About

Modern society is arguably increasingly reliant on ubiquitous information technology. Networked digital devices are the substrate of what is known as the Internet of Things where they play a critical role for healthcare, banking, commerce, entertainment and manufacturing to name just a few. Citizens, public and private organizations have all come to depend on digital services that directly impact their lives, even their very existence.

Yet, this critical medium is constantly subjected to attacks meant to steal private and personal information, intellectual property, trade secrets, financial records or even voter databases.

The purpose of the Connecticut Cybersecurity Center (C3) and its member centers is to break new technology grounds and advance the state-of-the-art with novel solutions to prevent, detect and cope with the plethora of attacks that threaten information technology systems holding our data. The Comcast Center of Excellence for Security Innovation focuses on networking products deployed in businesses and homes; the Center for Hardware and Embedded Systems Security and Trust (CHEST) is an industry-supported consortium tackling research issues in hardware security; the Synchrony center addresses threats to financial organizations and the Center for Voting Technology Research (VoTeR) supports the State of CT to ensure the safety of elections conducted with electronic terminals.

Areas of Expertise

- Security assessment of IoT and embedded devices such as routers, gateways, switches, VPNs, home security solutions, etc.
- Secure networking protocols expertise such as secure BGP or secure DNS
- Biometrics and key extraction
- Hardware root of trust and Physically Unclonable Functions (PUFs)
- Counterfeit electronics detection and prevention and supply chain risk management
- Anti-tampering and anti-reverse engineering
- Secure processor architectures
- Machine learning approaches to cybersecurity
- Formal techniques for security verification and validation
- Cryptography and coping with Kleptography
- Cryptographic attacks, side-channel attacks and defensive measures.
- Safely outsourcing computation to the cloud
- Multi-party computation

Center Characteristics

Overview

C3 and its member centers, Comcast CSI, CHEST, Synchrony and Voter carry out research in cybersecurity and cryptography. Their mission is to expand theoretical models and the boundary of cybersecurity technology to enable organizations to protect and safe keep the digital assets under their purview as well as enable safe, private, reliable and trustworthy computing in adversarial settings. Cybersecurity activity has been ongoing since 2006 within the VoTeR center that is devoted to securing the electoral process in the State of Connecticut. The Comcast CSI center, created in 2014, and CHEST center, created in 2017, have a track record in hardware security and, more specifically, IoT. CSI marks the engagement with a major network: Comcast.

Unique Capabilities

The centers benefit from a diverse faculty group with expertise in hardware, networking, software and system security allowing them to approach a broad range of challenges that require interdisciplinary collaboration delivering innovative approaches which, for instance, delivered novel ways to secure the supply-chain of electronic devices via PUFs and RFID technology. The holistic approach espoused by CSI for penetration testing is one of a kind and was pivotal to identify subtle vulnerabilities and neutralize critical threats early on during the development cycle. The systematic use of black-box in-depth testing within the VoTeR center is equally instrumental in exposing critical vulnerabilities that disqualified dangerous voting system terminals. In addition, C3 hosts an annual conference (CyberSEED) focused on the latest advances in hardware, system, and enterprise security along with hosting three cybersecurity competitions with nationwide participation.

Forging ahead

Adversaries are ever-changing chameleons, masters of disguises, and skillful technicians with a single purpose to infiltrate, capture and exploit critical information. Staying ahead of this threat maelstrom is a constantly evolving challenge that must be met. The centers are meant to offer to agencies, industries and the public at large, the necessary education, awareness and transparent technology they need to continue to operate effectively in such adversarial environments. Usable, measurable and impactful progress mandate foresight as well as a solid grounding in reality, both of which squarely rest at the core of the centers' mission.

Contact

Connecticut Cybersecurity Center

John Chandy, Ph.D.
Co-Director of C3
Phone: (860) 486-5047
Email: john.chandy@uconn.edu

Laurent Michel, Ph.D.
Co-Director of C3
Phone: (860) 486-2584
Email: ldm@uconn.edu

Innovation Partnership Building (IPB)

S. Pamir Alpay, Ph.D.
Executive Director of IPB | UConn Tech Park
Phone: (860) 486-6917
Email: pamir.alpay@uconn.edu

01/2020-HB

UCONN
INNOVATION PARTNERSHIP BUILDING

techpark.uconn.edu