UCONN | UNIVERSITY OF CONNECTICUT

Commerce Committee
February 26, 2015

Testimony

By
Dr. Kazem Kazerounian
Dean, School of Engineering
University of Connecticut

Chairman Hartley, Chairman Perone, and Ranking Members Scott and Camillo, and distinguished members of the Commerce Committee. My name is Kazem Kazerounian and I am the Dean of the School of Engineering at the University of Connecticut. ***I urge all committee members to support Senate Bill 835, An Act Concerning Cybersecurity.***

According to the FBI, in 2013 Connecticut state officials received more than 400 reports of security breaches that compromised the information of more than half a million residents. Such attacks pose serious risks to our civil and government infrastructure, utilities, businesses, and consumers. Recent cyberattacks on businesses such as Target, Home Depot and Anthem underscore the need for strong cyber defenses and public-private collaborations. Connecticut has much at stake. Our economy depends on vital industries – medicine, defense, communication, and insurance, among others – for which data security and privacy are of utmost importance.

Supported by partnerships with industry and government, UConn's School of Engineering has responded to these challenges. In the past three years we established two major centers to combat urgent cybersecurity threats. The UConn Tech Park, made possible by the General Assembly, played a major role in establishing these cybersecurity initiatives.

The Center for Hardware Assurance, Security and Engineering (CHASE) was established in 2012 to bring together commercial, academic and government expertise to enhance the nation's hardware assurance and security. Hardware assurance involves ensuring that our electronics hardware—from smartphones and personal computers to control systems for military hardware and business and government computer systems—are free from counterfeit parts and have not been tampered with.

Counterfeit hardware is a problem that has grown exponentially in recent years, having risen by a factor of nearly 700 over the last decade. Last November, Michigan Senator Carl Levin testified to the US Senate Committee on Armed Services that a study of "suspected counterfeit parts over a 2-year period…reported 1,800 cases covering a total of 1 million individual parts." 70% of these came from China. One estimate states that nearly 15% of all spare and replacement parts purchased by the Department of Defense are counterfeit.

CHASE is developing effective, lower-cost counterfeit detection technologies. We are improving hardware security and developing a system to continuously monitor counterfeiting trends, test techniques, and security attacks. The U.S. Department of Defense, National Science Foundation, and industry leaders such as Honeywell, Freescale Semiconductor, Qualcomm, and CISCO are among CHASE's as sponsors.

In 2013, UConn forged a partnership with Comcast, the nation's largest cable and Internet provider, to create **the Center of Excellence for Security Innovation (CSI)**, a cybersecurity research program that develops protections against Internet attacks and information breaches. Uniting the expertise of UConn's researchers with Comcast's leadership in Internet systems security has made the Center a national authority on hardware, software and network security. CSI is developing robust detection systems to shield Internet broadband systems from malicious attacks, unauthorized access, and counterfeit products. CSI shows how academic-industry partnerships can advance knowledge and create a new generation of highly-skilled workers, and it can serve as a model for others in the cybersecurity field.

In addition to the outstanding research from CHASE and CSI, we have held a number of public informational forums on cybersecurity, featuring such speakers as Rear Admiral David Simpson, Chief of FCC's Public Safety and Homeland Security Bureau; and Cheri Caddy, director of cybersecurity policy integration and outreach at the White House. We also held the very successful CyberSEED conference, a three-day event featuring expert talks and a hacking competition with teams from 43 universities. Such efforts have led the National Security Agency and the Department of Homeland Security to designate UConn as an NSA/DHS National Center of Academic Excellence in Information Assurance and Cyber Defense.

Education and workforce training is key. Without committed, highly qualified workforce, our battle for cybersecurity cannot be won. On Tuesday, at UConn's distinguished lecture and panel discussion on Cybersecurity, Liam Randall, CEO of Critical Stack, a cybersecurity firm, emphasized that what we need is "people, people, people . . . we need more smart people" who can fight cyber crime and secure our computing infrastructure.

