Rethinking a Secure Internet of Things

http://iot.stanford.edu

The Internet will soon connect us to the physical world through personal health monitors, proximity networks, smart homes, smart cars, and automation networks. These new networks provide tremendous opportunity, but also tremendous risk. Today, hackers steal credit card numbers; tomorrow, they will be able to control your home, steal your personal medical data, and track you as you walk down the street. Existing approaches to secure computing systems are insufficient for these new cyber-physical applications, as they have very different trust models and network architectures, bridging pervasive local area networks, personal mobile devices, server storage, and web-based applications.

The Secure Internet of Things Project (SITP) is a 5-year collaboration between Stanford, UC Berkeley, and the University of Michigan to research fundamentally new, better ways to secure the Internet of Things and make them easy to use. The project seeks to answer three principal questions:

Analytics: how will we integrate these enormous streams of physical world instrumentation with all of our existing data?

Security: how can pervasive sensing and analytics systems preserve and protect user security?

Hardware and software systems: what hardware and software systems will make developing new intelligent and secure Internet of Things applications as easy as a modern web application?

These three efforts are tightly connected. Internet of Things (IoT) applications will need novel cryptographic protocols that are able to work on tiny, low-power devices yet also scale up to enormous stores of data in the cloud.

End-to-End Security

The key guiding principle behind the project is end-to-end security that supports application data processing. With end-to-end security, data is encrypted before it leaves a sensor and is not decrypted until viewed by an end-user: private data remains confidential as it passes through gateways, mobile devices, and cloud systems. With end-to-end security, your data is safe even if any point along the entire data pipeline is compromised.

The pipeline must be able to process this data. Data analytics is one critical application for the Internet of Things. A data pipeline that can process and merge rich streams of data with existing, archival data will provide new insights and results. Today, analytics algorithms operate on huge repositories of data. This data is valuable and can be very sensitive. Holding this data is a liability and requires that the end user trust its holder. What if we could write applications whose servers perform complex analytics on data without knowing what the data means?

Recent advances in cryptography have shown that is possible to design cryptosystems that can compute on encrypted data. Put another way, it's possible to send encrypted data to a server, ask it to perform any computations as needed (e.g., answer queries, compute statistics), and yet not let it learn anything about the data. Furthermore, recent results have also shown that such cryptosystems can be practical as long as they are designed for a narrow set of computations. Cryptosystems that support arbitrary computation can have a million-fold slowdown, but crypto protocols designed for a specific application or algorithm can impose only a small constant factor overhead.

Application Development Frameworks

A system is only as secure as its hardware and software. Most IoT applications follow a common architecture, consisting of four parts: embedded devices, a gateway device such as a mobile phone, servers (in the cloud or within the network), and end-user applications. These devices span 3-6 orders of magnitude in resources and each use their own languages, operating systems, and application frameworks. Verifying and establishing security properties across this mish-mash of existing systems is intractable. We will research new operating systems,

network protocols, and tools that can verify that an application across all of these devices maintains its security properties.

Finally, if security is difficult to use, developers will work around it. Our goal is to make secure, powerful Internet of Things applications as easy as a modern web application. Rather than take 10 engineers two years, it should take 3 engineers two months. Making complex cyber-physical applications easy to prototype and deploy will democratize development and lead to a whole new ecosystem of tools, APIs, and software. IoT systems are unique in that they bridge hardware and software even in their earliest stages. Computer science departments across the world are educating hundreds of thousands of students, but most software engineers think hardware is daunting. We will explore software-defined hardware, that is, enabling software engineers to specify an entire IoT device by specifying what libraries and features their code needs.

Why Now?

Both industry and academia have been talking about the coming Internet of Things for several years. This raises the question: why tackle this research agenda now? Why is now the right time to embark on this research project? What's changed?

The low-level technology has. In the past 9 months, several technological advances deeply tied to the Internet of Things have become mainstream. Until now, long-lived embedded systems have been constrained to 8 or 16-bit microcontrollers. In the past year, several instances of the ARM Cortex M series -- a 32-bit processor, with the capabilities of a early -90s PC -- have hit the market. Unlike prior M processors, these new devices have sleep currents competitive with microcontollers (μA) and so can last years on small batteries. Second, Apple's inclusion and embrace of Bluetooth Low Energy through its iBeacon framework has opened the door to pervasive proximity networking. Connecting pervasive networks to mobile devices has always been challenging due to a lack of shared radio standards: standard Bluetooth is poorly suited to ubiquitous systems, and mobile devices do not support ZigBee/802.15.4, ZWave, or other ultra-low-power protocols.

Finally, the technology has caught up with the research. Furthermore, it has done so in fascinating and unexpected ways. Cortex M processors enable whole new classes of applications with much greater processing needs than has been possible before. Bluetooth Low Energy enables mobile and human-centric applications based on proximity networking. In short, we as a research community have been waiting for this day to come for the past decade, and it finally has.

Even more encouragingly, it is not too late. While there is a rush to build Internet of Things applications today, the dominant applications and architectures have not yet emerged. We are in the mid 90s of the world wide web: we can see the potential and people are struggling to harness it, but we do not yet have the tools to do so easily and safely. By researching the deep security and systems issues the IoT poses now, we will significantly influence and improve practice for the decades to come. The Internet of Things can be something that we trust and rely on, not something we fear or begrudgingly accept.

