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

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

splice-project.org – Check out our website and follow our blog for project updates:

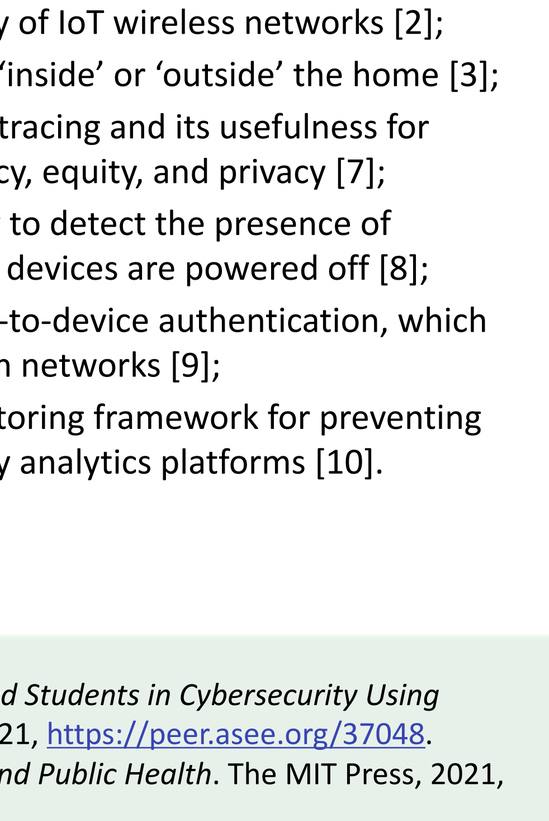
To watch a video presentation of this poster:

The Internet of Things (IoT) now involves the deployment of Smart Things in everyday residential environments – houses, apartments, hotels, senior-living facilities – resulting in **Smart Homes**. If not designed, deployed, configured, or managed as expected, these Things can create unsafe conditions and increase risk of harm to persons and property.

By examining the entire lifecycle of Smart Things, we take a **holistic, socio-technical approach** to protecting security and privacy in Smart Homes. We untangle the conflicting privacy, security, and economic needs of residents, owners, and vendors in order to **establish principles** for protecting the privacy and security of people who live in Smart Homes.

Key innovations and Contributions (selected):

- comparison of differing security and privacy attitudes,
- methods for discovering, identifying, authenticating, and classifying IoT devices in the smart-home context,
- methods for secure third-party security analytics,
- methods to leverage trusted hardware in embedded IoT platforms, and
- implementation of an "embedded" capture-the-flag competition in a graduate course – and the successes and barriers impacting the engagement of minority students in cybersecurity [6].

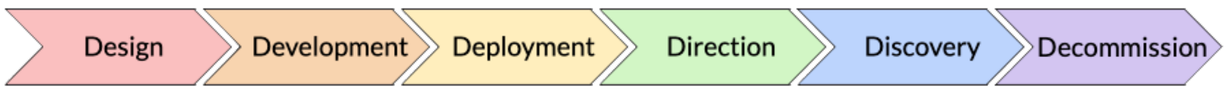


By focusing on the lifecycle of Smart Things – design, development, deployment, discovery, direction, and decommission – the SPLICE team addresses three fundamental scientific questions:

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

(B) How can we **leverage technology** to support the privacy and security of all users throughout the lifecycle of Smart Homes?

(C) What **practices and policies** will lead to manageable systems that enable users to live in a trustworthy digital environment while enjoying the benefits of a Smart Home?



These questions are particularly challenging for residences involving stakeholders -- owners, renters, management -- who have conflicting interests, resources, intentions and preferences.

Team publications thus far include:

- a study of systematic differences in the privacy and security knowledge or preferences of users who select one of the major platforms (Android or iOS) [1]
- an energy-efficient beamforming and direction-of-arrival estimation scheme, whose narrower beams may improve security of IoT wireless networks [2];
- a method for classifying IoT devices as being 'inside' or 'outside' the home [3];
- an introduction to the technology of contact tracing and its usefulness for public health, considering questions of efficacy, equity, and privacy [7];
- a new way to use harmonic-radar technology to detect the presence of electronic devices in homes – even when the devices are powered off [8];
- a recurring authentication scheme for device-to-device authentication, which may help detect spoofing attacks in Bluetooth networks [9];
- SCIFFS, an automated information flow monitoring framework for preventing sensitive data exposure in third-party security analytics platforms [10].

