TECHNICAL OVERVIEW

# Secure and Private Internet of Things Initiative @CyLab

## Why IoT? Why Now? What's Different?

The world is reaching a critical point in the growth of the Internet of Things or IoT. Cars, planes, satellites, thermostats, and refrigerators all now have computers connected together on the global Internet. Like many other disruptive technologies, IoT holds the potential for transforming industries, cities, as well as our daily lives.

While IoT has huge potential for societal impact, it comes with a number of key security concerns. Since IoT devices will typically be embedded deep inside networks, they are attractive attack targets and may become the "weakest link" for breaking into critical infrastructures, or for leaking sensitive information about users and their behaviors. These can entail significant negative consequences and costs, and these concerns may ultimately curtail the potential deployments and benefits in terms of new technology-enhanced capabilities, cost and energy savings, and societal applications.

As these devices sense and actuate the physical environment, they also raise new risks of *cyber-physical* threats in contrast to traditional cybersecurity concerns. These are not merely hypothetical concerns and several actual attacks have already been reported. What makes this especially challenging is that, IoT, unlike general purpose computers, typically have a limited interface and are designed to "just work" while typical laptops, tablets, and phones are general purpose and "for work." IoT devices should work without user configuration, be connected to the global network, but should also be much more resilient than general-purpose computers.

Carnegie Mellon University
CyLab
Security and Privacy Institute

## Our Vision for Secure and Privacy-Aware IoT

*Our goal is to develop an **end-to-end** and **operational** IoT "stack" that is **secure and privacy-preserving** from the **ground up** to serve as a reference platform for future products and deployments in industry, government and academia.*

Safety/security is the second basic level in Maslow's hierarchy---Without security, nothing else matters! Technologies with built-in security and privacy-awareness are enablers – imagine the innovation that could arise when trust is established between parties where it didn't exist before. For instance, the combination of websites with SSL certificates ignited e-commerce to the point where nobody thinks twice about the safety of ordering products online. IoT is at a similar inflection point where the (in) security and privacy fears may be fundamental impediments to realizing the potential societal benefits in many market verticals and thus it behooves us to tackle this imminent grand challenge.

Notice that we have highlighted three other key phrases that define our vision. First, by "end-to-end", we cannot afford a piecemeal approach that looks at hardware, middleware, applications, and users in isolation. Rather, we need to look at these with a holistic approach. Second, we believe in "operational" real-world systems that also apply to legacy infrastructures and not mere toy prototypes. Finally, we want to design resilient systems that are intrinsically "secure and privacy-preserving" rather than seek incremental band-aids.

## Our Approach: What's different?

We believe that Carnegie Mellon is uniquely positioned to realize this ambitious vision. CyLab is a university-wide security and privacy institute with an interdisciplinary culture and history of building real-world systems in collaboration with industry. With over 100 faculty, 120 graduate students, and 25,000 square feet of collaborative research space, CyLab is the largest academic hub of security and privacy experts.

New research at CyLab in secure architectures, software-defined networks, wireless systems, and automated program analysis have laid promising foundations to ensure that our vision of this new paradigm in IoT is within reach. We are currently designing and building an IoT testbed that integrates a wide variety of commercial devices alongside with emerging research prototypes. The testbed provides a reconfigurable communication fabric for emulation of network topologies with a mixture of physical layers (wired and wireless) and programmable link parameters and traffic patterns. This will enable us to flexibly support the emulation of key IoT market verticals (e.g., healthcare, industrial control systems, and smart cities). Each test device can be augmented with a set of external sensors and actuators that are able to record and control real-world I/O like temperature, light-level, vibration, audio and tactile switches. Our framework allows these transducers to be easily choreographed with network messages while providing logging and real-time visualization. Our goal is to create a comprehensive suite of tools that can use both cyber and physical properties to aid in identifying security risks, prototyping protection schemes, evaluating usability and analyzing interactions found in real-world IoT systems.

