WHAT HAPPENS WHEN EVERYDAY OBJECTS BECOME INTERNET DEVICES: A SCIENCE POLICY AGENDA

AAAS 2017: Serving Society through Science Policy

February 17, 2017

CCC

Computing Community Consortium

Catalyst

COMPUTING COMMUNITY CONSORTIUM

The **mission** of Computing Research Association's Computing Community Consortium (CCC) is to:

catalyze the computing research community and
enable the pursuit of innovative, high-impact research.

CCC conducts activities that
strengthen the research community,
articulate compelling **research visions**, and
align those visions with pressing **national and global challenges**.

CCC **communicates** the importance of those visions to **policymakers**, **government** and **industry stakeholders**, the **public**, and the **research community** itself.

- Established in 2006 as a standing committee of the Computing Research Association
- Funded by NSF through a Cooperative Agreement

CCC
Computing Community Consortium
Catalyst

CATALYZING: VISIONING ACTIVITIES

- Over 35 Workshops to date
- More than 2,750 participants

Inclusive Access

BRAIN

Personalized Education

Sustainability & IT

Financial Cyberinfrastructure

Extreme Scale Design Automation

Online Education

Cyber Security for Manufacturers

Uncertainty

Privacy by Design

Computing and Healthcare

Cyber-physical systems

Spatial Computing

ROBOTICS

Aging in Place

Big Data Computing

Human Computation

Disaster Management

Sociotechnical Cybersecurity

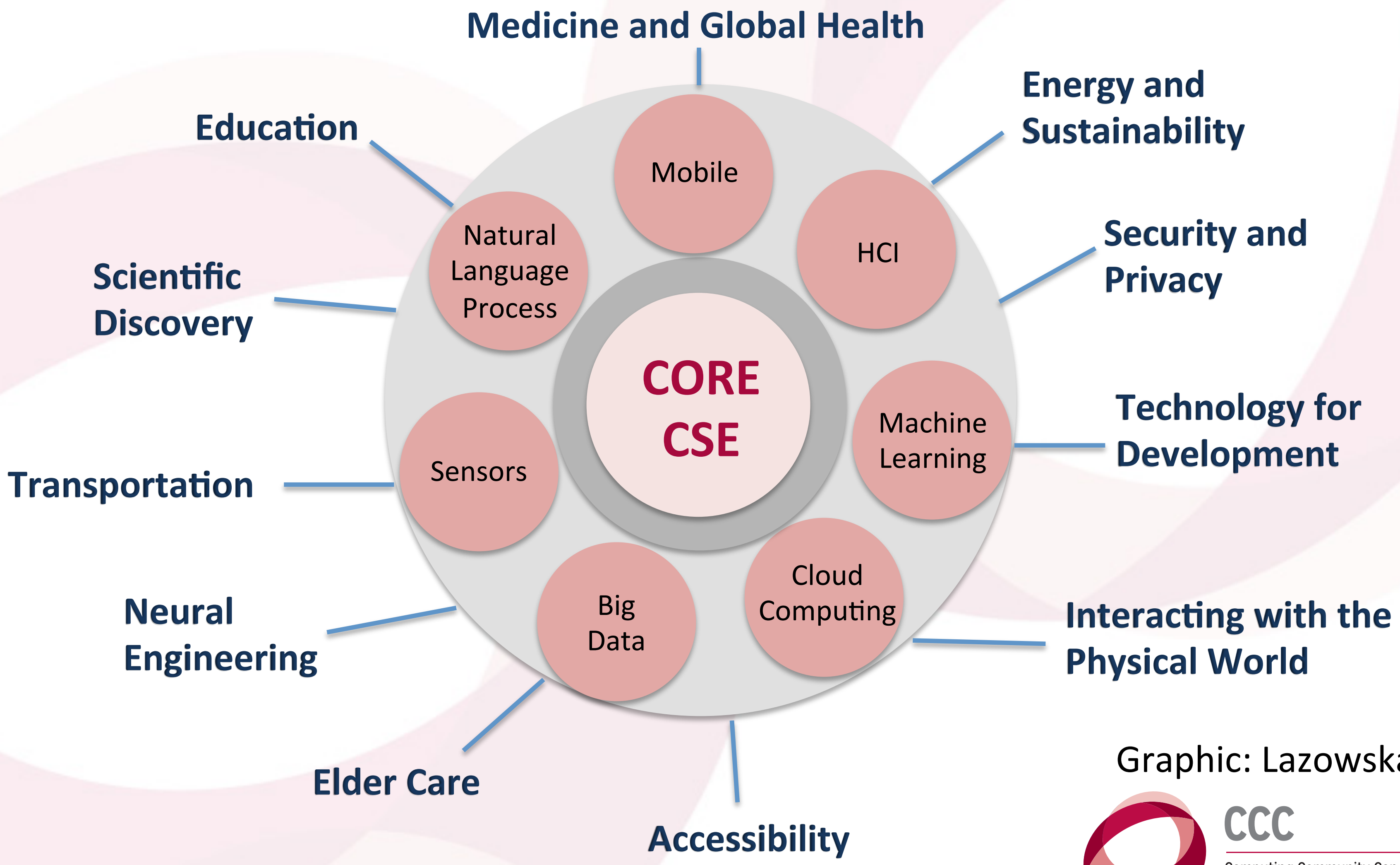
Theoretical Foundations for Social Computing

Learning Technologies

Cyber Social Learning Systems

Global Development

THE RAPIDLY EXPANDING WORLD OF COMPUTING



CORE CSE

Mobile

HCI

Machine Learning

Cloud Computing

Big Data

Sensors

Natural Language Process

Medicine and Global Health

Energy and Sustainability

Security and Privacy

Technology for Development

Interacting with the Physical World

Accessibility

Elder Care

Neural Engineering

Transportation

Scientific Discovery

Education

Graphic: Lazowska

CCC
Computing Community Consortium
Catalyst

OVERVIEW

- How People Think and Reason About An Internet of Things
  - Elizabeth Mynatt, Georgia Tech
- Programming a Secure, Robust and Sustainable Internet of Things
  - Ben Zorn, Microsoft Research
- The Future of Smart Environments and the Internet of Things
  - Shwetak Patel, University of Washington

INSTITUTE for PEOPLE and TECHNOLOGY

How People Think and Reason About an Internet of Things

Elizabeth Mynatt

mynatt@gatech.edu #mynatt

When Everyday Objects Become Internet Devices

Tesla Model S

Amazon Echo

Smart Meter

Yes, this is a computer too

Ring.com

Nest

My Background

Ubiquitous Computing
Xerox PARC

“Everyday Computing”
Georgia Tech

Aware Home

Pervasive Health

Weiser. 1999. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.* 3, 3 (July 1999), 3-11.

Want, Weiser and Mynatt. 1998. Activating Everyday Objects

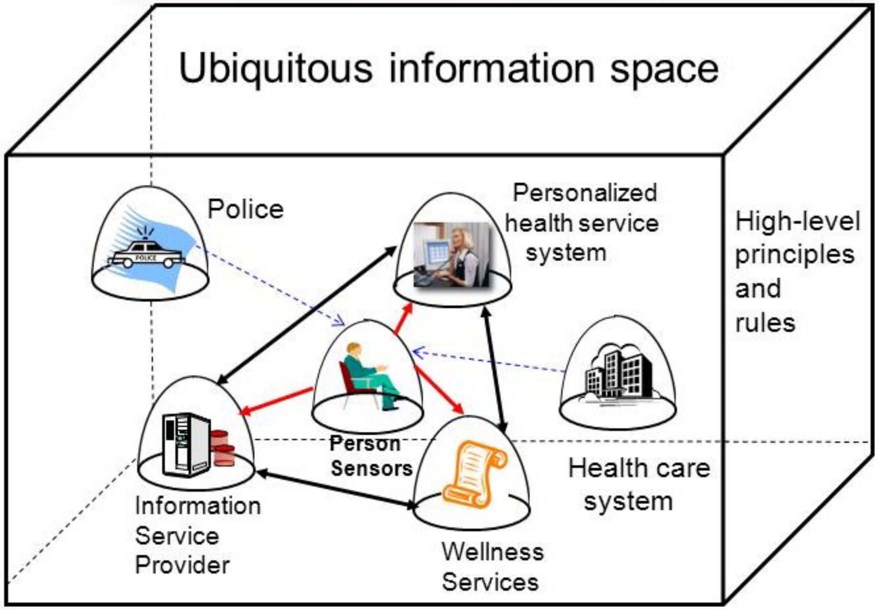
My Background

Ubiquitous Computing
Xerox PARC

"Everyday Computing"
Georgia Tech

Aware Home

Pervasive Health


Ubiquitous information space
Police
Personalized health service system
High-level principles and rules
Person Sensors
Information Service Provider
Health care system
Wellness Services

