Cameron Chandra

11/17/17

SI310/King

Security Case Study Write-up

To maintain user security, many online services have utilized a two-factor authentication system that requires multiple pieces of evidence to validate a user’s identity. This type of authentication negatively affects user’s interaction with software. Complex security protocols may confuse and frustrate users and simple protocols can be easily gamed. As the amount of software users grow, managing the trade-off between user experience and security becomes more challenging. Due to the vast diversity in users, it is impossible to create a security protocol that makes everyone happy.

When creating security protocol, UX designers must consider the security requirements of organizations and the user’s experience. Organizations are concerned about their user’s security because people do not use services that have frequent security breaches. For this reason, many services require password authentication. Platforms that contain user’s personal information, like Twitter, Facebook, and iCloud, require passwords to enter an account. By making authentication mandatory, services can guarantee a basic level of security. But, moving from a basic level of security may harm the way users interact with the product.

The increasing diversity of software users prevents universally satisfactory security protocols. One goal of UX designers is to improve the access of software. Technology is used by a diverse population in terms of age, literacy, intelligence, etc. While this improved access is a positive development in technology, it presents new security requirements. Authentication requires users to consent to sharing information with services. User demographics affect their willingness to consent to security protocol. Because of this, it is impossible for services to appease all their users. There will always be someone who requires more security and someone who is not willing to consent to elaborate authentication.

Considering user diversity, what can organizations do to improve upon the current two-factor authentication? First, organizations should mandate two-factor authentication, like many have mandated simple passwords. This increases users baseline security. This will warrant complaints, but users will adapt to the protocol as they have with passwords. From there, the only way two-factor authentication will improve is through technological advancements that appease the diverse user population.