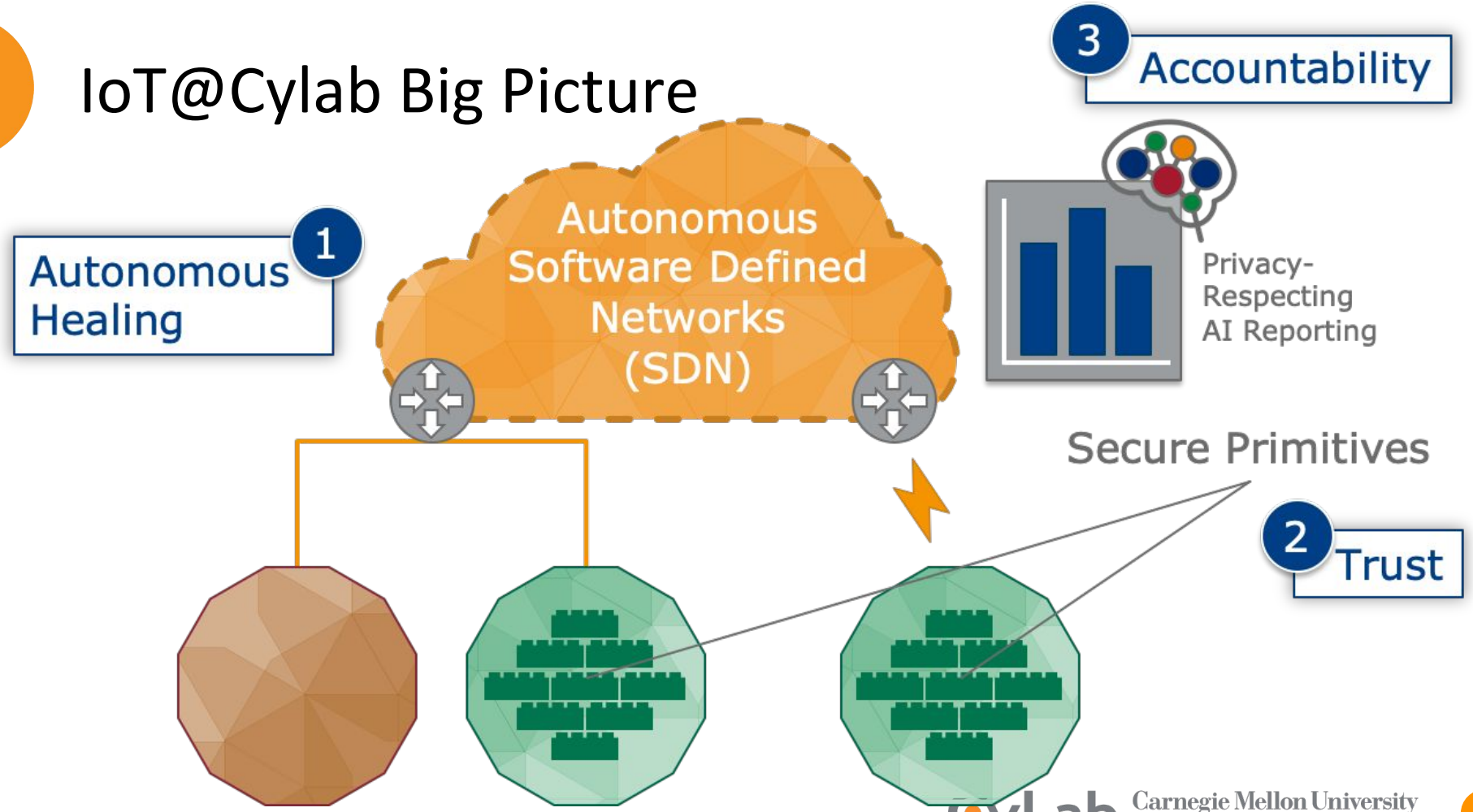
Carnegie Mellon University
CyLab
Security and Privacy Institute

The Secure & Private IoT Initiative Y2 Update

Anthony Rowe and Vyas Sekar
on behalf of IoT@Cylab PIs, students, postdocs, staff

IoT@Cylab Big Picture

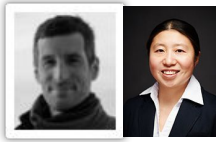


Beginnings

- Started 2019
- Year 1: 12 projects
- Year 2: 10 projects

TRUST Year 1 Projects

- Securing Embedded Software
  David Brumley



- Toward a smarthome IoT infrastructure free of privacy leaks and software vulnerabilities
  Lujo Bauer and Limin Jia

- Lightweight Quantized Deep Neural Networks for IoT Devices
  Shawn Blanton and Diana Marculescu

- IoT Device Privacy and Security Nutrition Labels
  Lorrie Cranor Yuvraj Agarwal

ACCOUNTABILITY Year 1 Projects

- Internet of Things Compliance Gaps Under New California Laws
  Aleecia M. McDonald

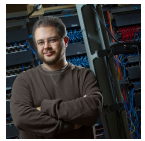
- Third-Party Network Traffic Attribution and Cross-Device User for IoT and Web
  Timothy Libert

- Privacy-preserving Inference and Decision-Making with IoT Data
  Gauri Joshi and Osman Yagan

- Privacy Preserving Data Analytics using Secure Multi-Party Computation
  Vipul Goyal

