SPLICE: Security and Privacy in the Lifecycle of IoT for Consumer Environments

The Internet of Things now involves the deployment of Smart Things in everyday residential environments – houses, apartments, hotels, senior-living facilities – resulting in Smart Homes.

How does IoT technology in the home create **novel security and privacy risks**, and how do these risks vary across **complex stakeholder relationships**?

Our research agenda allows the team to **synergistically address cross-cutting challenges** & fold discoveries from one research thread into solutions in another.

comparison of differing security and privacy attitudes

recurring authentication scheme for device-to-device authentication

methods for discovering, identifying, authenticating, and classifying IoT devices in the smart-home context

The "lifecycle" of Smart Things:

methods to leverage trusted hardware in embedded IoT platforms

methods for secure third-party security analytics

Select innovations as they relate to the lifecycle

Our BPC Goals: Create diverse learning communities and groups, opportunities for female and URM students to participate, training and professional development activities

Our Advisory Council spans academia, government, and industry, helping bring our research insights into practice.

Follow us at splice-project.org
Find our papers on Zotero

SaTC Frontier 2020-2025: CNS-1955805, -1955172, -1955228, -1955231

Denise Anthony[1], Adam Bates[2], Carl Gunter[2], Kevin Kornegay[3], Michel Kornegay[3], David Kotz (lead)[4], Susan Landau[5], Michelle Mazurek[6], Tim Pierson[4], Avi Rubin,[7]

[1]University of Michigan, [2]University of Illinois, [3] Morgan State University, [4]Dartmouth College, [5]Tufts University, [6]University of Maryland, [7]Johns Hopkins University