Ruotsalainen PS, Blobel BG, Seppälä AV, Sorvari HO,Nykänen PA. A Conceptual Framework and Principles for Trusted Pervasive Health J Med Internet Res 2012;14(2):e52

Main Points

People interpret their interactions with objects based on knowledge of people and spaces aka *places.*

Usability

Trust

Privacy

Main Points

People interpret their interactions with objects based on knowledge of people and spaces aka *places.*

Usability

Trust

Privacy

At Home with Ubiquitous Computing: Seven Challenges

(Edwards and Grinter (2001)

Challenge One: The "Accidentally" Smart *Place*

Challenge Two: Impromptu Interoperability

Challenge Three: No Systems Administrator

Challenge Four: Designing for Domenstic Use

Challenge Five: Social Implications of *Smart* Technologies

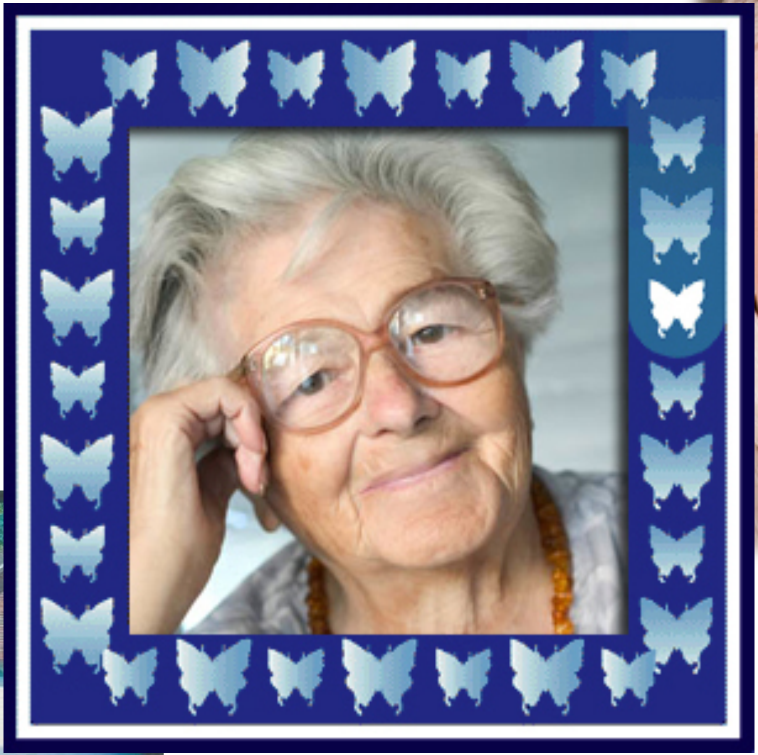
Challenge Six: Reliability

Challenge Seven: Inference in the Presence of Ambiguity

"Peace of Mind" Awareness

Adult children concerned about a parent living alone

Compromise on information sharing



Mynatt, E. D., Rowan, J., Craighill, S., and Jacobs, A. (2001). Digital family portraits: supporting peace of mind for extended family members. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '01). Seattle, WA. ACM, New York, NY, 333-340.

"Peace of Mind" Awareness

Did my mom have a "normal" day?

Situated in family relationships

RANCH HOME
2130 SqFt 3 Bed 2 Bath
58' X 64'
64
LIVING 20 X 18
MASTER SUITE 15 X 16
GREAT ROOM 18 X 18
BED 2 12 X 15
BATH
DINING 13 X 14
BED 3 12 X 12
PORCH 10 X 5
GARAGE 23 X 24
58
PLAN # 151034ULT33

Rowan, Jim, and Elizabeth D. Mynatt. "Digital family portrait field trial: Support for aging in place." *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2005.

Making Sense of Sensing Systems: Five Questions for Designers and Researchers

Bellotti, Back, Edwards, Grinter, Henderson, Lopes (2002)

Address: How do I address one (or more) of many possible devices?

Attention: How do I know the system is ready and attending to my actions?

Action: How do I effect a meaningful action, control its extent and possibly specify a target or targets for my action?

Alignment: How do I know the system is doing (has done) the right thing?

Accident: How do I avoid (or correct) mistakes?

Main Points

People interpret their interactions with objects based on knowledge of people and spaces aka *places.*

Usability

Trust

Privacy

Tesla accident

Tesla - Performance Improvement

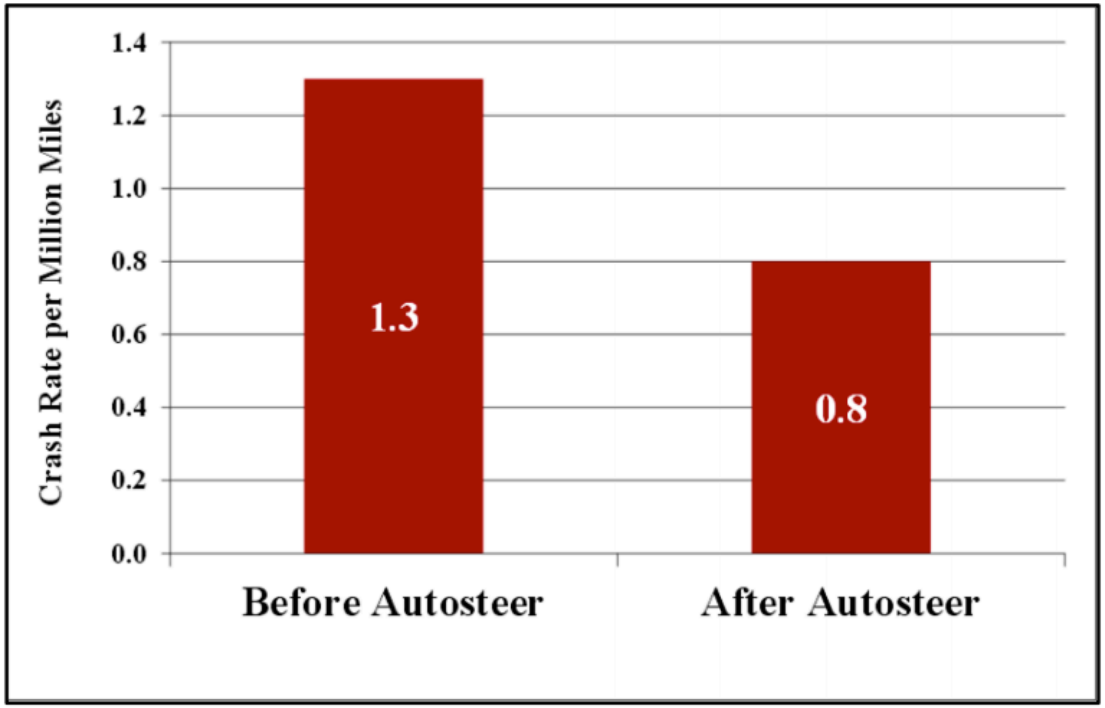
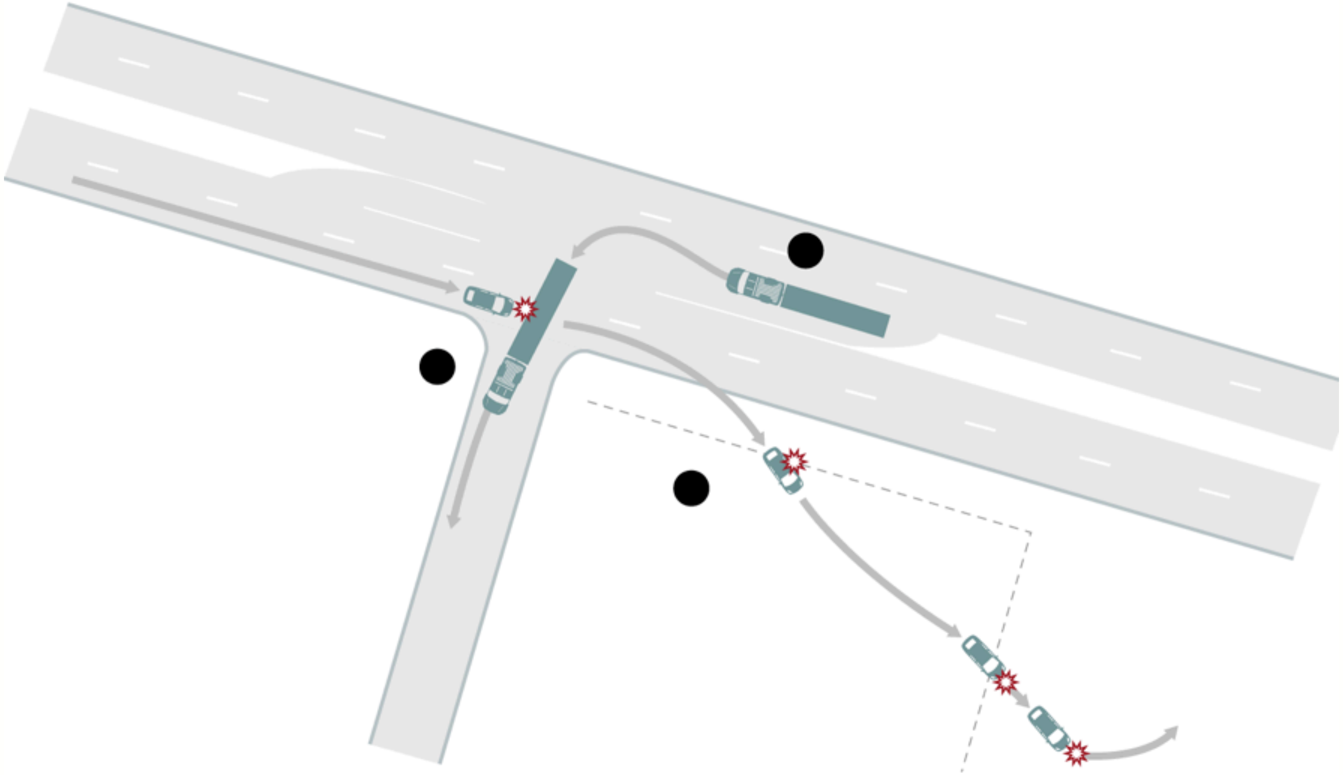


