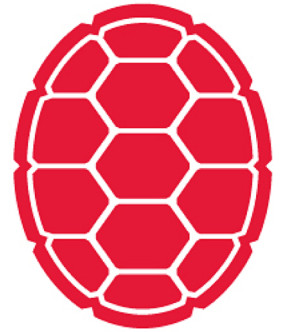

HUMAN-CENTERED SECURITY AND PRIVACY



MICHELLE MAZUREK

mmazurek@cs.umd.edu



WHY HUMAN-CENTERED?

[Follow](#)

Asking consumers to self-assess the privacy risks of digital products is like asking them to self-inspect their hamburgers for fecal contamination.

Most people now recognize the second proposition as an absurdity—but Silicon Valley did a good job selling “notice and consent.”

Crypto company can't access \$137M because dead owner didn't share passwords

BY JASON SILVERSTEIN

UPDATED ON: FEBRUARY 4, 2019 / 10:42 PM / CBS NEWS



WIDE OPEN —

Cryptography failure leads to easy hacking for PlayStation Classic

Plug-and-play hardware lacks even basic functional security for crucial bootrom.

KYLE ORLAND - 12/10/2018, 12:03 PM

OVERARCHING QUESTIONS

Why and how do people* make security- and privacy-relevant decisions?

How can we improve these decisions?

* End users, software developers, sysadmins, vulnerability analysts

TYPICAL APPROACHES

Surveys and interviews

Observational studies

Experiments

Designing and testing interventions (tools, systems, interfaces)

TRACKING TRANSPARENCY

Building tools to make tracking and targeted advertising visible and comprehensible to end users.

Understanding what kinds of tracking are appropriate, creepy, expected, surprising.

CHI 2018, WWW 2019

MAKING SECURE DEVELOPMENT EASIER

How do API design, documentation, and even Stack Overflow contribute to (in)secure development?

**How are tools and techniques designed to prevent vulnerabilities used in practice?
How can we make them more useful?**

**S&P 2016, 2017
CCS 2016**

EXAMINING THE SECURITY- ADVICE ECOSYSTEM

Where do end users get security advice?

**How do they evaluate what to apply and
what to ignore?**

What advice is currently available?

Is the advice readable, useful, correct?

Does this vary by source and topic?

**S&P 2016, CCS 2016
CHI 2017, EC 2018**

SUPPORTING VULNERABILITY ANALYSIS

How do reverse engineers and vulnerability analysts do their work? What makes them successful?

How can we build tools to support vulnerability discovery?

How does training and education contribute to success in vulnerability analysis?

MENTAL MODELS OF END-TO-END ENCRYPTION

How do end users value privacy and convenience in secure communications?

How can we correct misunderstandings that lead users to security errors?

**SOUPS 2016
EURO S&P 2018**