National Effort Joins Forces to Build a Secure Smart Home

Research focuses on strengthening trust around the household 'Internet of Things'

Hanover, N.H. – June 12, 2020 – A team of seven academic institutions will work together on a national research project to increase the security and privacy of high-tech products used in smart homes. The five-year program to develop trustworthy devices and systems in the home is funded by the National Science Foundation (NSF).

The project—Security and Privacy in the Lifecycle of IoT for Consumer Environments (SPLICE)—comes as households expand their reliance on smart products ranging from refrigerators to baby monitors. These devices can share information with each other as well as communicate with services across the internet.

SPLICE includes teams from Dartmouth College, the University of Illinois at Urbana-Champaign, Johns Hopkins University, the University of Maryland, the University of Michigan, Morgan State University, and Tufts University.

"The technology in the average home today is radically different from even a decade ago and is likely to change even more rapidly in the coming years," said David Kotz, a professor of computer science at Dartmouth and the lead principal investigator for the project. "Home is a place where people need to feel safe from prying eyes. SPLICE will address the challenges required for the vision of smart homes to be realized safely and successfully."

The shift toward smart devices and systems in residences—such as houses, apartments, hotels, and assisted-living facilities—offers benefits that include increased energy efficiency and personalized services. Through faulty configuration or poor design, however, these items can also create unsafe conditions and increase risk of harm to people and property.

Since many homes are complex environments in which residents, landlords, and guests have different privacy needs, researchers will consider the interests of all property owners and users.

"Cybersecurity is one of the most significant economic and national security challenges facing our nation today," said Nina Amla, lead program director of NSF's Secure and Trustworthy Cyberspace program. "NSF's investments in foundational research will transform our capacity to secure personal privacy, financial assets, and national interests."

--- MORE --

The program will develop technology and design principles related to smart homes. Breakthrough solutions envisioned for the program include:

- the first-ever toolkit to discover, identify, and locate cooperative and non-cooperative smart devices within a home's wireless network – allowing residents to have a complete understanding of their home's technological environment;
- tools that move away from the failed "notice and consent" model of privacy management – shifting the privacy burden away from end users, who are ill-equipped to manage an increase in the number of devices and decisions;
- identification of privacy issues in smart homes that must be addressed to advance consumer trust – informing the development of best-practice principles for smart homes.

Ten faculty experts will manage teams conducting research related to security, privacy, sociology, human-computer interface design, ubiquitous and mobile computing, embedded systems, wireless networks, and radio engineering.

As the lead institution for the $10 million project award, Dartmouth organized the program team and will coordinate its research and educational activities. More than half of the principal investigators leading SPLICE are from groups underrepresented in computing.

An advisory council composed of experts from government, industry and academia will provide guidance on current practice and future challenges.

"By working with a diverse group of leaders in the technology sector, we hope to influence the future of smart-home devices from design to disposal," said Kotz. "This is a win for consumers and for companies who want to make more privacy-respectful choices but feel they cannot do so while remaining competitive in the current market."

The research team will develop prototypes that integrate new insights emerging from the project while allowing them to seek feedback from experts and everyday consumers.

The group will also develop programs for students, junior researchers, and community members with the aim of encouraging more people from underrepresented groups to pursue careers in computing.

SPLICE is funded by NSF's Secure and Trustworthy Cyberspace Frontiers (SaTC Frontiers), a cross-cutting program to address fundamental scientific challenges related to privacy and cybersecurity.

The research program will begin on October 1, 2020. For more information and to follow SPLICE's progress, individuals can access the project blog at splice-project.org.

###

Notes for Editors:
Link to SPLICE project site: https://splice-project.org

Project Leadership Team

Dartmouth College
Lead Principal Investigator: David Kotz
Principal Investigator: Tim Pierson
Media Contact - David Hirsch: david.s.hirsch@dartmouth.edu

National Science Foundation
Program Manager: Nina Amla
Media Contact - Robert Margetta: rmargett@nsf.gov

University of Illinois at Urbana-Champaign
Principal Investigator: Adam Bates
Principal Investigator: Carl Gunter
Media Contact - Colin Robertson: colinr@illinois.edu

Johns Hopkins University
Principal Investigator: Avi Rubin
Media Contact - Doug Donovan: dougdonovan@jhu.edu

University of Maryland
Principal Investigator: Michelle Mazurek
Media Contact - Abby Robinson: abbyr@umd.edu

University of Michigan
Principal Investigator: Denise Anthony
Media Contact - Nardy Baeza Bickel: nbbickel@umich.edu

Morgan State University
Principal Investigator: Kevin Kornegay
Principal Investigator: Michel Kornegay
Media Contact - Larry Jones: larry.jones@morgan.edu

Tufts University
Principal Investigator: Susan Landau
Media Contact - Kalimah Knight: kalimah.knight@tufts.edu

Goodman Research Group (Contractor)
Project and Media Contact- Colleen Manning: manning@grginc.com