Figure 11. Crash Rates in MY 2014-16 Tesla Model S and 2016 Model X vehicles Before and After Autosteer Installation.

https://electrek.co/2017/01/19/tesla-crash-rate-autopilot-nhtsa/

What happened?



Trust and Reliance are Human Issues

Issues of trust in, trustworthiness of, and reliance on AI/ autonomy

Mr. Brown over-trusted the technology relative to its actual capabilities

A second, less widely recognized failure mode in this case

- □ Car continued autonomous driving after its “shearing” until it hit telephone pole

Under-trust can be just as harmful;
correct calibration of trust is required

Main Points

People interpret their interactions with objects based on knowledge of people and spaces aka *places.*

Usability

Trust

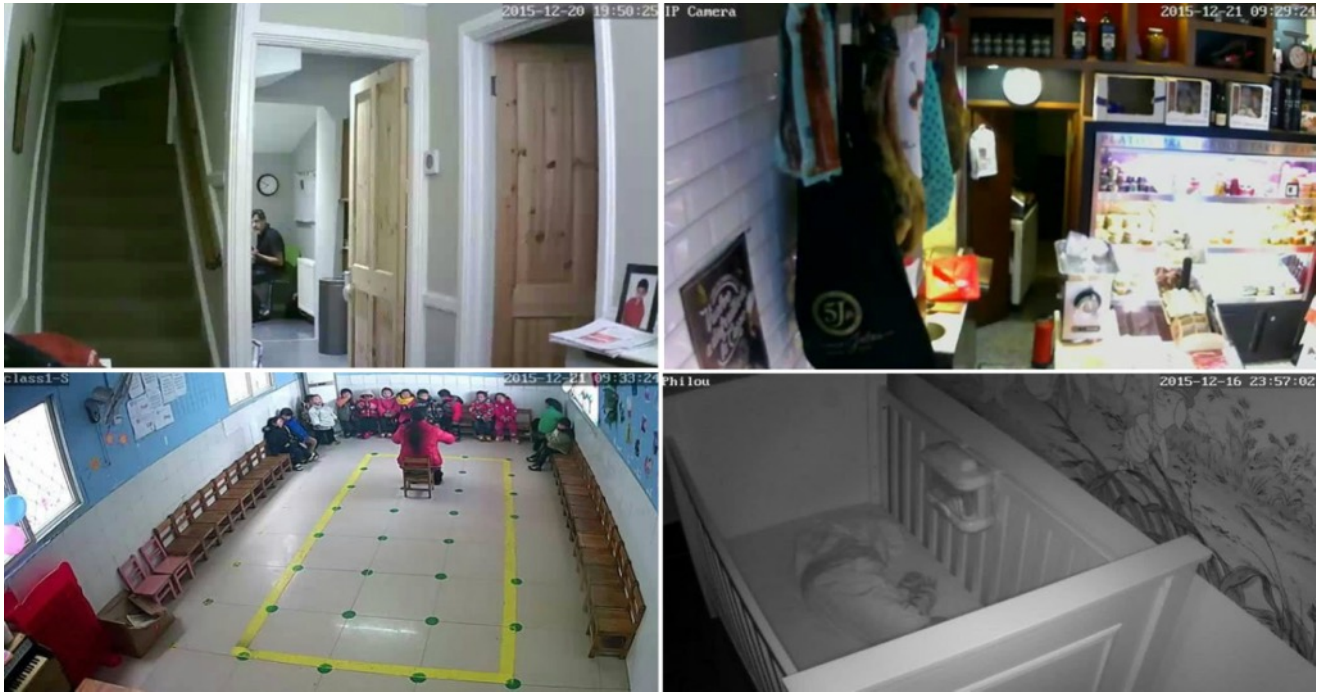
Privacy

The Internet of Insecure Web Cams

Cheap web cameras with default passwords.

Internet search engines to detect open RTSP feeds.

Millions of these cameras online.



The Internet is Always Listening and Observing

Internet appliances

Smart thermostats

Smart TVs

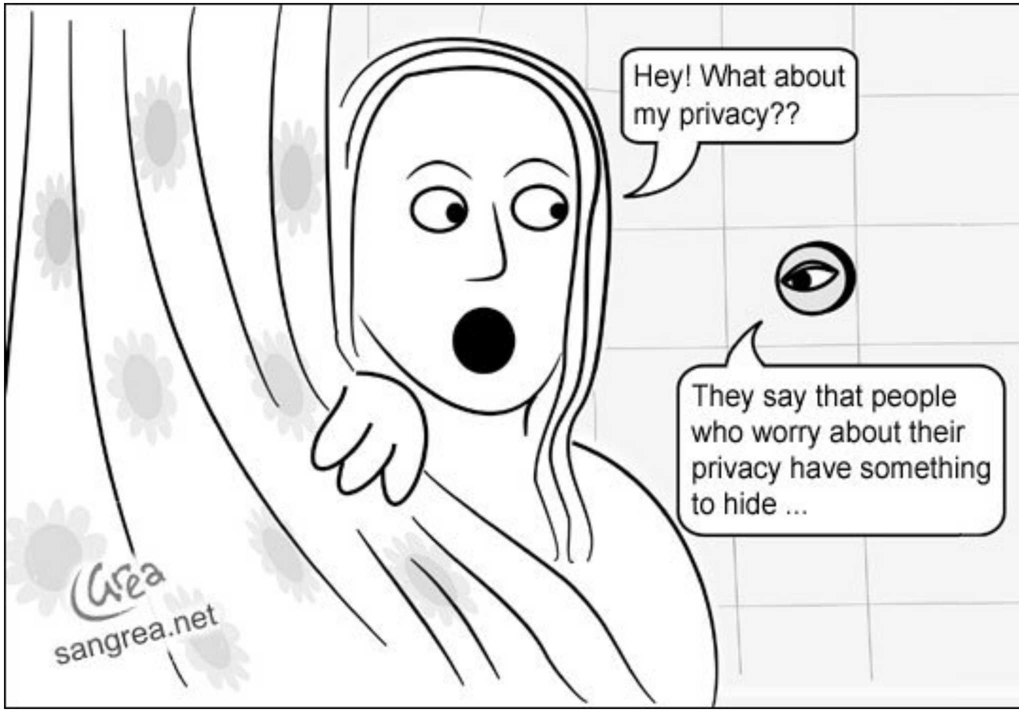
Privacy Mirrors

Why is it so difficult to see what others can see about ourselves?

Making ubiquitous computing visible
E Mynatt, D Nguyen - Proceedings of the 2001 CHI Conference on Human Factors in Computing Systems

Human Centered Privacy

- People (can) provide many traces of daily life.
- People interpret information exchange in terms of relationships.
- People may not understand the value of their data.
- People respond to the value of human-to-human connection.


