Security and Privacy

...

Introduction and Subcommittees

- Core Questions and Topics

  New techniques/systems/technologies design;

  Evaluation of existing/new system & lessons learned from real-world deployments

- Main Discipline related to Security and Privacy contributions

  Cyber security and privacy;

  Including but not limited to data/information/network/computer system(hardware)/software security and privacy

Introduction and Subcommittees

- CHI privacy and security subcommittee VS USENIX security

  USENIX is more technical oriented(mainly in Cyber security) while CHI accepts papers in a larger scope. E.g., Social experience/problem related to security issues.

- History

  Starting from CHI 2017 with subcommittee Privacy, security and visualization;

  In CHI 2020, subcommittee Privacy, security and visualization divided into 2 dedicated subcommittee 1)Privacy and Security and 2)Visualization

Why Phishing Works

...

Related Work

- Trust online
  - No paper considered that visual elements could be spoofed
- Anti-phishing toolbar
  - Users still gave private information 34% of the time
- Phishing emails using social networks

Components of the Study

1. Cognitive Walkthrough of Phishing Websites
   - 200 sample attacks from The Anti Phishing Working Group's "Phishing Archive"
   - Determined strategies for attacks
2. Evaluation of identification strategies
   - 5 types of strategies for identifying fake websites
3. Semi-structured interview after evaluation
   - SSL and certificate knowledge
   - Browser security indicators and phishing in general

Evaluating Strategies for Identifying Phishing Sites

Types of identification:

1. Security Indicators in website content only
2. Content and domain name only
3. Content and address, plus HTTPS
4. All of the above + padlock icon
5. All of the above + certificates

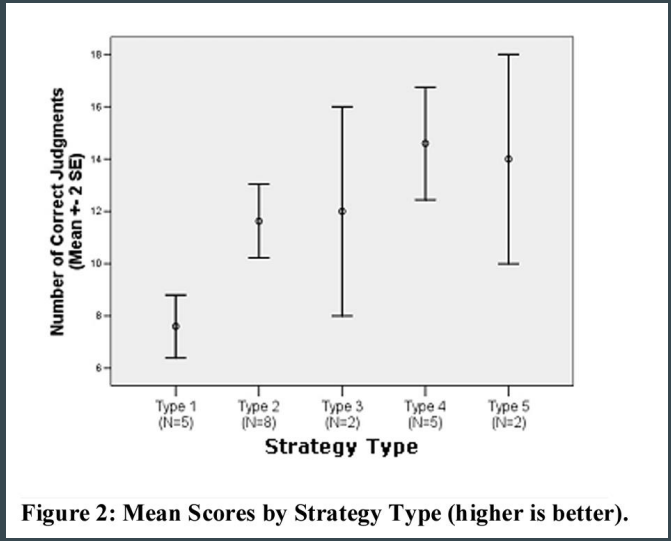

Figure 2: Mean Scores by Strategy Type (higher is better).

Findings

“In our study, neither age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing” (pg. 582)

- Call for human-centered security considerations.
- Assumption that visual elements can be spoofed and are inadequate as the sole indicators for (in)security.
- Indicators in periphery may not be notices
- Indicators showing insecurity may be more important than those

Discussion Questions

What privacy/security practices do you use?

How did you feel about some of the participants security practices?

What did you think about the way exploits and solutions were framed with respect to the users ability and knowledge?

How much should the burden be on the user to have security literacy or competence?

After reading this paper (2006), why do you think Privacy, Security and Visualization was originally together as a CHI subcommittee in 2007?

How could this study be more inclusive views of security and accessibility technology?

Why Johnny Can’t Encrypt:
A Usability Evaluation of PGP 5.0

Problem?

- User errors cause or contribute to most computer security failures,
- Yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent.
- Is this simply due to a failure to apply standard user interface design techniques to security?
- Security configuration errors are the probable cause of more than 90% of all computer security failures.

Understanding the problem

1- Defining usability for security

Definition:

Security software is usable if the people who are expected to use it:

- are reliably made aware of the security tasks they need to perform;
- are able to figure out how to successfully perform those tasks;
- don’t make dangerous errors;
- are sufficiently comfortable with the interface to continue using it.

Understanding the problem

2- Problematic properties of security:

- The unmotivated user property
- The abstraction property
- The lack of feedback property
- The barn door property
- The weakest link property

Understanding the problem

3- A usability standard for PGP

Stating the question in more detail, we want to know whether that person will, at minimum:

- understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people;
- understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people;
- understand that in order to sign email and allow other people to send them encrypted email a key pair must be generated, and figure out how to do so;

Understanding the problem

3- A usability standard for PGP

- understand that in order to allow other people to verify their signature and to send them encrypted email, they must publish their public key, and figure out some way to do so;
- understand that in order to verify signatures on email from other people and send encrypted email to other people, they must acquire those people’s public keys, and figure out some way to do so;
- manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up their private keys, and forgetting their pass phrases; and
- be able to succeed at all of the above within a few hours of reasonably motivated effort.

Aim and Argument:

- Show that effective security requires a different usability standard,
- Security will not be achieved through the user interface design techniques appropriate to other types of consumer software.

Approach:

- To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0.

- Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security.

Evaluation methods:

- We chose to evaluate PGP's usability through two methods:
    - an informal cognitive walkthrough in which we reviewed PGP's user interface directly and noted aspects of its design that failed to meet the usability standard;
    - a user test performed in a laboratory with test participants selected to be reasonably representative of the general population of email users.

Evaluation methods:

Cognitive walkthrough:

- Visual metaphors
- Different key types
- Key server
- Key management policy
- Irreversible actions
- Consistency
- Too much information

Evaluation methods:

User test

- Purpose
  - Our user test was designed to evaluate whether PGP 5.0 meets the specific usability standard.
  - We gave our participants a test scenario that was both plausible and appropriately motivating, and then avoided interfering with their attempts to carry out the security tasks that we gave them.
- Test design
  - Our test scenario was that the participant had volunteered to help with a political campaign and had been given the job of campaign coordinator
- Participants
  - The user test was run with twelve different participants

Results

- The analysis found
  - a number of user interface design flaws that may contribute to security failures,
  - the user test demonstrated that when our test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0, the majority of them were unable to do so successfully.

Conclusion

- We conclude that:
  - PGP 5.0 is not usable enough to provide effective security for most computer users, despite its attractive graphical user interface,
  - supporting our hypothesis that user interface design for effective security remains an open problem.