SoK: Social Cybersecurity

Gigi-Alexandru Dobre 341C5
Politehnica University of Bucharest
Faculty of Automatic Control and Computer Science
gigi.dobre@stud.acs.upb.ro

***Abstract*—The chosen paper is mainly focused on the analysis of previous work carried out in the social cybersecurity field, pointing out four important security and privacy relevant behaviours. Furthermore, these four behaviours are looked at from the perspective of four types of social relations.**

***Index Terms*—intimate, personal, social, public**

I. Solution description

There are various end-user cybersecurity and privacy behaviours that are influenced by social factors. Many tools designed to improve security and privacy have focused on individual behaviours rather than considering the connections of people on the internet.

This has led to an interest in studying end-user security and privacy in a social context, also known as social cybersecurity. Four key behaviour domains in this area include:

- negotiating access to shared resources
- shared and social authentication
- managing self-presentation
- influencing others' security and privacy behaviours

A. Negotiating access to shared resources

The purpose of this subsection is to examine how people share access to digital services, physical devices, and physical spaces (eg. Netflix, banking, work).

Intimate partners commonly share a variety of digital devices and resources. These behaviours may change as trust and commitment in a relationship progress, also making the process of ending account sharing difficult and burdensome. There have been efforts to support the social practices of **families and households** through technical means, such as the Family Accounts model for shared user accounts. However, unintended sharing can still occur.

Resource sharing with **social acquaintances and coworkers** can often be hindered by patchwork policies and a lack of coordination. **Strangers** may be involved in a variety of relationships, such as renting an Airbnb or taking part in different ridesharing situations that require the negotiation and specification of access control for shared resources.

B. Shared and social authentication

This subsection aims to discuss about an alternative related to group authentication methods, as a way to solve the existing issue of password sharing and the cognitive burden it places on users, such as having to remember which passwords have been shared with others and updating them when necessary.

From the perspective of **intimate, family, and social acquaintance** relations, sharing resources and authentication information, such as passwords and PINs, is common. This practice aids in the unlocking of shared media resources, devices, and finances, as well as the development of trust in these relationships. However, few systems have been developed specifically to facilitate group or social authentication without the use of passwords. As a result, when more effective methods are unavailable, people may resort to informal password sharing practices and ultimately, if that is not possible, trust must be placed in authenticating authorities to verify identities at the **public** level.

C. Managing self-presentation

The main goal of this subsection is to define self-presentation. Managing self-presentation involves sharing information about oneself with social circles and most of the times, people's willingness to share information about themselves depends on the type of information and the recipient.

Regardless of the type of **social relations**, users must constantly balance the desire to share personal information with others in order to build trust and connections, while also maintaining their privacy. They try to carefully control how they present themselves online, but controlling all of the information about themselves can be difficult. Existing tools for restricting who can see what information are not always adequate. This can result in sensitive information being shared with unintended recipients. There is a need for systems that give users more control over who can access the personal information they share online.

D. Influencing others' security and privacy behaviours

The last subsection proves there is evidence that people are more likely to engage in positive behaviours related to privacy and security when they are influenced by social triggers, rather than being forced to do so.

Regarding **intimate relationships**, there is a need for systems that can assist professionals who work with survivors of domestic violence in order to compensate for the professionals' lack of knowledge in S&P. At the **household level**, parents frequently use a "lockdown" approach to protect less technically literate family members. There has been research on using social nudges and alerts to educate people about privacy and security at the **social acquaintance level**, but these approaches do not always consider the social and cultural context in which people make decisions about these issues.

Technical work at the **public** level has focused on developing systems that use social influence to encourage better privacy and security behaviours, such as showing people the decisions made by others on issues related to cookies and firewall settings.

II. Related work

A. Breaking! A Typology of Security and Privacy News and How It's Shared [2]

The work presented in this article is mainly focusing on the S&P topics that are taking the scene along with the evolution of technology and cybercrime, raising an interest in how you can protect yourself and how you can spread awareness.