Hey! What about my privacy??
They say that people who worry about their privacy have something to hide ...
Grea
sangrea.net

Main Points

People interpret their interactions with objects based on knowledge of people and spaces aka *places.*

Utility
Trust
Privacy

Georgia Tech

INSTITUTE for

PEOPLE and TECHNOLOGY

How People Think and Reason About an Internet of Things

Elizabeth Mynatt

mynatt@gatech.edu #mynatt

Programming a Secure, Robust, and Sustainable Internet of Things

Ben Zorn

Principal Researcher and Research Manager

Research in Software Engineering (RiSE) Group

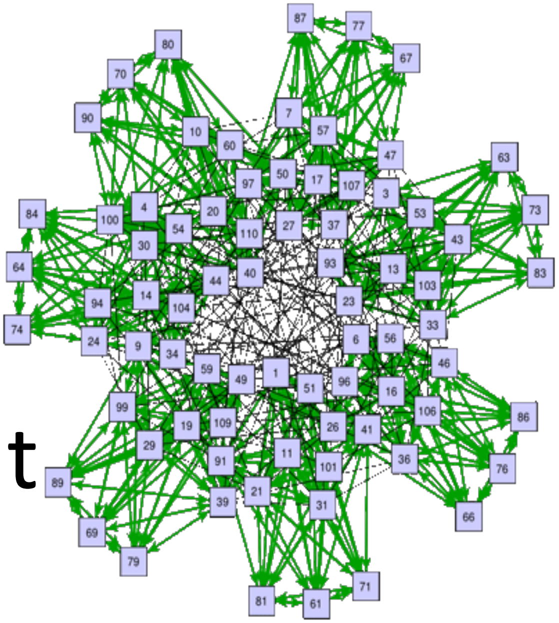
Microsoft Research, Redmond

Technology Disrupts Society (and Science)

AI

Machine Learning

Constraint Solvers



IoT

Drones

Smart Forks

Microsoft

Zorn, AAAS 2017

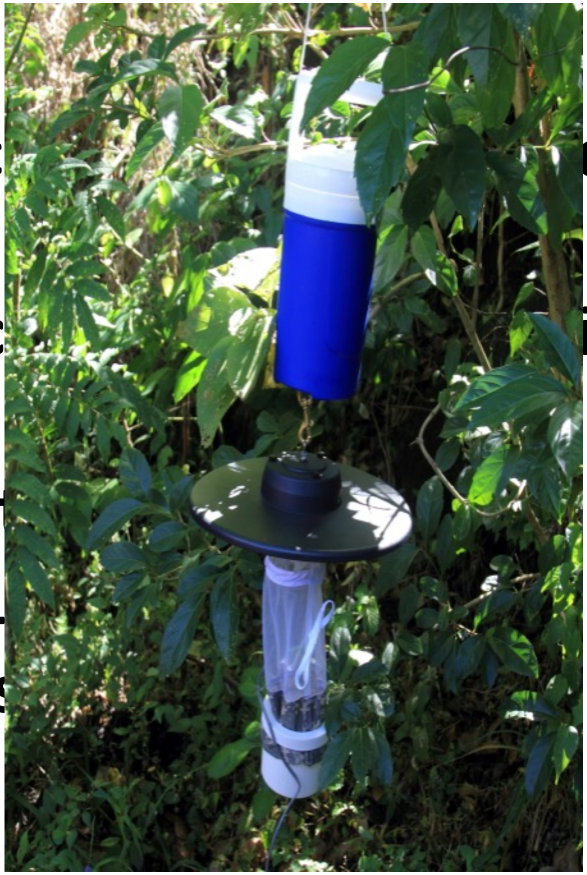
Disruption can start with a single question

Can we use mosquitos as sensors to detect and monitor infectious disease around the globe?

Microsoft

Zorn, AAAS 2017

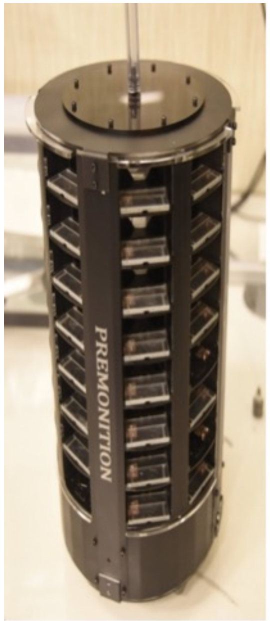
Project Premonition: Mosquitos as Sensors for Environmental Telemetry



Catc**cts** of

Macing frequency

Ligh
12-1
Reus



C02-baited CDC UV trap, circa 2015

Premonition trap, 2016

Microsoft

Images courtesy of Ethan Jackson

Zorn, AAAS 2017

Internet of (Field Biology) Things: Premonition

Analysis identifies Infectious diseases

Repeat

Drone identifies placement sites

Mosquito trap located in likely spots

DNA samples sent to cloud

Zorn, AAAS 2017

Deployed In Houston (June 2016)

87 experiments

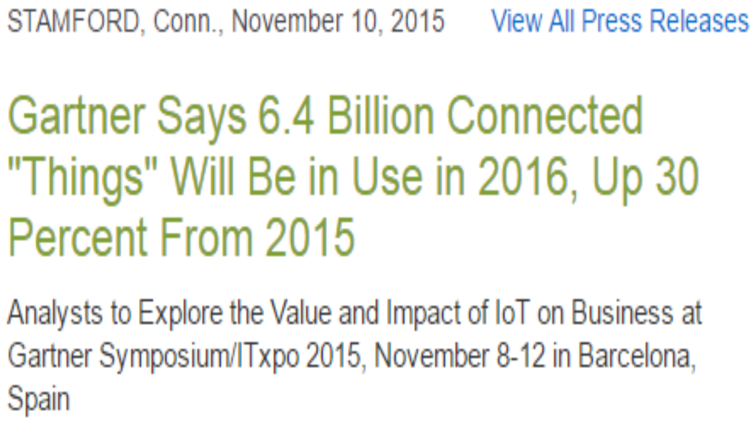
>19 hours data collection per experiment

>20 GB mosquito behavior and abiotic data

>22,000 mosquito events detected

IoT + AI is Disruptive but…

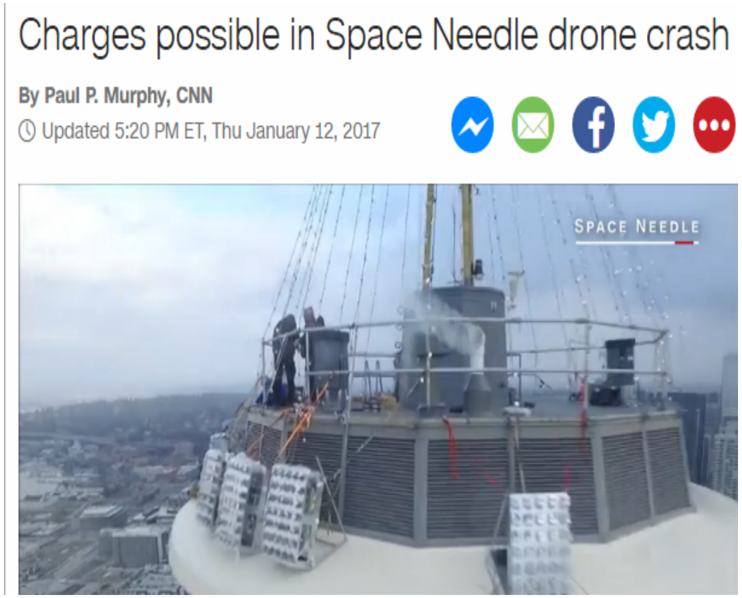
- Benefits and ability to disrupt lead to rapid widespread adoption
- Existing software vulnerabilities become amplified
- Cyber-physical nature of systems introduces new challenges



STAMFORD, Conn., November 10, 2015 View All Press Releases

Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

Analysts to Explore the Value and Impact of IoT on Business at Gartner Symposium/ITxpo 2015, November 8-12 in Barcelona, Spain



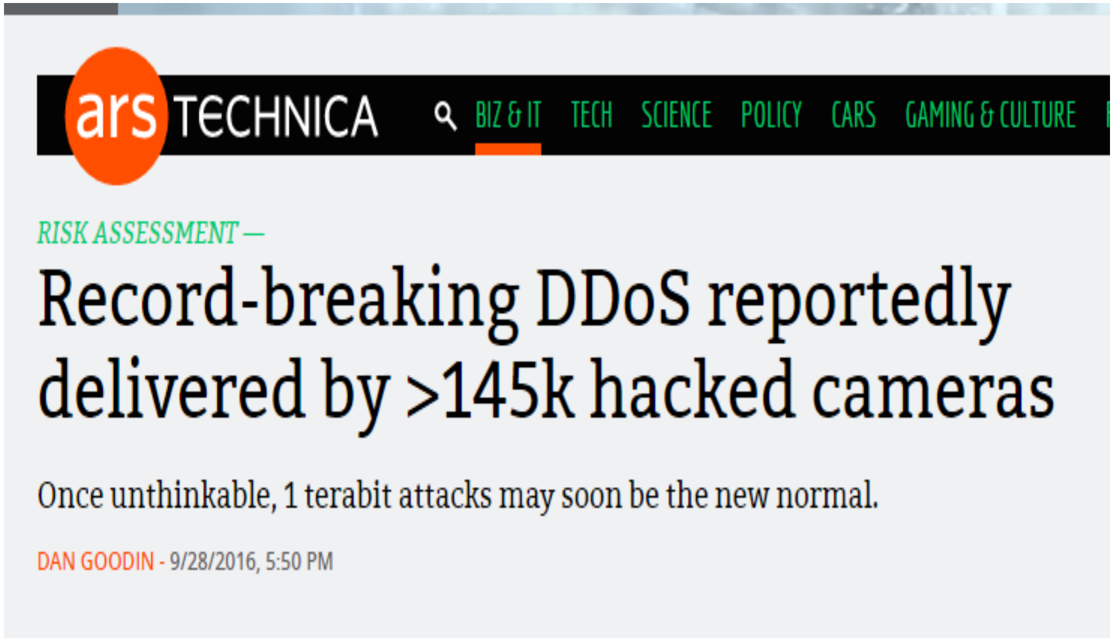
Charges possible in Space Needle drone crash

By Paul P. Murphy, CNN

Updated 5:20 PM ET, Thu January 12, 2017

Zorn, AAAS 2017

IoT Devices Cause Unintended Consequences



RISK ASSESSMENT —

Record-breaking DDoS reportedly delivered by >145k hacked cameras

Once unthinkable, 1 terabit attacks may soon be the new normal.