AUTONOMOUS HEALING Year 1 Projects

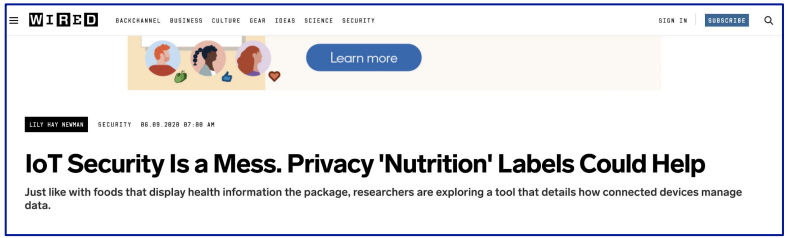
- Flipping the Cloud: Managing and Protecting IoT Interactions among Mutually Distrusting Stakeholders at the Network Edge
  Patrick Tague

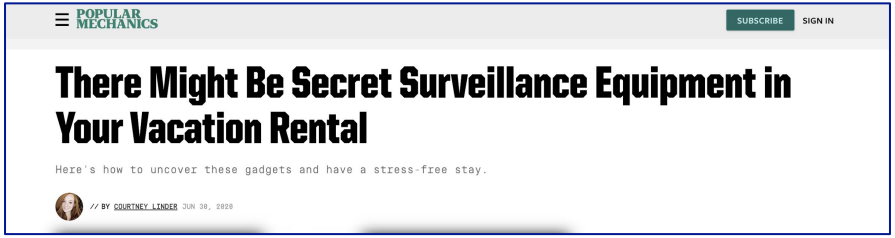


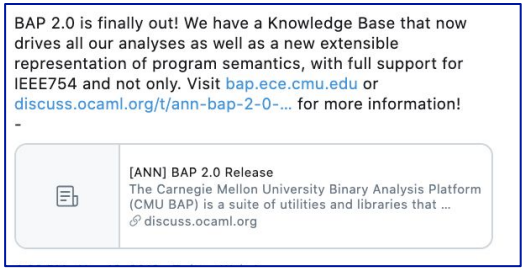
- IoTHub for Managing and Securing Devices in the Home
  Jason Hong

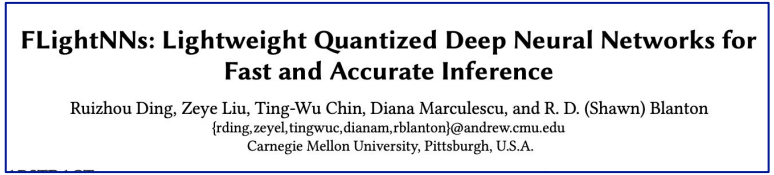
- Do-it-Yourself-Locally: An IoT architecture For L  Data Control for Privacy and Security
  Yuvraj Agarwal

Highlights and Mentions









.....

Year 1 vs Year 2

Year 1

- More consumer
- More home

Year 2

- Shift to more Industrial
- Industrial focus for the remaining duration
- Addition of an educational component

Overview of Year 2 Projects

Trustworthy Platforms

- Hardware Redaction via Designer-Directed Fine-Grained eFPGA Insertion (Ken Mai)
- Lightweight Security Architectures for IoT Fog Networks (Osman Yagan, Swarun Kumar)
- Quantized Deep Neural Networks for Fingerprint Recognition (Shawn Blanton)

Overview of Year 2 Projects

Accountability

- Third-Party Network Traffic Attribution for IoT, TV, Web, and Mobile (Tim Libert)
- IoTSniffer: Detecting Unauthorized Traffic in Industrial IoT (Swarun Kumar)
- Privacy Tradeoffs in Distributed Learning (Carlee Joe-Wong)

Overview of Year 2 Projects

Autonomous Healing Networks

- Systematic Attack Generation for Industrial Control Systems (Eunsuk Kang)
- Robust ML-based anomaly detection for industrial IoT (Lujo Bauer)
- Zero-Knowledge Network Security Analysis using Generative Adversarial Networks (Giulia Fanti)

Education

- Expanding picoCTF into IoT/IIoT—Year 0 (Hanan Hibshi, Maverick Woo)

Expanding picoCTF into IoT/IIoT—Year 0

Personnel

- Hanan Hibshi, Research & Teaching Scientist, INI (Co-PI)
- Maverick Woo, Systems Scientist, CyLab (Co-PI)
- Megan Kearns, Special Projects Administrator, CyLab
- Arjun Brar, Master's Student, INI

Objectives

- Conduct exploratory activities in 2020 to prepare for the production of a future IoT/IIoT-themed picoCTF competition, which will tentatively launch in AY21
- Produce syllabus covering IoT/IIoT concepts that are suitable for the typical picoCTF audience
- Organize an IoT/IIoT story writing competition in 2020 as a method to acquire an interesting IoT/IIoT-themed story for use in 2021 production activities

Updates

- Identified need to match expectation of AP CSP teachers when developing HS syllabus
- Hired first RA (and still hiring)
- Developed Android problem template on the picoCTF platform to facilitate writing future Android problems

Status

- Curating a collection of suitable IoT/IIoT concepts for syllabus
- Surveying existing IoT/IIoT exposures at HS level
- Writing several more Android problems before May
- Making problem development plans for summer—ARM, IDOR, MQTT

Synergies and Amplification

External

- Next Manufacturing, Manufacturing Futures Initiative
- Mill19

Internal

- Student run reading group and webinars
- New faculty/student engagements