SoK: Social Cybersecurity

Yuxi Wu
yuxiwu@gatech.edu
W. Keith Edwards
keith@cc.gatech.edu
Sauvik Das
sauvik@cmu.edu

Georgia Institute of Technology
Carnegie Mellon University

Originally published at IEEE S&P 2022

Many end-user cybersecurity and privacy (S&P) behaviors are inherently social: we share personal info in our social networks, ask friends and family for S&P advice, and negotiate with others to protect our privacy.

We analyze prior work in social cybersecurity and present a structuring of this literature based on its pertinence to four S&P-relevant social behaviors.

Methodology & Scoping

1

Gathering relevant prior work

Keyword searches for…
"human and societal aspects of security and privacy"
"social aspects of security and privacy"

Snowballing to include…
"social cybersecurity", "collaboration", "community", "couples", "intimate partner violence", "family", "households", "teenagers", "social networks", "workplace"

1000 articles from the last 5 years of…
CCS, CHI, CSCW, IEEE S&P, NDSS, PETS, SOUPS, TheWebConf, and USENIX Security + highly cited works from NSPW, UbiComp

"Does this work advance our knowledge of how social groups jointly navigate S&P decisions, behaviors, threats, or tools?

2

Identifying common themes among these papers

"Does this information advance our knowledge of how S&P threats, tools, or advice affects groups differently than individuals?"

Reflexive approach to thematic analysis

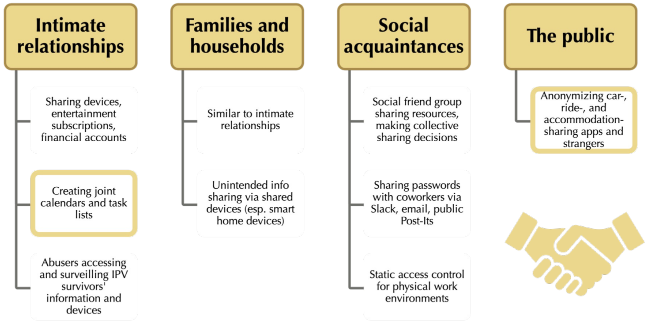
Iterative discussions to organize codes and generate categories

3

Grouping themes into taxonomically significant domains

4 Key Behavioral Domains in Social Cybersecurity Arranged by 4 Social Distances

Negotiating Access to Shared Resources



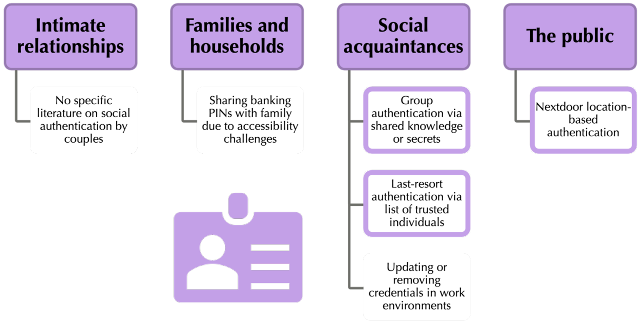
Intimate relationships
Sharing devices, entertainment subscriptions, financial accounts
Creating joint calendars and task lists
Abusers accessing and surveilling IPV survivors' information and devices

Families and households
Similar to intimate relationships
Unintended info sharing via shared devices (esp. smart home devices)

Social acquaintances
Social friend group sharing resources, making collective sharing decisions
Sharing passwords with coworkers via Slack, email, public Post-Its
Static access control for physical work environments

The public
Anonymizing car-, ride-, and accommodation-sharing apps and strangers

Shared and Social Authentication



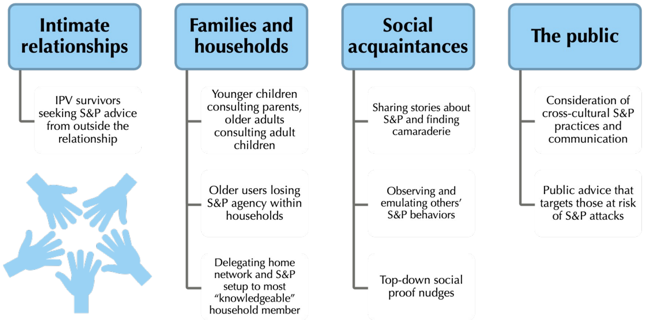
Intimate relationships
No specific literature on social authentication by couples

Families and households
Sharing banking PINs with family due to accessibility challenges

Social acquaintances
Group authentication via shared knowledge or secrets
Last-resort authentication via list of trusted individuals
Updating or removing credentials in work environments

The public
Nextdoor location-based authentication

Influencing Others' S&P Behaviors



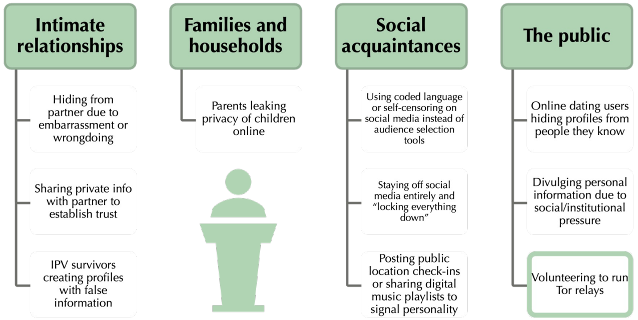
Intimate relationships
IPV survivors seeking S&P advice from outside the relationship

Families and households
Younger children consulting parents, older adults consulting adult children
Older users losing S&P agency within households
Delegating home network and S&P setup to most "knowledgeable" household member

Social acquaintances
Sharing stories about S&P and finding camaraderie
Observing and emulating others' S&P behaviors
Top-down social proof nudges

The public
Consideration of cross-cultural S&P practices and communication
Public advice that targets those at risk of S&P attacks

Managing Self-Presentation



Intimate relationships
Hiding from partner due to embarrassment or wrongdoing
Sharing private info with partner to establish trust
IPV survivors creating profiles with false information

Families and households
Parents leaking privacy of children online

Social acquaintances
Using coded language or self-censoring on social media instead of audience selection tools
Staying off social media entirely and "locking everything down"
Posting public location check-ins or sharing digital music playlists to signal personality

The public
Online dating users hiding profiles from people they know
Divulging personal information due to social/institutional pressure
Volunteering to run Tor relays

Identifying & evaluating the socio-technical gap in social cybersecurity work

Outlined behaviors in above diagrams answer "Yes" to these three questions and successfully navigate this gap

01

Are there existing systems that help facilitate this social use case?

- Majority of behaviors and use-cases involve *some* sort of technical system
- But there is a difference between…
  - extant systems that are worked around or modified to fit social needs
  - novel systems *designed to directly facilitate social behaviors*

02

Can users fit the affordances of existing S&P systems without altering their ideal social behaviors?

Many S&P systems are designed to be ignorant of social context, and force users to choose between security and social acceptability

03

Can users use these existing systems, as intended, to meet both their ideal social behaviors and S&P goals?

By failing to account for human social behaviors, many systems no longer serve their intended purpose, and S&P preferences fall by the wayside