DAN GOODIN - 9/28/2016, 5:50 PM

Mirai malware used to create
380,000 node device botnet

Botnet was leveraged to deliver massive DDOS attack on KrebsOnSecurity

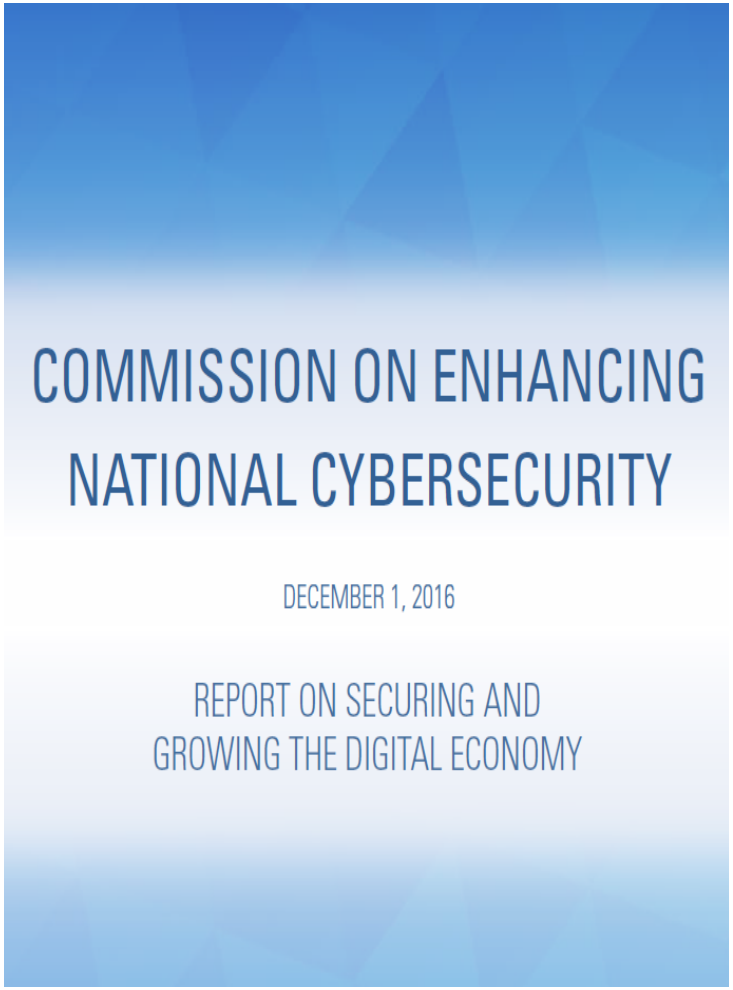
http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Microsoft

Zorn, AAAS 2017

Enhancing National Cybersecurity

- Managing complexity
  - How humans interact with IoT
  - Impact on small businesses
- Defining boundaries, abstractions
  - IoT blurs consumer, safety-critical system boundaries
- Defining metrics (otherwise, how to know if we've improved things?)



COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

Microsoft

Zorn, AAAS 2017

The Cathedral and the Skyscraper

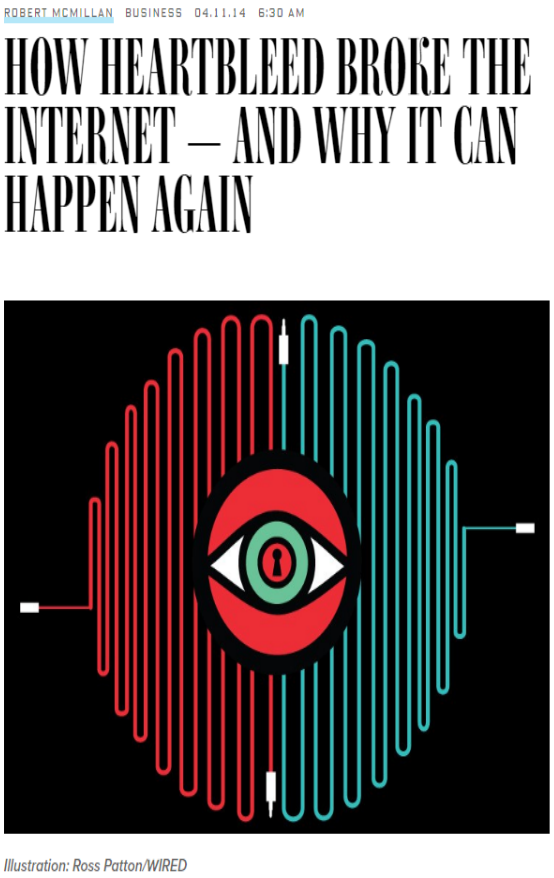
Heroic effort, amazing engineering, one of a kind…

Stronger materials, reusable components, mathematical analysis…

Microsoft

Zorn, AAAS 2017

Example of Infrastructure Weakness: HTTPS



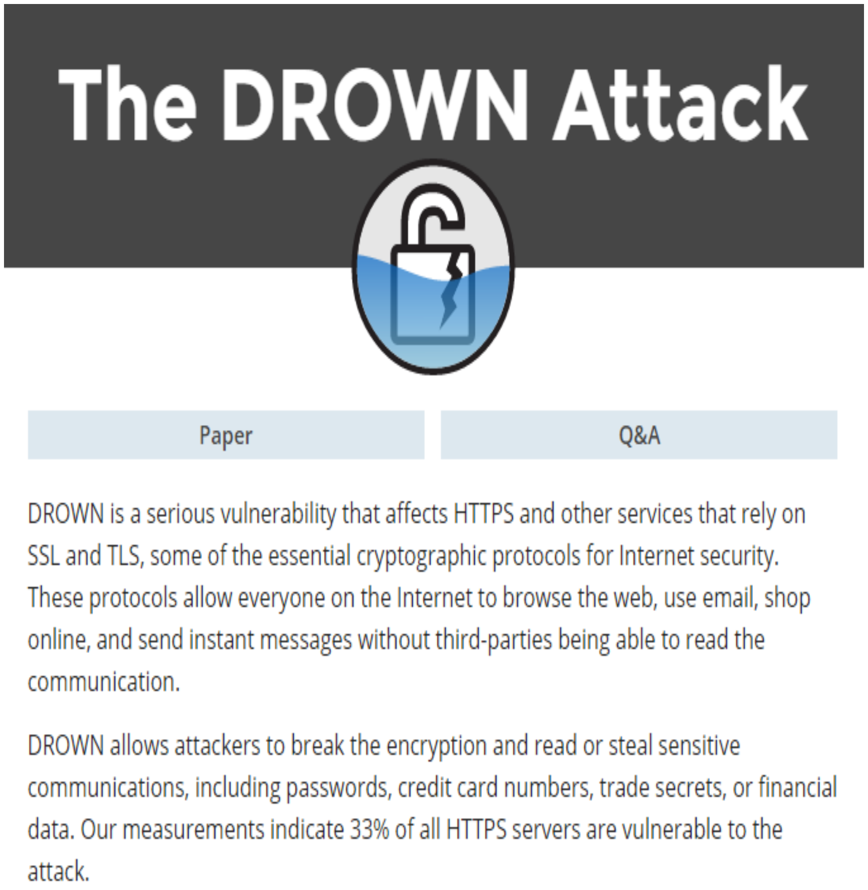
ROBERT MCMILLAN BUSINESS 04.11.14 6:30 AM

HOW HEARTBLEED BROKE THE INTERNET — AND WHY IT CAN HAPPEN AGAIN

Illustration: Ross Patton/WIRED

2014

https://www.wired.com/2014/04/heartbleedslesson/



The DROWN Attack

DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data. Our measurements indicate 33% of all HTTPS servers are vulnerable to the attack.

