SaTC: Frontiers: Collaborative:
Security and Privacy in the Lifecycle of IoT for Consumer Environments (SPLICE)

David Kotz (Dartmouth); with **Denise Anthony** (U.Mich), **Adam Bates** and **Carl Gunter** (U.Illinois), **Kevin Kornegay** and **Michel Kornegay** (Morgan State), **Susan Landau** (Tufts), **Michelle Mazurek** (U.Maryland), **Timothy Pierson** (Dartmouth), **Avi Rubin** (Johns Hopkins)

SaTC Frontiers award numbers 1955805, 1955172, 1955228, and 1955231, starting 1 October 2020.

Some of the problems SPLICE addressed:

Smart-home security, privacy, and complex social dynamics — Homes may soon contain hundreds of heterogeneous devices with multiple stakeholders (residents, landlords, tenants, technicians), creating conflicting requirements ("tussles") among safety, security, privacy, usability, and controllability. Significance: unresolved conflicts risk unsafe, unfair, or privacy-violating outcomes.

Confidential computing on edge devices — LLM agents and edge deployments must protect proprietary assets and runtime state on untrusted hardware (like Arm CCA). Significance: enables privacy-preserving, low-latency AI without ceding sensitive data to the cloud.

Poor quality of security/privacy advice and configuration — End users and even developers rely on contradictory, unvetted guidance, and manual privacy configuration is burdensome. Significance: better, automated, and usable advice/configuration is needed to achieve real-world security outcomes.

Underrepresentation in cybersecurity/STEM education — Limited diversity and few effective training pathways in the field. Significance: broadening participation is essential for building a workforce that designs technology serving all of society.

Examples of generalizable scientific impact:

Systematization-of-knowledge (SoK) contributions — SoKs on provenance auditing, mobile-device data confidentiality, and ultrasound/near-ultrasound protocol security establish taxonomies and open-problem roadmaps that seed and structure future research in adjacent domains.

Usable-security measurement instruments — Validated scales and interview-based methodologies (e.g., the Smartphone Security Behavioral Scale, studies of product reviewers and repair technicians) generalize to human-factors research across authentication, IoT, and organizational security.

RF/physical-layer sensing and detection — Harmonic-radar identification of electronic devices and secure short-range 'friendly-jamming' communication extend to hardware provenance, counter-surveillance, device authentication, and physical-layer security research.

Reproducible platforms and educational testbeds — Open-source reference platforms (medical-device security, application-driven IoT education, e-voting security engineering) generalize as reusable infrastructure and pedagogy for building rigor and workforce capacity across cybersecurity subfields.

Sample of technical approaches, key innovations, and new contributions:

Behavioral fingerprinting for Zero Trust IoT — Profiles IoT network traffic to build per-device fingerprints and dynamically modifies SDN switch flow tables, extending Zero Trust identity/access control to constrained IoT devices.

Characterizing Everyday Misuse of Smart Home Devices — explores how smart devices are misused (used without permission in a manner that causes harm) by device owners' everyday associates such as friends, family, and romantic partners, shedding light on the most prevalent security and privacy threats faced by smart homeowners.

Confidential edge agent execution (AgenTEE/CAEC) — Places agent runtime, inference engine, and third-party apps into independently attested confidential VMs on Arm CCA with efficient, secure shared-memory and minimal performance overhead.

Harmonic radar detection & classification — Extends nonlinear-junction detection to identify/classify electronic devices—and, newly, to detect batteries… *even when devices are powered off*.

Matter research enablement — A reproducible template for adding custom clusters to the open-source Matter SDK (e.g., a data-erase cluster) plus a network 'sniffer/AP' utility testbed for Matter experimentation and teaching.

Broader Impacts (on society):

Safer homes and everyday devices — More secure smart-home and IoT/embedded devices protect residents' safety and privacy.

Protected critical infrastructure — Stronger defenses for building-automation and OT networks guard essential services from cyber-physical attacks.

Patient safety — More secure medical devices reduce risk of harm to patients.

Individual privacy — Confidential computing, steganography, and side-channel defenses shield personal data from surveillance and misuse.

Education & training — A cohort of undergraduate and graduate students, and postdoctoral scholars, have been trained for industry and academia.

Broader impacts (on education):

Reproducible, hands-on security curricula — Open-source platforms and testbeds (medical devices, IoT, and Matter) enable consistent, practical teaching.

Engaged, real-world learning — CTF competitions, e-voting projects, and application-driven IoT courses build critical thinking and job-ready skills.

Broadening participation — Culturally responsive STEM programs increase interest and confidence among underrepresented students.

Public and pre-college outreach — Workshops for the general public and camps for schoolchildren raise security/privacy awareness beyond the university.

Pathways to advanced study — Programs that boost interest in graduate school and research.

Broadening participation in computing:

Reaching underrepresented students early — Camps like "Females are Cyber Stars" (FACS) engaged middle-school girls in cybersecurity.

Pathways to graduate school — One-day workshops at a Hispanic-Serving Institution increased underrepresented students' interest in CS&E graduate study.

Minority-serving research experiences — REU/RET and eCTF programs (e.g., at Morgan State) grow minority students' skills and research productivity.

Building a representative workforce — Collectively, these efforts widen the pipeline into industry and the professoriate.

SPLICE timeline: October 2020 – September 2026

Website & blog	splice-project.org/
Papers, theses (132)	www.zotero.org/groups/2647324/splice/library
Patents (13)	www.zotero.org/groups/2647324/splice/collections/QNJGKWIS/collection