13. Mental Models; User Education

Blase Ur
May 14th, 2019
CMSC 23210 / 33210
Mental Models
Mental Models Study

Rick Wash, “Folk Models of Home Computer Security” (SOUPS 2010)
Wash 2010

• How uses *perceive* and *understand* computer security

• Understand the *mental models* of users
Wash 2010

• 33 semi-structured interviews
• About 45 minutes each
• Broad questions
• Hypothetical scenarios
Wash 2010

• Folk models used to decide whether to follow security advice

• For example, “Use anti-virus software” was viewed as *important* to users who saw viruses as supporting crime and *less important* to users who viewed viruses as buggy software
Wash 2010: Viruses

- “Virus” as general term for malware
- Generically bad
- Buggy software
- Virus as annoyance
- Support crime
- Multiple of the above
Wash 2010: Hackers

- “Hacker” term used for malicious actors
- Digital graffiti artists
- Burglars
- Criminals who target valuable targets
- Contractors who support criminals
- Multiple of the above
Wash 2010

• Main takeaway: How users perceive threats can affect their security-related behavior.

• Users often do not understand threats the same way that sophisticated users do.

• Users may take actions that only make sense if you understand their behavior.
Software Updates

Java Update Available
A new version of Java is ready to be installed.

Java Update Available
Java 6 Update 22 is ready to install. Click the Install button to update Java now. If you wish to update Java later, click the Later button.

More information...
Software Updates


• Update = New features? Or security fix?
Emilee Rader and Janine Slaker, “The Importance of Visibility for Folk Theories of Sensor Data” (SOUPS 2017)

- Data collection is opaque, so how can users make decisions about data collection?
Expert vs. Non-Expert Mental Models

Expert vs. Non-Expert Mental Models

• What are the top three things you do to stay safe online?
• Experts
  – Update system
  – Use unique passwords
  – Use strong passwords
  – Two-factor auth
  – Password manager
  – Check if HTTPS
Expert vs. Non-Expert Mental Models

• What are the top three things you do to stay safe online?

• Non-experts
  – Anti-virus
  – Use strong passwords
  – Visit only known websites
  – Change passwords
  – Don’t share information
  – Use unique passwords
Drawing Mental Models

Revisiting Encryption Through Mental Models
Complexity of asymmetric encryption

• User creates a keypair
  – Public key should be widely distributed
  – Private key should never be distributed

• Private key protected with a password

• Two very different functions:
  – Encrypting (secrecy)
  – Signing (authenticity)

• Need person’s key to communicate
(Just some) usability problems

• Encryption is rarely configured by default
• Public/private key encryption
  – How to get someone’s public key?
  – How do I make it work on my phone?
• You often need a good password
  – …and you can’t lose it or forget it
• Configuring multiple devices
• “Only paranoid people use encryption”
Open vs. closed ecosystem

• Open standards
  – Don’t require specific ecosystem or software
• Messaging apps (some security-focused)
  – (Sometimes) can minimize configuration
  – More centralized trust

![Signal Private Messenger](image1)
![GPG](image2)
![WhatsApp](image3)
![Telegram](image4)
![ChatSecure](image5)
Whatsapp

Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Messages you send to this chat and calls are now secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.
Important distinctions

• **End-to-end encryption**: messages encrypted between sender and recipient
  – In theory, providers can’t access
  – **Perfect forward secrecy**: compromise of key does not compromise previous session keys

• As opposed to messages being encrypted between you and the company (e.g., WhatsApp), and then between the company and recipient
Do you have the right key?

- Man-in-the-middle attack

- Ways of trusting a person → key binding:
  - Public-key infrastructure (certifying authorities)
  - Web of trust (someone you trust vouches)
  - Exchange keys out of band
  - Platform provider verifies
  - Key servers: https://pgp.mit.edu/
Verifying you have the right key

Scan the code on your contact’s phone, or ask them to scan your code, to verify that your messages and calls to them are end-to-end encrypted. You can also compare the number above to verify. This is optional. Learn more about WhatsApp security.
Locally verifying key

- Out-of-band channel
- Interaction
  - Bump, button press, shake devices
- Location-limited channel
  - Bluetooth, sounds, wired connection
- Short string comparisons
Remotely verifying key

GnuPG
3A70 F9A0 4ECD B5D7 8A89
D32C EDA0 A352 66E2 C53D

OpenSSH

bubblebabble
xucef-masiv-zihyl-bicyr-zalot-cevyt-lusob-
negul-biros-zuhal-cixex

OTR
4206EA15 1E029807 C8BA9366 B972A136 C6033804

WhatsApp
54040 65258 71972 73974
10879 55897 71430 75600
25372 60226 27738 71523
Remotely verifying key

(a) OpenSSH Visual Host Key
(b) Vash
(c) Unicorn