Toward Critical Security and Cryptography

Ko (Natnatee) Dokmai,
Indiana University, Bloomington
Those who pursue a Science of Security should be cognizant of history—including that progress in science is neither steady nor straight-line. Simply wishing for a Science of Security will not make it happen. What is needed is for security researchers to learn and adopt more scientific methodologies.

Ontological and Epistemological Approach to Critical Security and Privacy

1. socio-political > technical
   ⇒ S&P needs to take into account the power relations

2. cultural > psychological
   ⇒ S&P research methodology needs to engage in cultural studies

3. situated knowledges > universal objectivity
   ⇒ S&P research needs to be contextualized and position-dependent
Toward
Critical Security and Cryptography

How?
The humans and infrastructures as an indispensable part of security and cryptography theoretical design

Theoretical foundations
Security and cryptography, Science and Technology Studies, Critical Geography

Methodological Framework
Ethnography, Grounded Theory

Humans

Physical Infrastructure

Theoretical Design

What are the meanings, practices, and power relations?

What technology is possible and practical?

How to design the most practical system?
Case Study: Trust networks in activism in Bloomington, Indiana

What technology has been used? What can be changed improved?

What needs a new design? Given what exists and is possible, what can we design?

Discussion

- Resilience over scalability
- Autonomy over centrality
- Speak to the community over academia/industry
- Scholar-activism: researchers need to engage in multiple disciplines and the community