Bills such as SB 835 are critical, then, for establishing the programs needed to train our next generation cybersecurity workforce. We must bring together academia, industry and government to advance the field of cybersecurity and to train the next generation of information technology, engineering, computer science, and management professionals who are capable of addressing our cyberinfrastructure vulnerabilities..

Public-private partnerships are prerequisite to any meaningful initiative toward a more secure digital world and UConn's School of Engineering looks forward to continuing to build partnerships to protect our State and residents. This bill would make a valuable contribution to our nation's security and economy.

Please support SB 835.

Thank you for the opportunity to testify and for your continued support of the University of Connecticut.

UConn Engineering Cyber Security Initiatives

UConn's School of Engineering has two independent centers focused on computer security: The Center for Hardware Assurance, Security and Engineering (**CHASE**) and the Comcast Center of Excellence for Security Innovation (**CSI**). These centers receive significant private sector and federal funding to conduct research, technology development, and education and workforce training. An engaged and committed industry sponsor base ensures efficient implementation of enhancements and improvements to corporate computer infrastructure and Internet security and increases UConn's capacity for sponsored research of interest to government and industry.

CSI and CHASE work with the School of Engineering on a number of educational initiatives, including courses on Information and Data Security, Computer Security, Modern Cryptography, Information Security Law and Policy, and Information Security Risk Management. In addition, CHASE and CSI support innovative courses and certificate and degree programs for continuing education, and facilitate technology transfer to industry.

CHASE https://www.chase.uconn.edu/

The Center for Hardware Assurance, Security and Engineering (CHASE) unites commercial, academic and government expertise to enhance the nation's hardware assurance and security. CHASE develops robust, secure, and trustworthy hardware technologies, design and detection techniques, tools and policies to provide unprecedented assurance in modern integrated circuits and systems. The Center houses $3 million in high-end analysis and research equipment and provides the physical and intellectual environment necessary to conduct interdisciplinary hardware-oriented research and address challenges in the field of assurance and security.

CHASE is creating more effective counterfeit detection systems at a lower cost and developing a system to continuously monitor counterfeiting trends, test techniques, and security attacks. The resulting hardware will reinforce the reliability, trustworthiness, security and economic value of computing, communication and networking technologies. CHASE also leads an initiative funded by a $7.5 million DoD grant that analyzes and upgrades security protections for nanoscale computer hardware.

Corporate and government sponsors interact closely with faculty and have access to CHASE's publications, reports, software, hardware, data, and much of the CHASE central laboratory equipment. Corporate members work with graduate and undergraduate students and recruit them as both interns and employees. These mechanisms ensure effective transition of new technologies to corporate and government users, with broad implications for society.

Corporate sponsors include: Agilent Technologies, Cisco, Freescale Semiconductor, Honeywell, Texas Instruments, Qualcomm ,Samsung, Juniper Networks, Synokey, LSI, Mentor Graphics, Verigy, R3 Logic, SRC, TSMC, GRC, MediaTek, Xilinx and Comcast,.

Government sponsors include: DoD, AFOSR, NSA, DoE, DARPA, AFRL, NSF, and ONR

CSI - http://www.csi.uconn.edu/

The Comcast Center of Excellence for Security Innovation (CSI) conducts cybersecurity research that develops protections against Internet attacks and information breaches. CSI is developing robust detection systems to shield Internet broadband systems from malicious attacks, unauthorized access, and counterfeit products.

CSI unites the expertise of UConn's researchers with Comcast's leadership in Internet systems security to make the Center a national authority on hardware, software and network security. CSI's academic-industry partnership advances knowledge, creates a new generation of highly-skilled workers, and serves as a model for others in the cybersecurity field.

CSI recently hosted CyberSEED (http://www.csi.uconn.edu/cybersecurity-week), a very successful three-day conference that featured expert talks and a hacking competition with teams from 43 universities. Through programs such as CyberSEED, CSI attracts new pool of talented students excited about cutting-edge industry challenges and develops unique workforce by early identification of exceptional students to be trained in various domains of security.