[1] Abrokwa, Desiree, et al. "Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms." *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, USENIX Association, 2021, pp. 139–58, https://www.usenix.org/conference/soups2021/presentation/abrokwa.

[2] Belay, Hailu, et al. "Energy Efficiency Analysis of RLS-MUSIC Based Smart Antenna System for 5G Network." *Conference on Information Sciences and Systems (CISS)*, IEEE, 2021, https://doi.org/10.1109/CISS50987.2021.9400325.

[3] Gralla, Paul. *An inside vs. Outside Classification System for Wi-Fi IoT Devices*. Dartmouth College, 4 June 2021, https://digitalcommons.dartmouth.edu/senior_theses/215/.

[4] Jois, Tushar, et al. *WDPKR: Wireless Device Profiling Kit and Reconnaissance*. 2021, https://par.nsf.gov/servlets/purl/10283800.

[5] Kornegay, Kevin, and Willie Lee Thompson II. *Decentralized Root-of-Trust Framework for Heterogeneous Networks*. Morgan State University, 2020, https://patents.google.com/patent/US20180196945A1/en.

[6] Kornegay, Michel A., et al. *Engaging Underrepresented Students in Cybersecurity Using Capture-the-Flag(CTF) Competitions (Experience)*. 2021, https://peer.asee.org/37048.

[7] Landau, Susan. *People Count: Contact-Tracing Apps and Public Health*. The MIT Press, 2021, https://mitpress.mit.edu/books/people-count.

[8] Perez, Beatrice, et al. "Detecting the Presence of Electronic Devices in Smart Homes Using Harmonic Radar Technology." *MDPI Remote Sensing*, vol. 14, no. 2, Jan. 2022, https://doi.org/10.3390/rs14020327.

[9] Peters, Travis, et al. "Recurring Verification of Interaction Authenticity Within Bluetooth Networks." *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ACM, 2021, pp. 192–203, https://doi.org/10.1145/3448300.3468287.

[10] Polinsky, Isaac, et al. "SCIFFS: Enabling Secure Third-Party Security Analytics Using Serverless Computing." *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, ACM, 2021, pp. 175–86, https://doi.org/10.1145/3450569.3463567.

Broader Impacts:

Through **work with standards-development organizations and industry leaders** on our Advisory Council, our research insights will help establish a consumer-focused ecosystem for secure and privacy-protective IoT. The council provides a direct path for technology transfer to vendors like Amazon, Apple, Arm, Google, IBM, Intel, and Microsoft, and an indirect path for much broader influence through NIST, UL, and Consumer Reports. NIST and other agencies often call upon us to advise about policy relevant to security and privacy technology. Furthermore, several of our PIs often testify before government bodies – including the US House and Senate – on technology issues related to our research.

Education and Outreach:

- We have engaged undergraduate students in research through REU supplements, the ASURE program at Dartmouth, and more
- SPLICE students have attended various research-focused conferences and trainings
- SPLICE students have an opportunity to engage in cross-institutional exchanges
- Team professional development sessions
- PIs Gunter and Kotz each built a new course around SPLICE themes
- At a public SPLICE panel "Privacy Implications for the Internet of Things," a high-school teacher asked for advice to bring back to their students, regarding security and privacy in Smart Homes

Broadening Participation:

- SPLICE and ProperData hosted a joint workshop: *Why IoT's Even Harder: Policy, Legal, and National Security Issues for Ubiquitously Connected Devices* with 74 total participants
- Six SPLICE team members have graduated on to roles at Mastercard, Palantir, Qualcomm, Appian, and Riverside Research
- All SPLICE grad students and postdocs have secondary mentors at different SPLICE institutions
- SPLICE faculty hosted 2-week summer camp for middle-school girls, at Morgan State
- Incoming undergrads: the SPLICE team supports a summer bridge program at Morgan State