Secure Systems

Electrical & Computer Engineering

We live in the age of networked computer systems and big data. These technologies bring tremendous new benefits for business, personal growth, and communication, but also new opportunities for malice and attacks. The pace of attacks and sophistication of hackers is escalating. Today we must deal with security and privacy threats ranging criminals stealing personal information, to targeting government systems and surveillance. Security and privacy is not just about thwarting attackers: it is also about building trust. When computers and systems are secure and ensure privacy, new opportunities for communication and business arise.

ECE security faculty researchers collaborate to tackle ambitious goals; building trustworthy systems, automatically checking the world's software for exploitable bugs, developing new privacy-respecting and privacy-checking techniques, login without passwords, and designing the next generation secure internet. The fight against malware requires collaboration between software analysis and formal methods (what does this program do, is it good or bad?), advances in cryptography (who built the software?), privacy (is the developer trustworthy?), network security (where did I download it from?), and even economics (can we discourage malware authors?). In addition to academic collaborations, security faculty maintain strong relationships with businesses as well as government and non-profit agencies that can impact policy and large-scale social welfare.

ECE offers one of the most extensive computer security curricula in the world, with courses including cryptography, software security, network security, and human factors at the undergraduate, graduate, and Ph.D. levels. Our faculty also support outreach programs, such as running the world's largest computer security competition for high-school students and the top ranked computer security contest competition team.

Electrical & Computer ENGINEERING

Carnegie Mellon University
5000 Forbes Avenue | Pittsburgh, PA 15213 | www.ece.cmu.edu

ECE expertise

ECE is home to CyLab, one of the world's premier cyber security centers. CyLab takes a unique cross-disciplinary approach to security, involving over 50 faculty members, 100 graduate students, and a consortium of over a dozen industry partners in a multi-disciplinary, cross cutting approach to security. *Contact: Virgil Gligor.*

Trusted systems

The traditional notion of system trustworthiness has been based exclusively on a system's provable security properties. This led to systems that are, at best, serving niche application areas and markets, such as defense and aerospace. In contrast, our research adds provable security properties to commodity operating systems and applications, and allows users to verify that those properties are present at all times; e.g., have malware-free components at all times. We aim to preserve the rapid innovation taking place in the commodity systems market while adding tailored security properties as needed. Our research has introduced new security notions such as software attestation, verifiable boot, and user-verifiable trusted path from remote systems to users. *Contact: Virgil Gligor.*

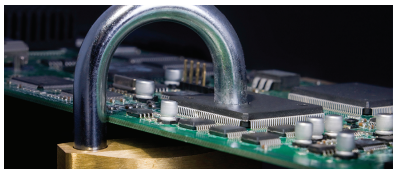
Software security

Attackers often break into systems by exploiting security-critical bugs. Unfortunately, bugs are plentiful, and typical program analysis does not tell us which bugs are security-critical, and which are mundane. Our research emphasizes formal methods that provide provable guarantees, with applications such as checking the world's software for exploitable bugs. *Contact: David Brumley.*

Network security

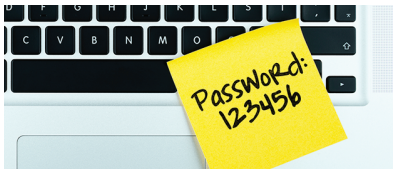
As networked applications and new killer apps emerge (e.g., mobile computing, Internet-of-Things), network security plays an increasingly critical role in securing critical infrastructures. Our researchers are working to develop systematic defenses against unforeseen attack vectors; e.g., non-traditional and near-terabit scale attacks against critical infrastructures. We also rethink traditional network security architectures via network virtualization, software-defined networking, and cloud computing. *Contact: Vyas Sekar.*

Privacy



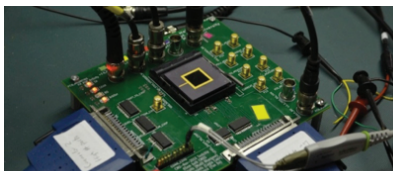
Privacy has become a significant concern in modern society as personal information about individuals is increasingly collected, used, and shared, often using digital technologies, by a wide range of organizations. ECE faculty have played a pivotal role in developing the research area of Privacy through Accountability by designing computational tools that can check audit logs and software systems operating on big data for compliance with formally stated privacy expectations, regulations, and organizational policies. These tools have been applied to address significant healthcare and Web privacy problems, including the first complete logical formalization of the HIPAA Privacy Rule. *Contact: Anupam Datta.*

Human factors



A system is unlikely to be secure if it does not take into account its users. For example, users write down passwords if they are required to be too long and complex and routinely don't notice security indicators that warn them of insecure websites. We focus on understanding the security and privacy needs, requirements, and attitudes of both lay-users and experts, and we research how to build systems that acknowledge human limitations and yet meet the security goals of both their designers and their users. Socio-economic factors also play a large role in determining which attacks are most likely to occur (as a large number of online nuisances are motivated by economic profit), and which security mechanisms are likeliest to be deployed. Our research combines modeling efforts of complex ecosystems influenced by the incentives of both attackers and targets, as well as designing systems that are compatible with these incentives. *Contact: Lujo Bauer, Nicolas Christin.*

Hardware security



At the lowest level of all electronic systems is the hardware itself. Hardware security considers a range of design decisions to improve security, spanning the manufacturing process and supply chain, circuit and system design, and the computer architecture exposed to programs. ECE research considers each level of the hardware, the interaction between levels, and the overall system. For example, faculty research looks at how to ensure secure manufacturing of integrated circuits using split manufacturing and anti-counterfeiting techniques. We also investigate novel and efficient secure circuit primitives, such as hardware random number generators and physically unclonable functions. At the architecture level, we consider crypto-processors, hardware roots-of-trust, memory and storage safety, as well as methods for securing these blocks against invasive and non-invasive attack. ECE actively pursues technology transfer in application domains ranging from the home user to safety-critical applications like SCADA infrastructure and medical devices. *Contact: Ken Mai*