To analyze these aspects, the authors conducted a survey that included twenty events with at least 1000 shares on social media amongst 100 participants for each one of them (1999 in total) on Amazon's Mechanical Turk platform. Out of all these responses, 729 had heard about at least one event, 664 had not heard about any event but provided a similar one and 606 had not heard about any event and also could not provide a similar one. They also provided details about where they heard this information from:

- online news articles - 70%
- television news - 36%
- social media - 29%
- another person 17%
- service provider 4%

B. The effect of social influence on security sensitivity pp.143–157 [3]

An interesting section of this paper talks about the part related to passwords from the interview that was conducted. It is pointing out that over 76% of the respondents are using passwords as their one and only way of security while navigating the internet.

Although this is their primary method, most of them change the password very rarely or not at all. Some of them even keep their passwords on the email or text messages.

”Respondent 4: I've never changed a password [. . .] It's off head.” (143)

”Interviewer: How do you stay safe on the Internet? Respondent: By keeping my information in my email and then locking it up with my password.” (143)

While this might seem very unsafe and prone to cyberattacks, it is a common practice among most people, regardless of their age.

C. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults [4]

The purpose of this study was to take a look at the security and privacy practices of adults in urban India. In most cases, people that are not experts in S&P act as guides or ”family tech managers”(11) for the elderly, imposing their knowledge and beliefs by creating different guidelines, protecting the older members of the family from cyberattacks.

This can lead to multiple problems, such as: breaches in their system, lack of knowledge and lack of motivation to learn about S&P practices and behaviours regarding the older adults. This paper strongly encourages the development of technology to support the management of security and privacy, as well as promoting education and empowerment for those involved.

D. ”We hold each other accountable”: Unpacking how social groups approach cybersecurity and privacy together [5]

This research paper aims to find out how the decisions regarding their jointed accounts (”e.g. friends sharing Netflix accounts, roommates sharing game consoles”(1)) are made by those groups of individuals that are sharing digital resources.

The approach was to form nine groups made out of thirty-four participants and observe their behaviour when it comes to shared devices. The study showed that they typically tend to rely on implicit agreement and individual accountability, and while making a jointed decision on how to handle the privacy, it seems that there are a lot of missed opportunities to improve their communication and S&P behaviours. It also suggests that there is a need of better cybersecurity and privacy controls to support such small groups.

E. To Self-Persuade or be Persuaded: Examining Interventions for Users' Privacy Setting Selection [6]

This study looked into how social groups influence people's security and privacy behaviours. Previous research, such as the original chosen paper, has shown that personal connections can effectively impact these behaviours, but it might be difficult to quantify.

Moreover, it discovered that expert and non-personal social groups had comparable levels of impact, and that people with strong collective identities were more likely to be swayed by non-personal social influence. According to the findings, future designs for S&P interfaces should consider using behavioural persuasion techniques that are based on groups to which individuals have no personal ties because of how promising they are.

References

[1] Yuxi Wu, W. Keith Edwards, Sauvik Das, ”SoK: Social Cybersecurity”, in *IEEE Security & Privacy (S&P)*, 2022, pp. 1-17

[2] S. Das, J. Lo, L. Dabbish, and J. I. Hong, ”Breaking! a typology of security and privacy news and how it's shared” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–12

[3] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, ”The effect of social influence on security sensitivity” in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 143–157

[4] S. Murthy, KS. Bhat, S. Das, N. Kumar, ”Individually vulnerable, collectively safe: The security and privacy practices of households with older adults” in *Proceedings of the ACM on Human-Computer Interaction 5 (CSCW1)*, 2021, pp. 1-24

[5] H. Watson, E. Moju-Igbene, A. Kumari, and S. Das, ””We hold each other accountable”: Unpacking how social groups approach cybersecurity and privacy together” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–12.

[6] I. Krsek, K. Wenzel, S. Das, JI. Hong, L. Dabbish, ”To Self-Persuade or be Persuaded: Examining Interventions for Users' Privacy Setting Selection” in *CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1-17