Usable Security

Dr. Asem Kitana

Usability

- The mechanism of employing a system to achieve a set of goals, by taking in the consideration effectiveness, efficiency, and satisfaction.

- Usability is deployed to improve user experience and interaction with systems.

Usability Components

- Effectiveness:

The ability of a system to provide facilities/features to users to reach their goals.

- Efficiency:

The amount of available resources (e.g. time, effort, actions) that can be utilized by users to reach their goals.

- Satisfaction:

The measurement of how pleasant the user is when using a system.

Usability Components

- Effectiveness:

Can users achieve their goals with the system?

Can users do what the system says it should be able to do?

- Efficiency:

How much effort is required from users in order to achieve their goals?

- Satisfaction:

Is the system pleasant to use?

Security vs. Usability

- Security is a process, rather than a product.
- In security, humans are the weakest link.
- Therefore, hackers only need one error from this weakest link (humans) in the security process, in order to conduct a successful attack.
- Social engineering attacks work pretty good in this context.

Security vs. Usability

Confidentiality
Integrity
Availability

VS.

Effectiveness
Efficiency
Satisfaction

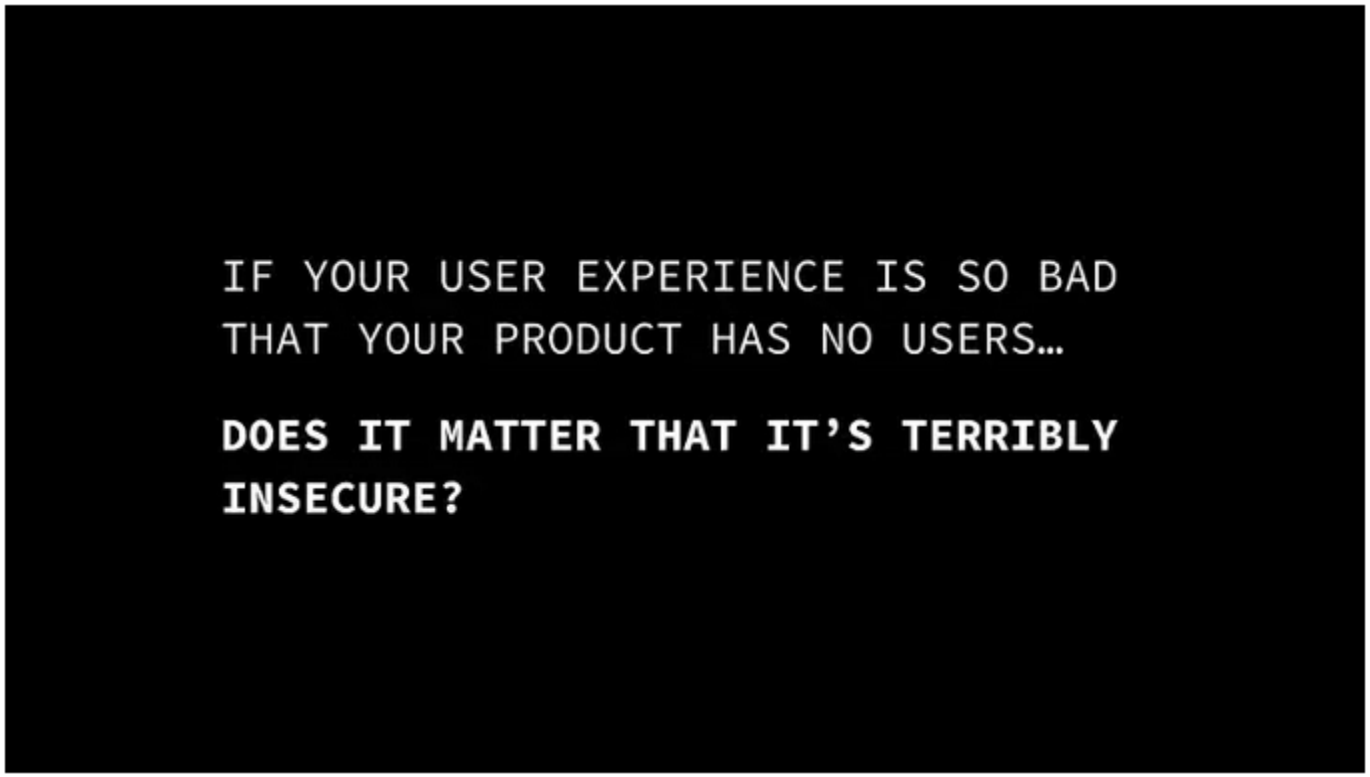
Security vs. Usability

Security vs. Usability

Security vs. Usability

Security vs. Usability

Security vs. Usability



Security vs. Usability

Security-Usability dilemma

- Usually the user looks for the effectiveness, efficiency, and satisfaction of a system, rather than the confidentiality, integrity, and availability of that system.

- In other words, users look for the ease of use, rather than the security of a system.

Example: Passwords

- If a password is *very* strong (secure), then it is not usable (hard to remember).
- If a password is usable (easy to remember), then it is very weak (insecure).
- If a strong password should be used, but the user can not remember it, then the user will write it down.

Usable Security

Passwords Security-Usability dilemma solutions:

- Passphrases
- Frequently changed passwords
- Dynamic passwords
- Graphical passwords
- Hardware-based solutions (e.g. Tokens)

Graphical Passwords

- Graphical passwords could be a good solution for the security-usability dilemma:
  - Larger password space
  - More difficult to build dictionary
  - Easier to remember and harder to forget
  - Better balance between security and usability

Example2: CAPTCHA

- Completely Automated Public Turing test to tell Computers and Humans Apart
- Represents a form of challenge-response test used in systems to determine whether the user is human.

Usable Security

- CAPTCHA security-usability dilemma:

- If a captcha is very strong, then it is hard for machines, and also hard to be solved by users.
- If a captcha is easy for users to solve, then it is often weak (easy for machine to recognize).

Usable Security

- Can we find a better CAPTCHA scheme that provides a good balance between security and usability?

- CAPTCHA + Behavioral Biometrics
- CAPTCHA + BMI (Brain-Machine Interface)

Usable Security

Usable Security is the study of how we can best ***balance*** the needs of security with how the users of that system wish to use it.

Usable Security

- Good Practices:

- Deploy strong cryptography algorithms in data communications.
- Assure the user involvement in the system design process.
- Conduct user modeling for new security features.