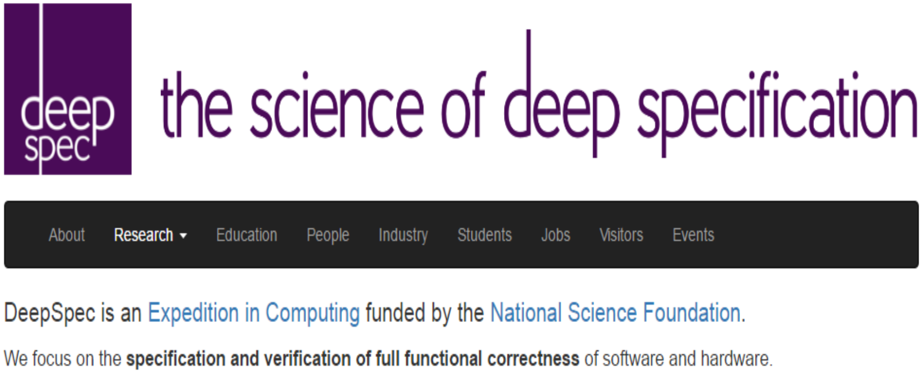
2016 https://drownattack.com/

Microsoft

Zorn, AAAS 2017

Trust but **Verify**
Two Science Expeditions: DeepSpec and Everest

Scalable reasoning meets software verification at scale



DeepSpec is an Expedition in Computing funded by the National Science Foundation.

We focus on the **specification and verification of full functional correctness** of software and hardware.

http://deepspec.org/

Princeton, MIT, Yale, UPenn
$10M NSF Expedition in Computing
Awarded 2016

https://project-everest.github.io/

Microsoft Research (Cambridge, Redmond, Bangalore), INRIA

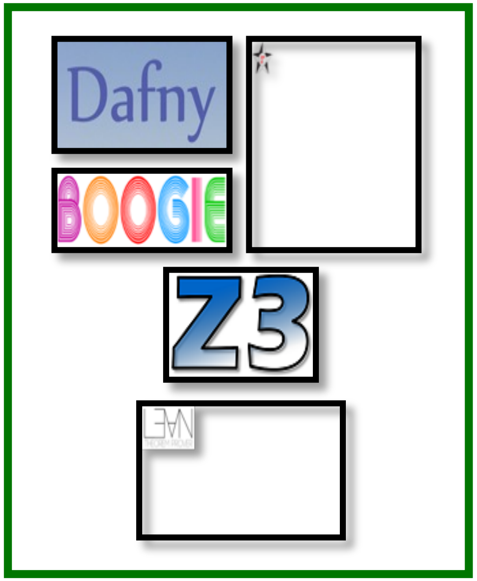
Microsoft

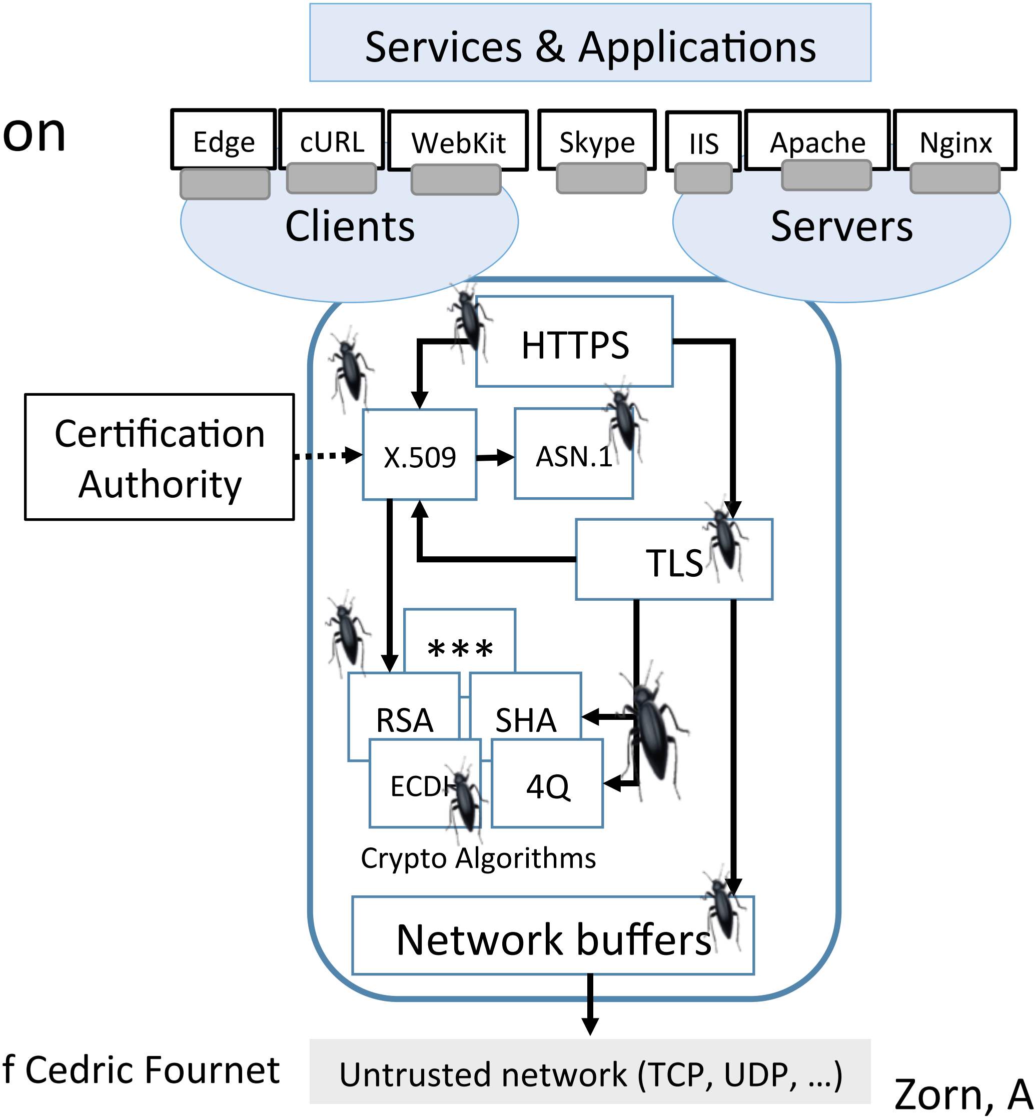
Zorn, AAAS 2017

Everest Mission: Verified HTTPS

Challenges:

