Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication by Karlof et al.

October 25, 2017

It is easy for computer science experts to focus on technical aspects of the use of computers: we think of software and systems, but often disregard the impact of users in the system. To a certain extent, we can say our perception of a computer system differs from that of someone outside the field: we like to think of the computers, but users are not there for the apps or the security features.

Whitten and Tygar [1] launched the field of usable security. In this work, they had the idea of asking various people to send an encrypted email using PGP, and observed their behavior. The authors noted that the PGP documentation is full of jargon, and that users were quite confused during the study. Only about 30% of participants in the study were able to successfully send an encrypted email, and some participants committed severe security breaches, like emailing their private—instead of their public—keys to the researchers. This is a lesson about the disconnect between how software is used and how designers hoped it would be used.

1 Security for web authentication

The basic scheme for authentication consists in entering usernames and passwords. Recent studies have looked at password choices. Here are some highlights:

- A recent study looked at 70M Yahoo accounts. These account contain sensitive information, like users' email. It was found that the 10 most frequent password choices accounted for 1% of all passwords, and the top 1000000 to 50%. Clearly, high-entropy passwords are not commonly used.
- Another study found that there is a high reuse of passwords, with users managing a total of about 6 passwords for all authentication needs.

Websites implement some practices to encourage users to choose good passwords, like refusing to accept a password unless it meets some requirements, but it has been found that these measures are not effective: users choose do the least effort to get their password choice to comply with the rules. Another mechanism used by websites is showing users a meter which tells them the strength of their password. This mechanism has been found to result in modest improvements.

Yan et al. [2] ran a study at the University of Cambridge to assess password selection. First-year students were split into 3 groups of about 100 each. Each group was given alternative forms of advice regarding how to set a password, and measured the effect that this advice had on password strength. The advice was different as follows: a control group was given the same advice as students in previous years (Your password should be at least seven character long and contain at least one non-letter); the second group was asked to select a password by closing their eyes and picking randomly characters and digits from a piece of paper marked with these characters; there was also a passphrase group who was asked to form passwords based on a mnemonic. The researchers then tried cracking the password files, and found out that for each group they were able to crack 32%, 8%, and 6% of the passwords, respectively. A big factor of the second and third group's rate was non-compliance.

Burden of authentication is another issue that should be considered when devising mechanisms. A recent study found that on average people are asked to authenticate 23 times per day. A recent paper argued that one should consider having a fixed budget of burden: users are willing to spend some effort on authentication, but they have limits.

2 Password managers

With password managers, users can choose high quality passwords, but it turns out managers are not used that often. A recent study asked the public about their impressions of password managers, and found two obstacles to adoption:

1. Password managers are perceived as insecure. Participants in the study were concerned that their passwords were being stored locally in their machines, and someone who accessed their machine could now access their private data.

2. Participants showed concern about losing access to certain sites if their password manager stopped working

These studies are further lessons that we, as system designers, have to understand fears that users may have.

3 Browser indicators

Browsers display on the address bar certain symbols to indicate whether the certificates of a site are correct. The truth is users don't notice as it is much easier to overlook the absence of an item (e.g. a lock icon) than the other way around; to make matters worse, users have been conditioned to enter their credentials in login boxes. Some remedies which have been attempted to address this are persistent cookies and client certificates, as the user cannot be tricked into revealing something they do not know.

4 IoT Pairing

A recent work discussed the problem of pairing a device A with a device B. On the one hand, device A could display in its screen a dialog asking the user whether he wanted to accept being paired with device B. This is easy to attack since the user is conditioned to simply press "okay." On the secure side of things, one could imagine device A asking the user to type the public key of device B, but this is burdensome for the user. A middle path is for device A to offer the user a list of choices, i.e. "which of the following is the B's PK?"

References

[1] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, 1999.

[2] Jianxin Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. The memorability and security of passwords–some empirical results. Technical report, University of Cambridge, Computer Laboratory, 2000.