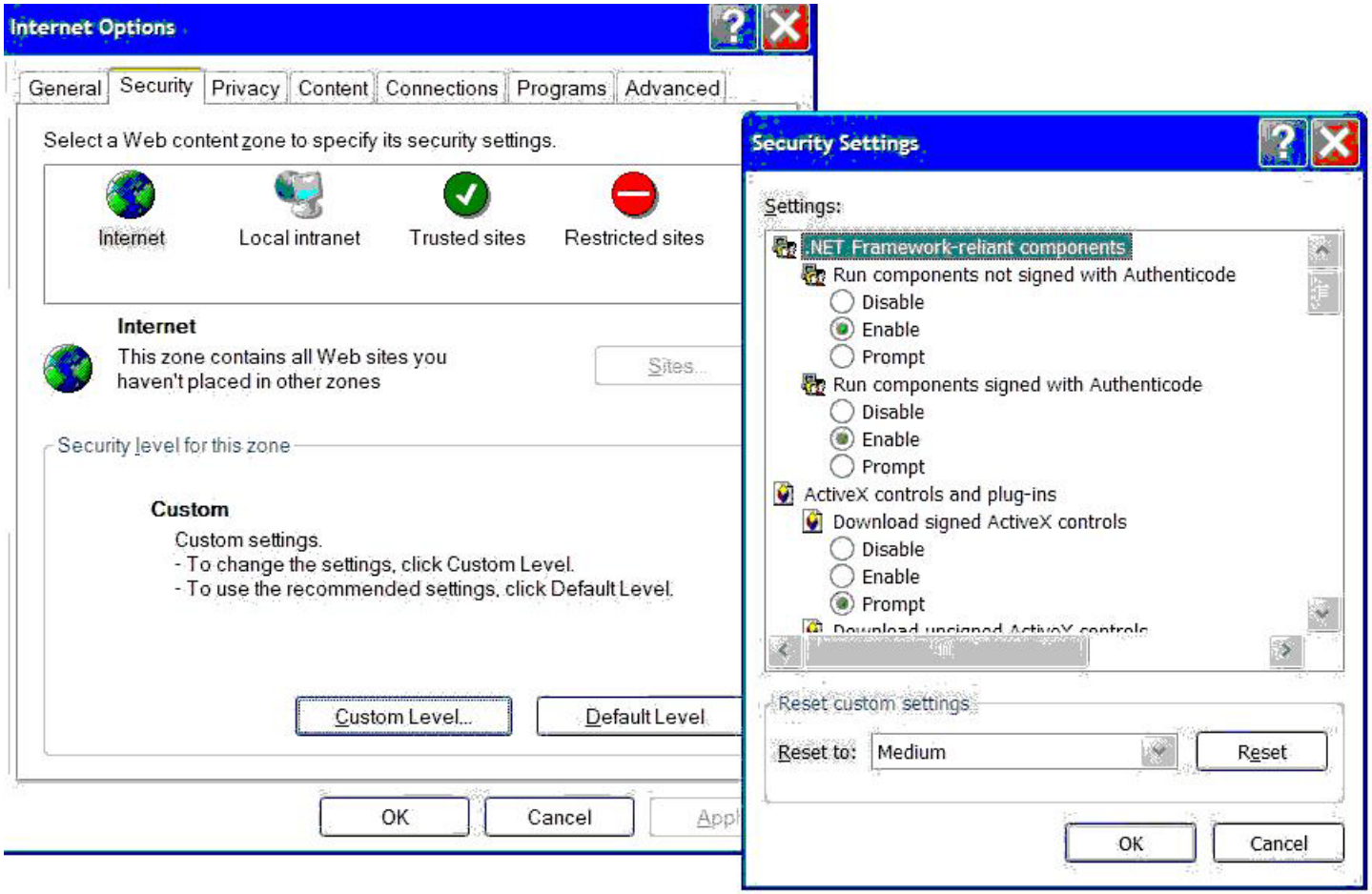
- New technologies
  - Social media and web services
  - Data analytics, cloud computing
  - Mobile phones