## Key Research Challenges

We envision four broad classes of research challenges in realizing our vision. These research thrusts naturally correspond to different stages of the lifecycle of design, development, deployment, and operations:

**HARDWARE AND PLATFORM DESIGN**

We need new primitives and abstractions for developing secure operating systems and networking technologies, and corresponding testing and verification mechanisms to formally reason about their correctness.

**APPLICATION DEVELOPMENT**

We need user-friendly and intuitive programming and policy abstractions and toolchains for application developers to express their intents.

**INTEGRATION AND DEPLOYMENT**

The technology stack must deal with limited interfaces, different zones-of-trust, BYOD (bring your own device), and dynamically reconfigure itself as new threats arise.

**OPERATIONS**

Finally, we need to develop the corresponding "DevOps" like abstractions for day-to-day management of the IoT system to keep the system updated and secure in response to new threats, vulnerabilities, and potential breaches in other parts of the ecosystem

**Hiring a top engineer costs over $200K/year without overhead. For the same cost through this sponsorship, you will extend your team by 10+ of the world's best and leading researchers in security, privacy and IoT technology with decades of experience. Your company will get direct access to a team working on a $1M+ project, and at least a 5X amplification of your research dollars.**

## Value proposition for our sponsors

Progress is being made, however greater collaboration is required to reduce the security issue hindering IoT adoption that everyone is talking about.

We have the opportunity to disrupt industries with the first secure IoT internet-ready research, principles, and testbed technology. But we recognize industry participation is a key ingredient, and we need leaders with visionaries of their own on staff who want to get us out of the insecure rut we're all in with IoT.

We care passionately about IoT security, so we are investing the next five years in this pursuit. We've dedicated space, hired the brightest minds in IoT from all over the world and brought the smartest graduate students to CMU. Now we want to focus that effort to change the world.

It takes experts to create brand-new paradigms, so we want to work alongside a limited number of hand-picked technology leaders. We believe having the right people on a collaborative team can disrupt an industry.

We also understand management looks for additional value added. In our program, your company will be given the opportunity to:

- **Build your company brand on campus** to enhance recruitment of top, high-value in-demand students. You will develop personal relationships and gain preferred access to the world's foremost experts in security — the kind that are incredibly difficult to find, and even more difficult to hire.
- **Hold a position on the initiative Board of Directors** with a seat at the table and vote during a yearly strategy meeting evaluating which promising projects to fund.
- **Have early access to research and a living lab** that provides a springboard for innovative thinking and products. Research you can leverage to get a head-start on where to focus your in-house research and development teams to build intellectual property and get to market faster at a lower cost. Gain deep understanding of research results through exclusive meetings, events, private forums and on-site space for direct access to researchers and persistent access to students working on the living lab.

As the IoT world continues to boom, there has never been a more crucial time to push towards more reliable but affordable security and privacy.

# Do you want to work alongside CMU and other technology leaders to build a secure IoT world ?

The first step towards realizing our shared vision is an exploratory session with Michael Lisanti, Associate Director of Partnership Development for CyLab. Michael can be reached at mlisanti@cmu.edu or 412-268-1870.

We look forward to hearing from you!

ANTHONY ROWE

**Secure and Private IoT@CyLab**

VYAS SEKAR

CyLab professors Dr. Anthony Rowe and Dr. Vyas Sekar teach in the Electrical and Computer Engineering (ECE) department within the College of Engineering at Carnegie Mellon. Their research stretches across the IoT ecosystem from real-time embedded systems and sensing for critical infrastructure to software defined networking and security. Recognized nationally and internationally for their expertise, Rowe and Sekar have won multiple research awards from federal agencies including Advanced Research Projects Agency-Energy (ARPA-E), U.S. Department of Energy (DOE), National Science Foundation (NSF) and Office of Naval Research (ONR). They have published in top research conferences Association for Computing Machinery (ACM), Cyber Security Awareness Week (CSAW) and Institute of Electrical and Electronics Engineers (IEEE). Rowe and Sekar have an extensive track record working with industry partners.

Carnegie Mellon University
CyLab
Security and Privacy Institute

"We are passionate about creating a world in which people trust technology."

**cylab.cmu.edu**