- scalability of verification
- performance
- usable tool chain

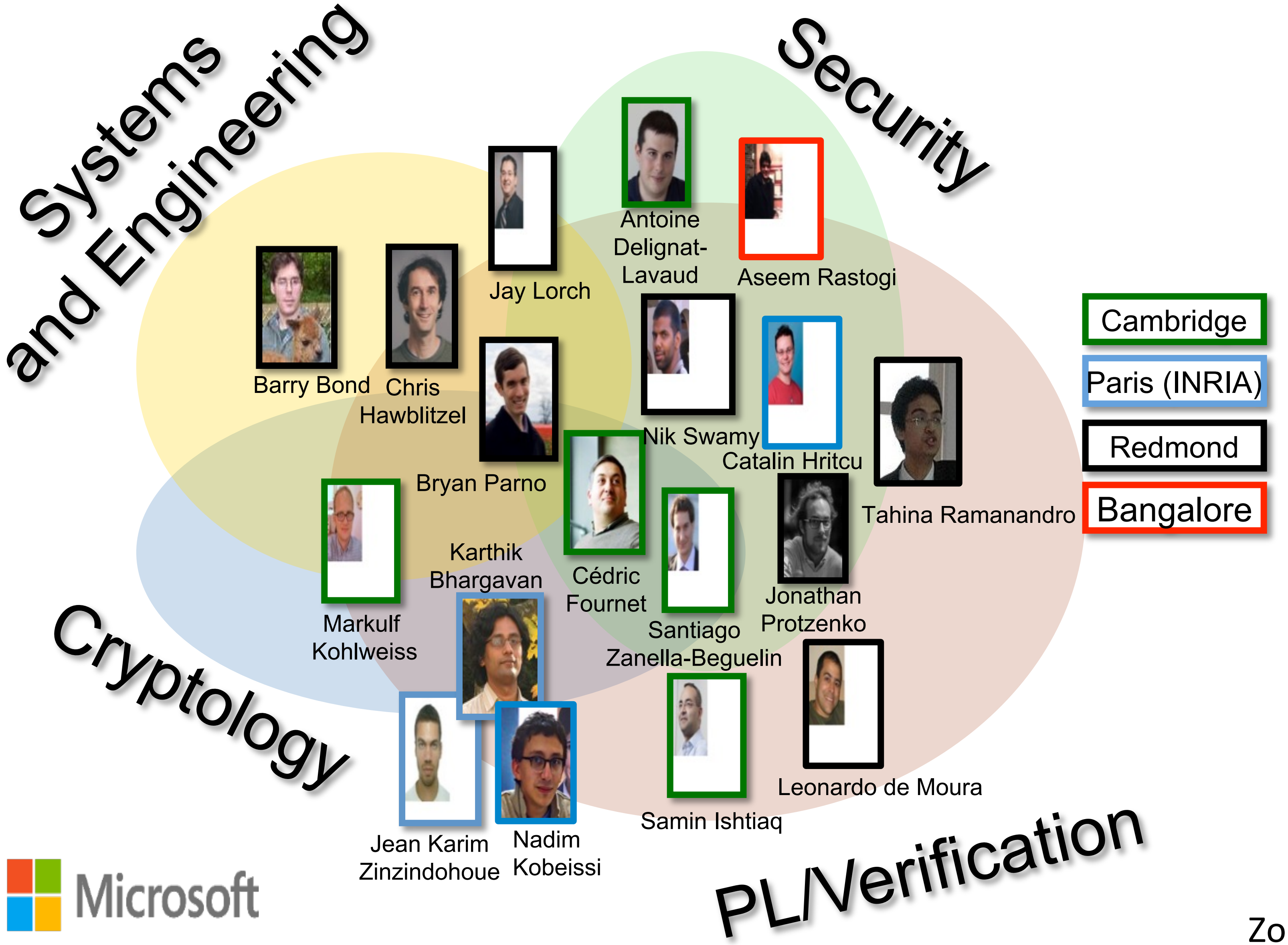




Slide courtesy of Cedric Fournet

Zorn, AAAS 2017

Everest Team Members



Systems and Engineering

Security

Cryptology

PL/Verification

Barry Bond

Chris Hawblitzel

Jay Lorch

Antoine Delignat-Lavaud

Aseem Rastogi

Nik Swamy

Catalin Hritcu

Tahina Ramanandro

Bryan Parno

Cédric Fournet

Santiago Zanella-Beguelin

Jonathan Protzenko

Markulf Kohlweiss

Karthik Bhargavan

Jean Karim Zinzindohoue

Nadim Kobeissi

Samin Ishtiaq

Leonardo de Moura

Cambridge

Paris (INRIA)

Redmond

Bangalore

Microsoft

Zorn, AAAS 2017

Everest Impact on the TLS 1.3 Standard

Everest verification efforts led to many of their proposals being included in the standard:

#4	log-based key separation
	extended session hashes
	(fixing attacks we found on 1.2)
#11	stream terminators
	(eventually fixing an attack)
#14	downgrade resilience
#15	session ticket format
#17	simplified key schedule
	pre-shared-key 0RTT
#18	PSK binding (fixing an attack)

Conclusions

- Science and society will increasingly depend on infrastructure including Cloud Computing, AI, IoT, and Big Data
- To ensure safety, security and privacy, we need to:
  - Understand and measure risks better
  - Develop technical solutions to manage complexity through
    - Well-defined components
    - Automation in testing and verification
    - Ensure critical components are highly vetted
- Empower people to understand the system and potential threats

Thank you!

Research in Software Engineering (RiSE) at Microsoft Research

https://www.microsoft.com/en-us/research/group/research-in-software-engineering-rise/

CCC Computing in the Physical World Task Force

CCC

Computing Community Consortium

Catalyst

http://cra.org/ccc/task-forces/computing-in-the-physical-world/

Follow me: @benzorn https://twitter.com/benzorn

Microsoft

The Future of Smart Environments and the Internet of Things

Shwetak Patel

University of Washington

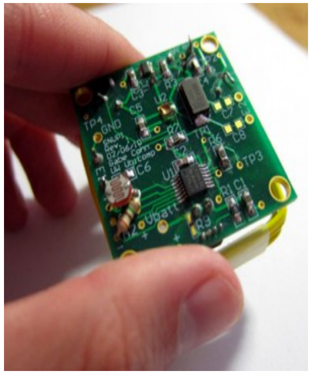
Emerging Smart Environments

- Increasing computation and connectedness in things we may not even be exposed to

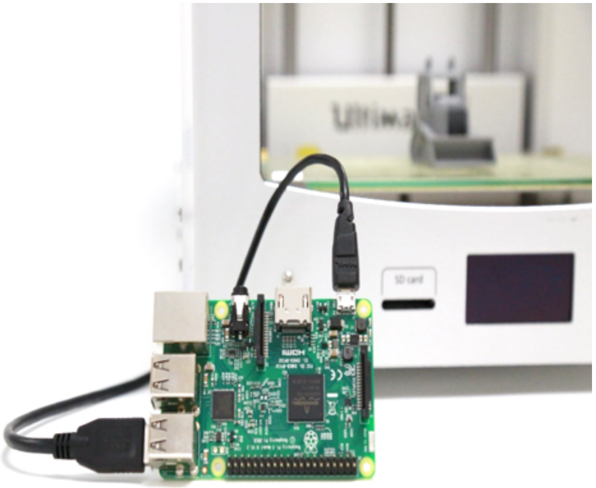
Malfunction
Low Fluid Maintenance Needed
Supply Low, Inventory Needed
Production Complete
Software Update in Progress

The Perfect Storm

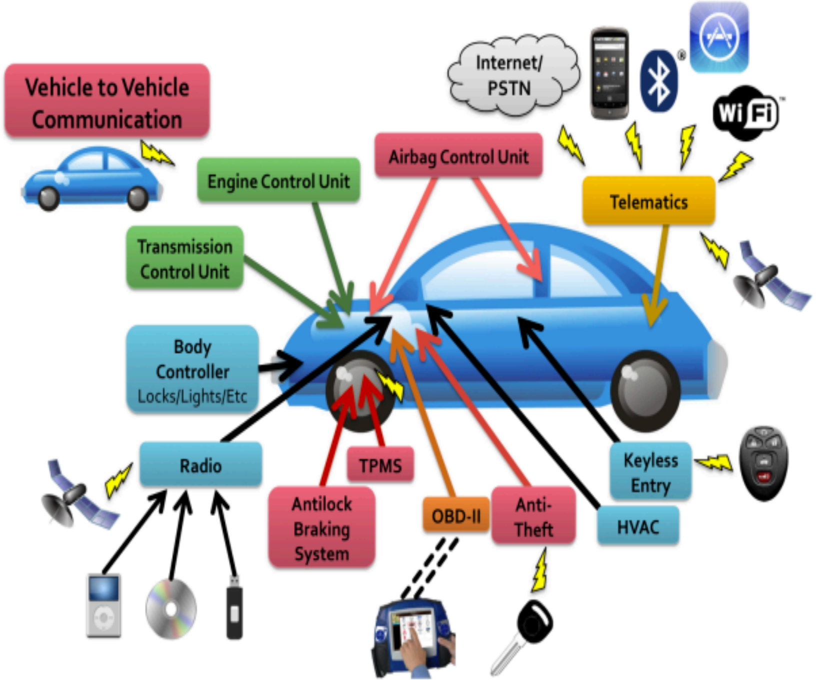
- Reduced computational costs
- Sensor advancements
- Cloud computing
- Rapid prototyping
- Increasing investments in IoT



KICKSTARTER



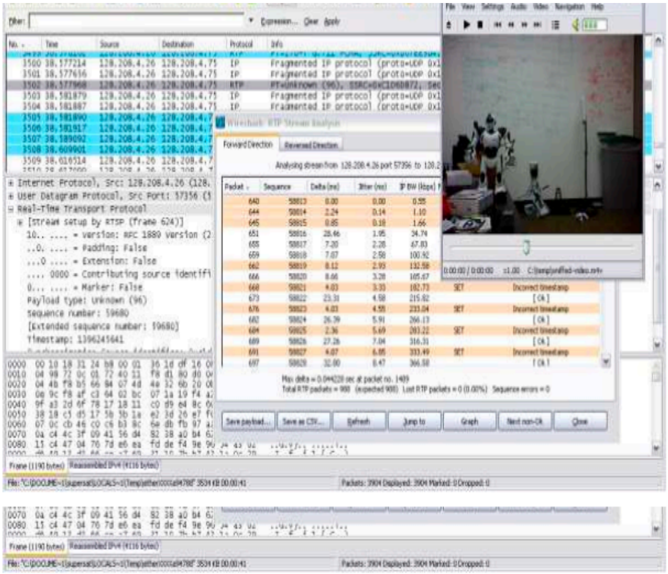
Example Scenarios: The Modern Automobile