- New privacy concerns (not just identity and data)
  - Location privacy
  - Behavioral tracking

- Information Integration

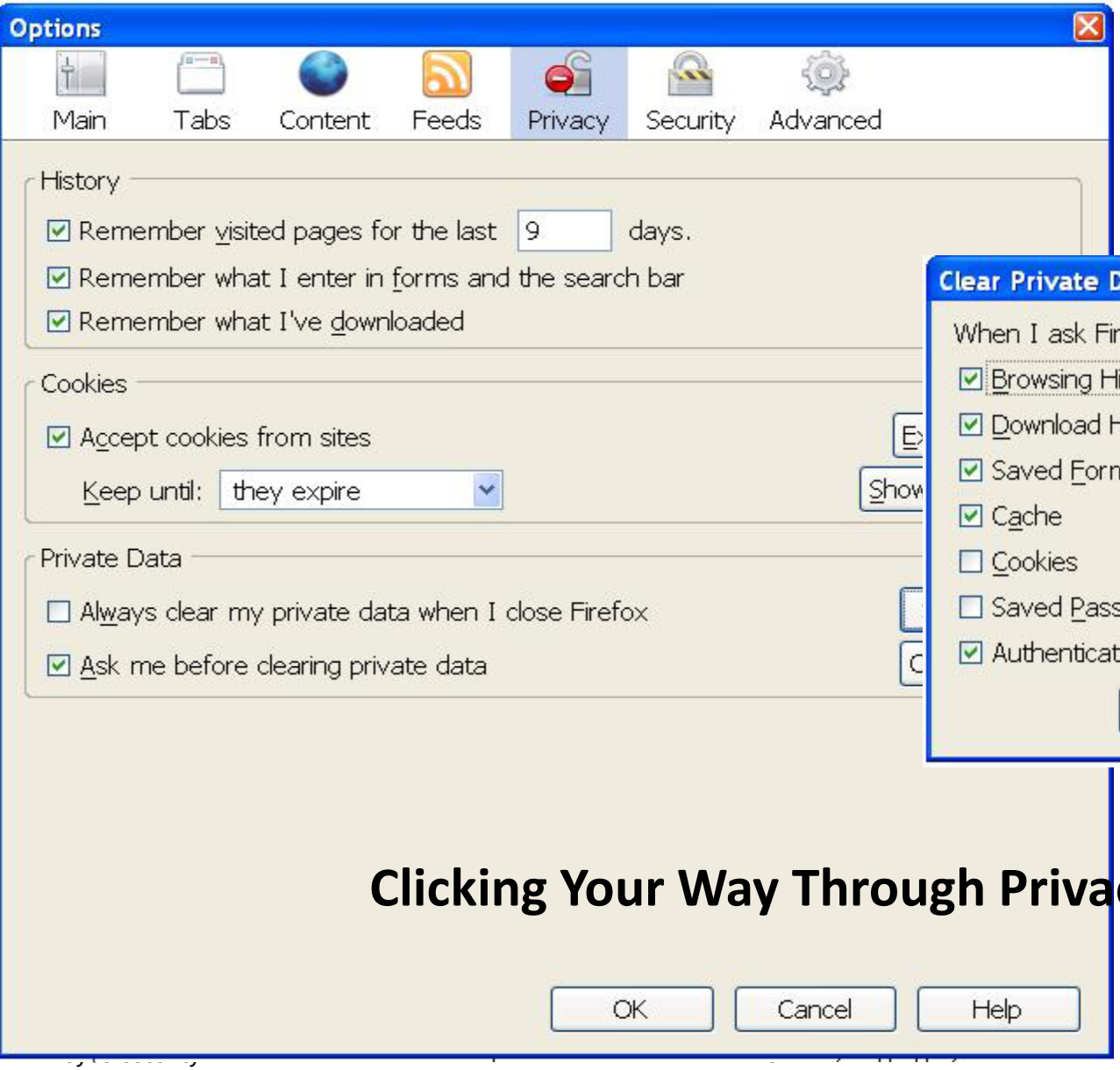
- Auditing, accountability, compliance

Usable Security (IE)



