Human Interdependencies in Security Systems

Rick Wash
Michigan State University

Emilee Rader
Michigan State University

Human beings—users—are a central component of any sociotechnical system. Securing a system involves exercising some amount of control over it, through actions such as creating or modifying code, administering and enforcing policies, or making everyday computing decisions like whether or not to install an update. People are often the "weakest link" in terms of security, the component of the system that behaves most unpredictably and is hardest to secure [1].

Borders between systems exist where transitions of control and responsibility take place; for example, different groups are responsible for developing updates to specific apps than to an operating system. We believe that humans create interdependencies between systems that cross these boundaries—connections where insecurity in one system can cause an insecurity in another system—even when no technical relationship exists between the systems. These interdependencies can introduce vulnerabilities; however, with appropriate study and design, we believe it is possible to use these interdependencies to strengthen security rather than weaken it. Thus, we propose the grand challenge to help human users strengthen security by taking advantage of interdependencies between systems that they create.

Many systems interoperate at a technical level. This interoperation is commonly seen to create an interdependence in the security of the systems. For example, a web browser interoperates with DNS; an insecurity in DNS that allows an attacker to create unauthorized DNS entries will also allow the attacker to violate security guarantees in the web browser. This technical interdependence between systems is well known and much work goes into creating secure systems in the face of this interdependence.

Computing systems also have human users who must make numerous decisions about how to use them, and many of these decisions create opportunities for malicious actors. Rob Joyce, Chief of Tailored Access Operations at the US National Security Agency, recently spoke about how insecure user decisions provide more reliable access to systems than most technical attacks [2].

The are two common strategies for addressing the vulnerability that users create: remove the decision from users (when possible), and educate users [1]. Unfortunately, we cannot remove users from all decisions. And, education has some severe limits. We cannot train everyone in the inner workings of every computing system they interact with [5]; and even if we did, simply knowing how a system works is still not necessarily enough to ensure secure decisions. This relationship—that the security of a system depends on the decisions of its users—is well known, and "Human Factors" are already a major aspect the US Strategic Plan in CyberSecurity.

However, we believe that the biggest vulnerabilities, and the biggest opportunity for increasing security in sociotechnical systems, comes not from the direct relationship between technology and user, but from interdependencies created when many people each use multiple different systems across their lives. These interdependencies can be divided into two main categories: how one user creates interdependencies across the different systems that they use; and how multiple users of the same system can influence each other.

One User, Many Systems Each person does not use only a single computing system; he or she uses a wide network of different systems, many of which are not technically interconnected. For example, a typical person does not have a single password on a single website; instead, he or she likely has passwords on tens or hundreds of websites. These websites generally do not technically interoperate. However, their security is linked through decisions made by their users. In a recent study, we found that users are most likely to re-use a password if it is complex (high entropy) and if the person is required to enter it frequently [6]. Thus, a website with a strong password policy and a short login timeout may actually be less secure because those security policies lead users to re-use its password on other, less secure websites.

Another example of people using multiple systems involves software updates. When iTunes 11 was released, it was distributed as a software update, using the same update distribution system that distributes minor patches and security updates. It also dramatically changed the user interface of the software. We encountered a number of people who felt betrayed (e.g., "I couldn't find my music") and thus decided to not install any more updates [4]. They often did not distinguish between security updates and functionality updates. And this decision was not always limited to just iTunes; some people stopped installing updates on other, more critical software also, after experiencing what they perceived to be negative consequences due to the iTunes update.

One System, Many Users Humans are social creatures. People naturally talk with each other often about their experiences, and this includes topics such as how they use their computers and challenges or problems they face when using technology. We collected hundreds of stories that people had been told about security issues, mostly from family and friends. Approximately 72% of our participants reported that these stories contained "lessons" that they can learn from [3].

These stories, and the lessons that they contain, create an interdependence across people. As multiple people use the same system, they talk to each other and can learn from each other. Some of our participants learned to "buy Macs because people can't get into them" or "to not give away passwords!". While some lessons are concrete (e.g., "Don't click on links on Facebook"), others can be vague and difficult to put into action (e.g., "be very careful about information I post online") [3]. Thus, both secure and insecure decisions can spread across people.

The Grand Challenge Humans do not only create vulnerabilities in the specific system in use. The two interdependencies identified above mean that vulnerabilities can be opened across systems used by a given user, or in a given system used by many users sharing information with each other. However, this interdependency also provides an opportunity: good, secure decisions can spread through users and across systems also.

Thus, we propose a grand challenge to find ways to utilize the interdependencies created by users across system boundaries to amplify security rather than to weaken it. How might a secure system be designed to help users learn to make better security decisions on other, related systems? What approach might we develop to take advantage of the natural storytelling of users to spread beneficial security practices? Can technologies be designed that help users to help each other? What organizational or governmental policies might encourage or discourage these interdependencies?

Solving this challenge will require fundamental advances in the social scientific understanding of how people share security practices, how people learn about security, and how they generalize that learning to the use of other systems. It will require sociotechnical advances in how to design computing systems that are not only secure when used correctly, but also help users learn how to use them securely, that demonstrate to users how that learning can be used on other systems, and that both encourage users to share their knowledge with other users and account for learning across system boundaries.

We should set our security goals higher than "a system that can be used securely", and instead create systems that make others around them more secure. By taking advantage of the fact that human users interact with each other and interact with multiple computing systems on a regular basis, we can make that goal a reality.

References

[1] Cranor, L. F. A Framework for Reasoning About the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSec)* (2008).

[2] Joyce, R. NSA TAO chief on disrupting nation state hackers. In *USENIX Enigma* (2016).

[3] Rader, E., Wash, R., and Brooks, B. Stories as informal lessons about security. In *SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security* (July 2012), ACM.

[4] Vaniea, K. E., Rader, E., and Wash, R. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2014), pp. 2671–2674.

[5] Wash, R. Folk models of home computer security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (Seattle, WA, 2010).

[6] Wash, R., Rader, E., Berman, R., and Wellmer, Z. Understanding password choices: How frequently entered passwords are re-used across websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (Denver, CO, 2016).