http://www.autosec.org/

Example Scenarios: Home Automation

Example Scenarios: Connected Toys



```
No.   Time       Source        Destination   Protocol Info
3500 38.577214  128.208.4.26  128.208.4.75  IP       Fragmented IP protocol (proto=UDP 0x1
3501 38.577636  128.208.4.26  128.208.4.75  IP       Fragmented IP protocol (proto=UDP 0x1
3502 38.577968  128.208.4.26  128.208.4.75  RTP      PT=Unknown (96), SSRC=0xC1D60872, Seq
3503 38.581879  128.208.4.26  128.208.4.75  IP       Fragmented IP protocol (proto=UDP 0x1
3504 38.581887  128.208.4.26  128.208.4.75  IP       Fragmented IP protocol (proto=UDP 0x1
3505 38.581890  128.208.4.26  128.208.4.7
3506 38.581917  128.208.4.26  128.208.4.7
3507 38.589092  128.208.4.26  128.208.4.7
3508 38.609901  128.208.4.26  128.208.4.7
3509 38.610514  128.208.4.26  128.208.4.7
```

```
+ Internet Protocol, Src: 128.208.4.26 (128.
+ User Datagram Protocol, Src Port: 57356 (5
- Real-Time Transport Protocol
  + [Stream setup by RTSP (frame 624)]
    10.. .... = Version: RFC 1889 Version (2
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifi
    0... .... = Marker: False
    Payload type: Unknown (96)
    Sequence number: 59680
    [Extended sequence number: 59680]
    Timestamp: 1396245641
```

```
0000  00 10 18 31 24 b8 00 01  36 1d df 16 0
0010  04 98 72 0c 01 72 40 11  f8 d1 80 d0 0
0020  04 4b f8 b5 66 84 07 4d  4e 32 6b 20 0
0030  0e 9c f8 af c3 64 02 bc  07 1a 19 f4 a
0040  9f a3 2d 6f 78 17 18 11  c0 d9 e4 8c 0
0050  38 18 c5 d5 17 5b 5b 1a  e2 3d 26 e7 f
0060  07 0c cb 46 c0 c6 b3 8c  6e db fb 97 a
0070  0a c4 4c 3f 09 41 56 d4  82 38 a0 b4 6
0080  15 c4 47 04 76 7d e6 ea  fd de f4 9e 9
```

Frame (1190 bytes) Reassembled IPv4 (4116 bytes)

Analysing stream from 128.208.4.26 port 57356 to 128.2

Packet	Sequence	Delta (ms)	Jitter (ms)	IP BW (kbps)	Marker	Status
640	58813	0.00	0.00	0.55		
644	58814	2.24	0.14	1.10		
645	58815	0.85	0.18	1.66		
651	58816	28.46	1.95	34.74		
655	58817	7.20	2.28	67.83		
659	58818	7.07	2.58	100.92		
662	58819	8.12	2.93	132.58		
666	58820	8.66	3.28	165.67		
668	58821	4.03	3.33	182.73	SET	Incorrect timestamp
673	58822	23.31	4.58	215.82		[Ok]
676	58823	4.03	4.55	233.04	SET	Incorrect timestamp
682	58824	26.39	5.91	266.13		[Ok]
684	58825	2.36	5.69	283.22	SET	Incorrect timestamp
689	58826	27.26	7.04	316.31		[Ok]
691	58827	4.07	6.85	333.49	SET	Incorrect timestamp
697	58828	32.00	8.47	366.58		[Ok]

Max delta = 0.044220 sec at packet no. 1409
Total RTP packets = 900 (expected 900) Lost RTP packets = 0 (0.00%) Sequence errors = 0

File: "C:\DOCUME~1\supersat\LOCALS~1\Temp\etherXXXXa04788" 3534 KB 00:00:41 Packets: 3904 Displayed: 3904 Marked: 0 Dropped: 0

```
0070  0a c4 4c 3f 09 41 56 d4  82 38 a0 b4 6
0080  15 c4 47 04 76 7d e6 ea  fd de f4 9e 9
```

Frame (1190 bytes) Reassembled IPv4 (4116 bytes)

File: "C:\DOCUME~1\supersat\LOCALS~1\Temp\etherXXXXa04788" 3534 KB 00:00:41 Packets: 3904 Displayed: 3904 Marked: 0 Dropped: 0

Emerging Challenges

- Physical and safety security is now threated through a digital connection
- Many more entry points for malware
- Technology abandonment
- “Zombie” devices – Devices that are no longer supported
- Difficult design tradeoffs

Example of a Design Tradeoff Challenge in IoT

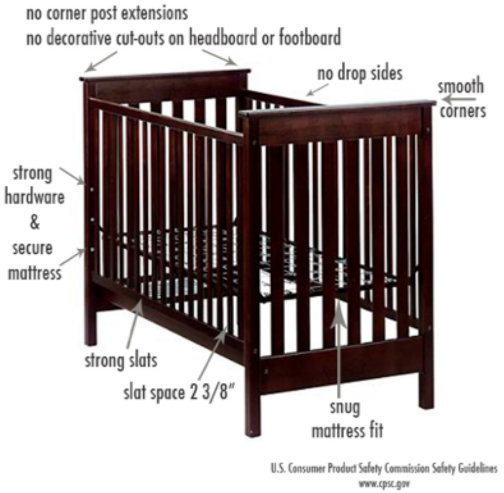
- Updating the firmware of a WiFi-enabled lightbulb

New Considerations

- Guidelines around physical safety
  - Think about what happens in a home inspection

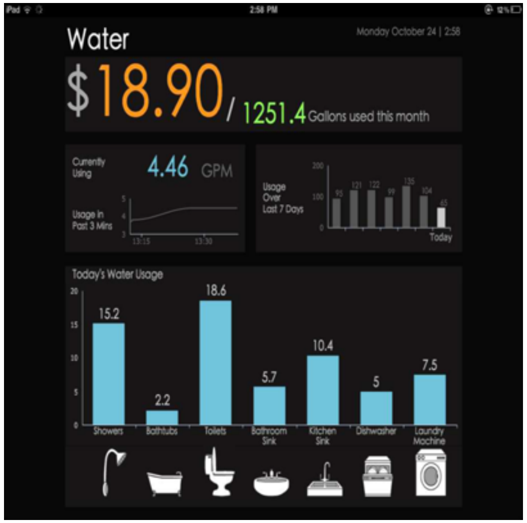
New Considerations

- Guidelines need to go beyond just interoperability
  - Think about baby cribs or child car seats and the minimum requirements for them now


no corner post extensions
no decorative cut-outs on headboard or footboard
no drop sides
smooth corners
strong hardware & secure mattress
strong slats
slat space 2 3/8"
snug mattress fit
U.S. Consumer Product Safety Commission Safety Guidelines
www.cpsc.gov

The Future of Smart Environments and IoT

- Huge potential to improve our daily lives (and already is)



iPad 2:58 PM

Water

Monday October 24 | 2:58

$18.90 / 1251.4 Gallons used this month

Currently Using 4.46 GPM

The Future of Smart Environments and IoT

- Will require a much more coordinated effort between the R&D and policy sectors

- Fundamental rethinking of standard and priorities

- Societal adaption and how to manage/mitigate risk (e.g., when opting out is no longer possible)

Policy Suggestions

- Define lifecycle requirements for IoT devices and the companies that sell them.
- Define objective measures of software quality (akin to existing certification) for a broader range of software/ IoT devices
- Consider user interfaces as a part of quality checks (akin to FDA 510k usability tests)
- Create mechanisms for privacy audits. How is information in the home collected, stored and shared?

Thanks!

- shwetak@cs.washington.edu
  - https://ubicomplab.cs.washington.edu/

- CCC Computing in the Physical World Task Force
  - http://cra.org/ccc/task-forces/computing-in-the-physical-world/

RELATED RESOURCES

- Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things
  - http://cra.org/ccc/SafetyinIoT

- Systems Computing Challenges in the Internet of Things
  - http://cra.org/SystemChallengesinIoT

- Smart and Pervasive Health Research Roadmap: Executive Summary
  - http://cra.org/ccc/SmartHealthExec

- AAAS Panel Slides: What Happens When Everyday Objects Become Internet Devices: A Science Policy Agenda
  - http://cra.org/ccc/CCCatAAAS17

- CCC Task Forces (http://cra.org/ccc/task-forces/)
  - Artificial Intelligence and Robotics Task Force
  - Healthcare Task Force
  - Computing in the Physical World Task Force
  - Convergence of Data and Computing Task Force
  - Privacy and Fairness Task Force

CCC
Computing Community Consortium
Catalyst

WHAT HAPPENS WHEN EVERYDAY OBJECTS BECOME INTERNET DEVICES: A SCIENCE POLICY AGENDA

Elizabeth Mynatt
Georgia Tech
mynatt@cc.gatech.edu

Ben Zorn
Microsoft Research
Ben.zorn@microsoft.com

Shwetak Patel
University of Washington
shwetak@cs.washington.edu

Ann Drobnis
CCC Director
adrobnis@cra.org