CAREER:
Identifying, quantifying, and explaining design principles and user practices that enable effective long-term key management

Scott Ruoti, University of Tennessee, Knoxville

https://userlab.utk.edu/projects/nsf-career-2023

Since *Why Johnny Can't Encrypt*, we've known that usable key management is critical to the success of cryptographic systems. 20+ years later, usable key management remains a largely unsolved problem.

Objectives

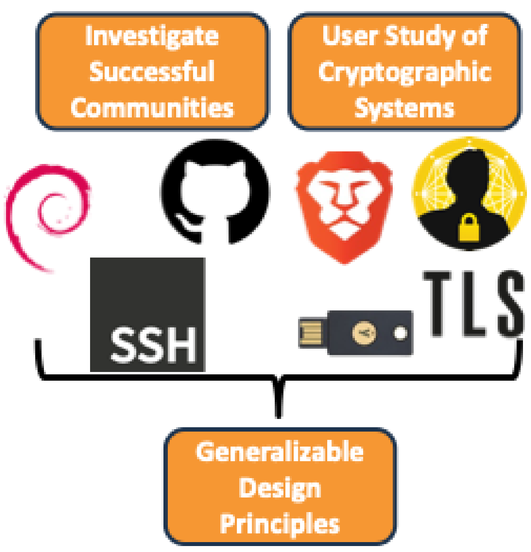
- Support the design of future cryptographic systems by providing a foundation of tried-and-true design principles and user practices that enable effective key management
- Identify specific impediments to persistent and universal key management that future research will need to address before users can turn over their data and lives to advanced cryptographic systems

Scientific Impact

- This research will identify the design principles and user practices that have enabled the adoption of cryptographic systems relying on long-term key management.
- This research will identify paint points that hinder the adoption of key management even for highly-technical users. Future research will be needed to address these pain points.

Approach

1. Investigate communities that successfully use cryptographic keys
   a. Measure key usage and management for these community
   b. Interview community members to understand best practices and software usage
2. Have senior- and graduate-level students adopt systems requiring key management
   a. Use over the course of a semester (i.e., long-term key management)
   b. Gather quantitative data and qualitative feedback about their experiences
3. Conduct user study examining multi-key management, synchronization, and recovery



Impact on Society

Improved key management will support the proliferation of advanced cryptographic systems that could revolutionize users' privacy and security. Examples included decentralized identity wallets, self-sovereign identity, cryptographically secured email, secure multi-party computation, cryptocurrency.

Impact on Education

I am working with Loan Oak Farms to create security and privacy curriculum for K–12 students, include 2–3 hands-on units for summer camps.

Results from this research have been integrated into units on key management, PKI, and usable security for an *Applied Cryptography* course

Impact on Students

This grant has supported 1 Ph.D. dissertation, 2 MS theses, and 2 REU. It is currently supporting 1 Ph.D. candidate and 2 REU.

Students come from a range of background, including traditionally underrepresented communities.

Video