What is usability?

Mainack Mondal

CS 60081
Autumn 2020

Mainack Mondal

Roadmap

- What is usability?
  - Properties of usability
  - How do usability mix with security?

- Why is usable security and privacy hard?

A definition of usability

The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

- ISO 9241

Properties of a usable system

- **Learnability:** time taken by typical users to learn actions to do specified task(s)

Properties of a usable system

- **Learnability:** time taken by typical users to learn actions to do specified task(s)

- **Efficiency:** How long does it take to perform a typical task by a typical user

Properties of a usable system

- **Learnability:** time taken by typical users to learn actions to do specified task(s)

- **Efficiency:** How long does it take to perform a typical task by a typical user

- **Errors:** The rate of errors users make when performing tasks (example?)

Properties of a usable system

- Learnability: time taken by typical users to learn actions to do specified task(s)

- Efficiency: How long does it take to perform a typical task by a typical user

- Errors: The rate of errors users make when performing tasks (example?)

- Memorability: How users can retain their knowledge about the system over time?

Properties of a usable system

- Learnability: time taken by typical users to learn actions to do specified task(s)

- Efficiency: How long does it take to perform a typical task by a typical user

- Errors: The rate of errors users make when performing tasks (example?)

- Memorability: How users can retain their knowledge about the system over time?

- Satisfaction: Do users like parts of the system?

How to measure usability?

- System usability scale (SUS)

    - 10 multiple choice questions

    - Options are 5-point scale for each questions

        - From strongly agree to strongly disagree

    - https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

Questions

1. think that I would like to use this system frequently.

2. I found the system unnecessarily complex.

3. I thought the system was easy to use.

4. I think that I would need the support of a technical person to be able to use this system.

5. I found the various functions in this system were well integrated.

6. I thought there was too much inconsistency in this system.

7. I would imagine that most people would learn to use this system very quickly.

8. I found the system very cumbersome to use.

9. I felt very confident using the system.

10. I needed to learn a lot of things before I could get going with this system.

Usable Security and Privacy

- We need to consider security / privacy and usability together

- Need to take an interdisciplinary approach
  - Security + network analytics + HCI + …

Why is usable security different than HCI?

- We NEED to consider a threat model

    - Generally no threat model in HCI

- Usability is not enough, we also need security

    - Adversary will (try to) fool users
    - Users will behave predictably
    - Users will act under stress and make mistakes
    - Users will be careless, unmotivated, busy

Putting together Security and Usability

Security	Usability	Usable Security
Security constraints are first, humans come second	Humans come first, security constraints are very rarely considered	Security constraints and human behavior both are primary constraints

Putting together Security and Usability

Security	Usability	Usable Security
Security constraints are first, humans come second	Humans come first, security constraints are very rarely considered	Security constraints and human behavior both are primary constraints
Humans are adversaries	Humans are normal users	Humans are both users and adversaries

Putting together Security and Usability

Security	Usability	Usable Security
Security constraints are first, humans come second	Humans come first, security constraints are very rarely considered	Security constraints and human behavior both are primary constraints
Humans are adversaries	Humans are normal users	Humans are both users and adversaries
Threat model	Mental model, cognitive model, perception	BOTH threat model (adversary) and mental model (user)

Putting together Security and Usability

Security	Usability	Usable Security
Security constraints are first, humans come second	Humans come first, security constraints are very rarely considered	Security constraints and human behavior both are primary constraints
Humans are adversaries	Humans are normal users	Humans are both users and adversaries
Threat model	Mental model, cognitive model, perception	BOTH threat model (adversary) and mental model (user)
Security properties	Usability properties	BOTH security properties and usability properties

Putting together Security and Usability

Security	Usability	Usable Security
Security constraints are first, humans come second	Humans come first, security constraints are very rarely considered	Security constraints and human behavior both are primary constraints
Humans are adversaries	Humans are normal users	Humans are both users and adversaries
Threat model	Mental model, cognitive model, perception	BOTH threat model (adversary) and mental model (user)
Security properties	Usability properties	BOTH security properties and usability properties
System design/measurement	User studies	System design/measurement + User studies

Putting together Security and Usability: Passwords Example

Security	Usability	Usable Security
# all possible passwords? How to make the password space larger (introducing new password creation rules) to make the password harder to guess? Can an **attacker** guess the password for given set of creation rules by observing users to type in the password?		

Putting together Security and Usability: Passwords Example

Security	Usability	Usable Security
# all possible passwords? How to make the password space larger (introducing new password creation rules) to make the password harder to guess? Can an **attacker** guess the password for given set of creation rules by observing users to type in the password?	How difficult is it for a human to create, remember, and enter a password in your interface? How long does it take? How hard is it for users to learn the system? Does the system support users with disabilities? E.g., blind users?	

Putting together Security and Usability: Passwords Example

Security	Usability	Usable Security
# all possible passwords? How to make the password space larger (introducing new password creation rules) to make the password harder to guess? Can an **attacker** guess the password for given set of creation rules by observing users to type in the password?	How difficult is it for a human to create, remember, and enter a password in your interface? How long does it take? How hard is it for users to learn the system? Does the system support users with disabilities? E.g., blind users?	All the security + usability questions How do **users** select their passwords? How can we help them choose passwords which are less guessable by **attackers?** As we add more and more password creation rules, what are the impacts on usability properties of the system and predictability in the choice of passwords?

Roadmap

- What is usability?
  - Properties of usability
  - How do usability mix with security?

- Why is usable security and privacy hard?

Challenges of Usable Security and Privacy research

- Interdisciplinary: Requires thinking about both HCI & security

Challenges of Usable Security and Privacy research

- Interdisciplinary: Requires thinking about both HCI & security

- Balancing act: trade-off between Security/Privacy & Usability

Challenges of Usable Security and Privacy research

- Interdisciplinary: Requires thinking about both HCI & security

- Balancing act: trade-off between Security/Privacy & Usability

- Evaluation: Easy to measure "How long does it take to do X in System Y". Hard to measure "Do you feel system Y is secure"? Users *cannot accurately* describe security issues

Challenges of Usable Security and Privacy research

- Interdisciplinary: Requires thinking about both HCI & security

- Balancing act: trade-off between Security/Privacy & Usability

- Evaluation: Easy to measure "How long does it take to do X in System Y". Hard to measure "Do you feel system Y is secure"? Users *cannot accurately* describe security issues

- Ecological validity: How to emulate attacks of real-world?

Challenges of Usable Security and Privacy research

- Interdisciplinary: Requires thinking about both HCI & security

- Balancing act: trade-off between Security/Privacy & Usability

- Evaluation: Easy to measure "How long does it take to do X in System Y". Hard to measure "Do you feel system Y is secure"? Users *cannot accurately* describe security issues

- Ecological validity: How to emulate attacks of real-world?

- Modelling adversaries: Need to account for perceptions of adversaries too? ("I am not interesting enough")

Challenges of Usable Security and Privacy research

- **Interdisciplinary**: Requires thinking about both HCI & security

- **Balancing act**: trade-off between Security/Privacy & Usability

- **Evaluation**: Easy to measure "How long does it take to do X in System Y". Hard to measure "Do you feel system Y is secure"? Users *cannot accurately* describe security issues

- **Ecological validity**: How to emulate attacks of real-world?

- **Modelling adversaries**: Need to account for perceptions of adversaries too? ("I am not interesting enough")

- **Technology change**: Users are often not familiar with changing technologies and attacks.