Project Goals and Affiliates Program

Our goal is to, over the next five years:

1. Research and define new cryptographic computational models for end-to-end secure analytics and actuation on enormous streams of real-time data from the Internet of Things.
2. Research and implement secure, open source hardware/software frameworks to prototype and build Internet of Things applications that correctly use these new computational models.

The Secure Internet of Things Project is seeking industrial members to join us in achieving these goals. This help takes two forms. First, we hold yearly retreats (around May) in which we present our most recent results to hear feedback and guidance from our members. We also meet with them in smaller settings. These meetings and discussions will help drive our research to solve impactful problems. Second, affiliates support students and faculty

research through an unrestricted contribution. In addition to this industrial support, SITP will also be funded by government (DARPA, NSF, etc.) sources.

A one-year membership in the SITP Affiliates program is $125,000. This funding is sufficient to support a graduate student for a year, hold the yearly retreat, support faculty research over the summer and administrative costs. SITP works closely with other affiliates programs at Stanford, such as the Stanford Data Science Initiative. Please contact Philip Levis and Steve Eglash if you would like to explore joining the program.

Staff and Faculty

Philip Levis
Faculty Director

Steve Eglash
Executive Director

Faculty

Dan Boneh is a Professor of Computer Science at Stanford University where he heads the applied cryptography group. Dr. Boneh's research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, security for mobile devices and the Internet of Things, Web security, and cryptanalysis. He is the author of over a hundred publications in the field and is a recipient of the Godel prize, the Packard Award, the Alfred P. Sloan Award, the RSA award in mathematics and five best paper awards. In 2011 Dr. Boneh received the Ishii award for industry education innovation.

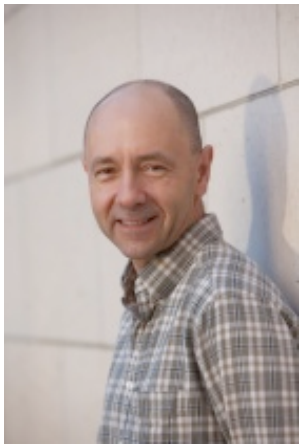
Prabal Dutta is an Assistant Professor of Electrical Engineering and Computer Science at the University of Michigan. He envisions a future in which the Internet of Things results in a trillion new wireless, embedded Internet hosts online within a decade or so. His research interests include how these devices and their software systems should be designed so that they survive and thrive in this not-too-distant future. More broadly, his research interests straddle the hardware/software interface and include embedded systems, networking, and architecture.

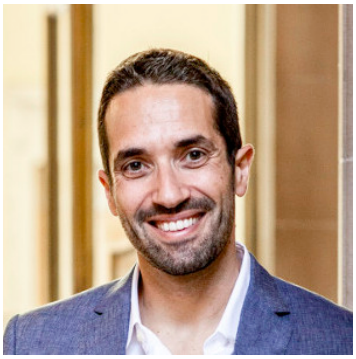
Dawson Engler is an Associate Professor in EE and CS at Stanford. His research focuses on techniques that automatically find serious errors in real code, ranging from system-specific static analysis, to model checking, to symbolic execution. His research group has won numerous ``Best Paper'' awards and its static checking work formed the basis of Coverity, recently purchased by Synposys. His group has submitted thousands of bug reports to the Linux kernel and core libraries such as libc; in some cases these bugs had been known but unfound for over a decade. He won the 2006 ACM SIGOPS Mark Weiser Award and 2009 Grace Hopper Award.

Björn Hartmann is an Assistant Professor in EECS at UC Berkeley. He co-founded the CITRIS Invention Lab where he teaches classes in IoT product design and also co-directs Berkeley's Swarm Lab. His research in Human-Computer Interaction focuses on design, prototyping and implementation tools for the era of post-personal computing. As computation moves away from single-user desktop applications, he investigates how new algorithms, applications and design principles can support the creation of novel user interfaces. He has received a Sloan Fellowship, NSF CAREER, and an Okawa research award.

Mark Horowitz is the Yahoo! Founders Professor at Stanford University and was chair of the Electrical Engineering Department from 2008 to 2012. He co-founded Rambus, Inc. in 1990 and is a fellow of the IEEE and the ACM and a member of the National Academy of Engineering and the American Academy of Arts and Science. Dr. Horowitz's research interests are quite broad and span using EE and CS analysis methods to problems in molecular biology to creating new design methodologies for analog and digital circuits and systems.