Clicking Your Way Through Security

Usable Privacy (Firefox)



Clicking Your Way Through Privacy

Research Challenges in Usability

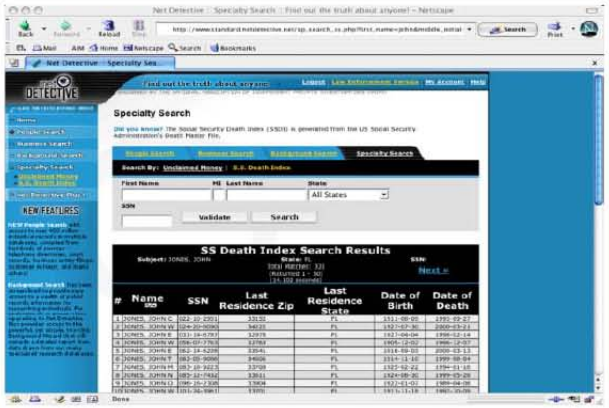
- Balance between usability and security, privacy, and reliability
  - E.g., statistical model of privacy allows a tradeoff between utility and privacy
  - E.g., economic models capture cost/risk-benefit tradeoffs

- How much does the user need to know? How much control should the user have? Control vs. convenience.

- Is the "notice and consent" model outdated? Is a "nudge" model better?

Sampling of Results from Experimental Studies on Behavioral Economics of Privacy (Alessandro Acquisti)

+



= SSN

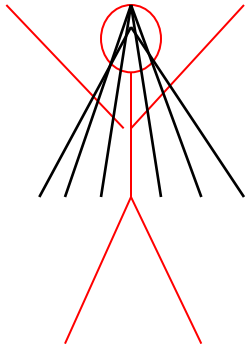
Easy to predict social security numbers from public data (e.g., date and state of birth from Facebook page, plus non-random issuance of SSNs) *[PNAS 2009]*

- Individuals more likely to disclose sensitive information to unprofessional sites than professional sites.
- People assign different values to their personal information depending on whether they are focusing on **protecting it** or **revealing it**
- People may make disclosure decisions that they stand to later regret.
- Risks greatly magnified in online information revelation

Trust in Cyberspace

Trust in Networks of Humans and Computers
(Gligor and Wing)

How can I (a human) trust the information I read over the Internet?



receiver

sender

Networks of Humans and Computers

Insight

- Computational trust defines trust relations among devices, computers, and networks

- Behavioral trust defines trust relations among people and organizations

  - Beliefs
  - Preferences
    - Risk Aversion
    - Betrayal Aversion

- A theory of trust for networks of humans and computers needs to include elements of both.

New Research Directions: A General Theory of Trust (for Networks of Humans and Computers)

- Needs to build on elements of computational trust and behavioral trust
  - Research (foundational): What are those elements? How do they reinforce or complement each other? How do they compose?
- Should elucidate new trust relations and show how they provide new economic value
  - Research (security economics): What are those new relations and how does one monetize them?
- Should thus suggest new computational infrastructure to support behavioral trust in a computational setting
  - Research (systems): What new computational mechanisms and systems/network architectures and protocols could support betrayal aversion?

Summary: CPS Meets CyberTrust

Trustworthy Computing: It's not just cybersecurity
Reliability + Security + Privacy + Usability

- *Reliability*: Cyber-Physical Systems poses fundamentally new and hard research problems in formal models, logics, and verification.
- *Security*: Cyber-Physical Systems are new targets of attack and provide new attack vectors.
- *Privacy*: Cyber-Physical Systems, e.g., smart grid, sensors, collect data about individuals.
- *Usability*: Cyber-Physical Systems, e.g., cars, robots, interface with people. CPS are no longer embedded and hidden.

Thank you!

Credits

- Copyrighted material used under Fair Use. If you are the copyright holder and believe your material has been used unfairly, or if you have any suggestions, feedback, or support, please contact: jsoleil@nsf.gov

- Except where otherwise indicated, permission is granted to copy, distribute, and/or modify all images in this document under the terms of the GNU Free Documentation license, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation license" (http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License)