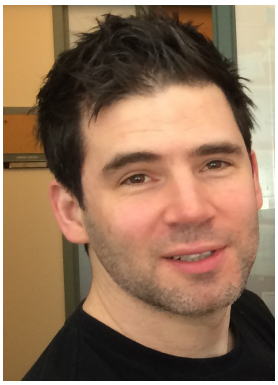
Greg Kovacs is a Professor of Electrical Engineering at Stanford University, with a courtesy appointment in the Department of Medicine, Cardiovascular Division. He holds a BASc (EE) from from the University of British Columbia, an MS (BioE) from U.C. Berkeley, a PhD (EE) and an MD from Stanford. He is a Fellow of the IEEE and AIMBE. Greg has been active in cardiovascular device design, physiology in extreme environments, mixed-signal circuit design, and sensor development, as well as many educational initiatives and co-founding the Bioengineering Department at Stanford. His extensive government work includes serving as Investigation Scientist for the Columbia space shuttle accident investigation as well as Director of the Microsystems Technology Office of DARPA, guiding investment of $1.6B from 2008 - 2010. In 2010, he received the Secretary of Defense Medal for Exceptional Public Service. He has co-founded several companies, including molecular diagnostics innovator Cepheid, and is active in the angel and private equity investment communities. Greg is a pilot, scuba diver, mountaineer and maker.





Christos Kozyrakis is an Associate Professor of Electrical Engineering & Computer Science at Stanford University. He works on architectures, runtime environments, and programming models for parallel computing systems. He co-led the Transactional Coherence and Consistency (TCC) project that developed hardware and software mechanisms for programming with transactional memory. He also led the Raksha project, which developed practical hardware support and security policies to deter high-level and low-level security attacks against deployed software. Christos received a BS degree from the University of Crete (Greece) and a PhD degree from the University of California at Berkeley (USA), both in Computer Science.

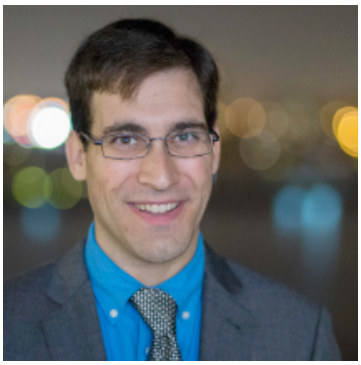
Philip Levis is an Associate Professor of Computer Science and Electrical Engineering at Stanford University, where he heads the Stanford Information Networks Group (SING). His research centers on computing systems that interact with or represent the physical world, including low-power computing, wireless networks, sensor networks, embedded systems, and graphics systems. He has been awarded the Okawa Fellowship, an NSF CAREER award, and a Microsoft New Faculty Fellowship. He's authored over 60 peer-reviewed publications, including three best paper awards, one test of time award, and one most influential paper award. His research is the basis for Internet standards on how embedded devices connect to the Internet (RFC6550 and RFC6206). He has an Sc.B. in Biology and Computer Science with Honors from Brown University, a M.S. in Computer Science from The University of Colorado at Boulder, and a Ph.D. in Computer Science from The University of California, Berkeley.



David Mazières is an associate professor of Computer Science at Stanford University, where he leads the Secure Computer Systems research group. Prof. Mazieres received a BS in Computer Science from Harvard in 1994 and Ph.D. in Electrical Engineering and ComputerScience from MIT in 2000. Prof. Mazieres's research interests include Operating Systems and Distributed Systems, with a particular focus on security. Some of the projects he and his students have worked on include SFS (a self-certifying network file system), SUNDR (a file system that introduced the notion of fork linearizability), Kademlia (a widely used peer-to-peer routing algorithm), Coral (a peer-to-peer content distribution network), HiStar (a secure operating system based on decentralized information flow control), tcpcrypt (a TCP option providing forward-secure encryption), and Hails (a web framework that can preserve privacy while incorporating untrusted third-party apps).

Raluca Ada Popa will be an assistant professor of computer science at UC Berkeley in 2015. She is interested in security, systems, and applied cryptography. Raluca developed practical systems (such as CryptDB and Mylar) that protect data confidentiality by computing over encrypted data, as well as designed new encryption schemes that underlie these systems. Some of her work has had early impact, with Google applying CryptDB's design to their SQL-like BigQuery service and surgeons at Boston's Newton-Wellesley hospital using Mylar to secure their medical application. Raluca is the recipient of a Google PhD Fellowship, Johnson award for best CS Masters of Engineering thesis from MIT, and CRA Outstanding undergraduate award from the ACM. Raluca has received her PhD in computer science as well as her two BS degrees, in computer science and in mathematics, from MIT.

Christopher Ré (Chris) is an assistant professor in the Department of Computer Science at Stanford University. His work's goal is to enable users and developers to build applications using analytics that enable them to more deeply understand and exploit data. Analytic techniques and tools from his group has been incorporated into scientific efforts including the IceCube neutrino detector and PaleoDeepDive, and into Cloudera's Impala and products from Oracle, Pivotal, Google Brain, and Microsoft's Adam.



Keith Winstein is an assistant professor of computer science at Stanford University. His work applies statistical and predictive approaches to teach computers to design better network protocols and applications. Winstein and colleagues created the State Synchronization Protocol and the Mosh (mobile shell) tool for remote access over challenged networks, the Sprout algorithm for transporting video over cellular networks, which was awarded a 2014 Applied Networking Research Prize, and the Remy system, in which computers design network protocols from first principles. He received a B.S. and M.Eng. in electrical engineering and computer science, an E.E., and a Ph.D. from the Massachusetts Institute of Technology.