02. Usable Encryption

Blase Ur, March 29th, 2017
CMSC 23210 / 33210
Today’s class

• Reasoning about the human in the loop
• Usable encryption
The Human in the Loop
(Continued)
What to do about hazards?
Best solution: remove hazard
If all else fails: warn
HOLE
HOLE
Automate and change tasks to reduce need for user involvement

Might be dangerous

User must decide

Use automated analysis to determine probability of danger
Support user decision

- High probability of danger
  - Block

- Might be dangerous
  - User must decide

- Very low probability of danger
  - Don’t bother user

Improve warnings

Help user decide by asking question user is qualified to answer
Warnings and visual communication
浴衣・スリッパのままで、客室フロア（廊下）以外へ
お出になることは、非常時を除き、ご遠慮ください。

×

×
What state is this system in?
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegafonse.
Bad question

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

Don’t go there  Go there anyway
Better question

You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Go to yourbank.com  Go to evilsite.com
Why do user studies?

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Useful to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess needs</td>
<td>Decide what to build</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Determine whether system meets requirements and what needs to be improved</td>
</tr>
<tr>
<td>Understand tradeoffs</td>
<td>Decide which features/approaches/systems best fit particular needs</td>
</tr>
<tr>
<td>Find root causes</td>
<td>Determine where redesigns or new approaches are needed</td>
</tr>
</tbody>
</table>
What do we Want?
EVIDENCE BASED SCIENCE
When do we Want It?
AFTER PEER REVIEW
Excuses for not doing usability studies

• If people weren’t so lazy/stupid/careless the system would work just fine
• I’m a cryptographer, not a usability expert
• I already know what people want
• No time, no money
• I find the system easy to use so it must be usable
• My kids can use the system so it definitely must be usable
User study steps

• Identify research questions, metrics, and use cases
• Decide on type of study and design study protocol
• Develop detailed scripts, surveys, scenarios, incentives, instrumentation, prototypes, recruiting materials, etc.
• Obtain ethics approval
• Pilot and iterate on study design
• Collect data
• Analyze results
• Repeat some or all of these steps as needed
Usable security study challenges

- Keeping it real (ecological validity)
  - Create realistic sense of risk (**but not real risk**)  
  - Provide realistic incentives
  - Don’t bias participants
- Measuring the right thing
  - Design the right protocol
  - Control the variables
  - Instrument
- Observing infrequent events and small differences
- Legal, ethical, and practical issues
Some core usability principles
Where is the light switch?
How do you unplug the sink?
How do you turn on this shower?
More or less confusing features
People were confused until they posted instructions.
Normally you pull handles
Which way do you turn it to make it hot?
Perspective matters
Is the ladies’ room on the left or the right?
From which direction will users be viewing the instruction?
Design communicates function
Locking and unlocking door automatically changes color of lock indicator
Inconvenient designs
Unfortunately these Urinals are out of order. We aim to resolve this maintenance problem as soon as possible.

We apologise for any inconvenience caused.

Thanks for the apology, but how about telling me where I can find one that works?
Stove layout
Stove layout
Stove layout
Doors
Doors
Doors
A better solution would be to add a spring so the door won’t slam.
Encryption: A crash course
Encryption basics

• Putting information in code so that unauthorized people can’t read it

• What might you want to encrypt?
  – Email or text message
  – Individual file
  – Hard drive, USB stick
  – Communication with a website
  – Everything
Quick clarification of primitives

- **Hash function:** one-way (irreversible)
  - Small change in input → big change in output
  - `md5(blase) = 12b872adb2588c668d706d847fc1da7e`

- **Encryption:** reversible (if you know secret)
  - “this is a test” → `Xe0yUqyOnY8JskyCQ2cYIg==`
  - `Xe0yUqyOnY8JskyCQ2cYIg==` and `chicago` (secret)
  → “this is a test”
Two main encryption approaches

• Symmetric encryption (same key used for encryption and decryption)
  – Prominent examples: AES, DES, etc.
  – Requires key exchange (out of band)

• Asymmetric encryption (keypair: public key and private key)
  – RSA, ElGamal, elliptic curve crypto
Properties of encryption

• **Secrecy**: Is Blase the only person who can decrypt my message?

• **Authenticity**: Did this message really come from Blase?

• **Integrity**: Has someone tampered with Blase’s message?
Usable encryption
Why Johnny can’t encrypt

• Why can’t Johnny encrypt?
• Why was it so hard for participants to complete the tasks?
• How did the experimenters motivate the tasks and get participants to care about security?
• What role did attackers play in this user study?
Why Johnny can’t encrypt

• Security principles
  – Unmotivated user
  – Abstraction property
  – Lack of feedback
  – Barn door property
  – Weakest link property

• Cognitive walkthrough vs. user test

• Bad metaphors
Why Glenn couldn’t encrypt
Why Glenn couldn’t encrypt
Why Glenn couldn’t encrypt
Why Glenn couldn’t encrypt
Why Glenn couldn’t encrypt

• [http://vimeo.com/56881481](http://vimeo.com/56881481)

• “And yet, Greenwald still didn't bother learning security protocols. ‘The more he sent me, the more difficult it seemed,’ he says. ‘I mean, now I had to watch a f***ing video . . . ?’”

• Snowden ended up reaching out to Laura Poitras instead

gpg - GNU Privacy Guard

SOURCE

Message that could get source killed

INTERNET

Public GPG Key

JOURNO

BEGIN PGP MESSAGE
Version: GnuPG v1.4.10 (GNU/Linux)

hQGMAweld0xv7hmgA0wvYXac8BN3HMyppj1W8TMp56NGH4JyaFVTDPkxYx16bGJ2S
hQG307F52dC3Q2p1PfidbymybAhMoxalqF931AIg3Fv32X3Ksadn8s51DwVXhQeqa6
SnpQEGc58SBZ354M//pQ0PR5TPpHs9-MMDxGnkVxKxhLWw9rMTbYvK4v5lXZt1cDMD
EOOCVer33xXYv7Pj=4KlRBT1TrawGr72zCJdV3S3C3xMxvStlijpw+MBnhpGvSNiE6sOuT
InrWwPvIsy9NS2s5hAsv5=+avy/hVRKz1AA2vugK+OW193C11dD4eCkKkwCkhKZN
2HzWwxx2q=dlWpDVLvkg/z3bLyyq/toaM5BM5yNO4Mj/z2kFDCv0fnszsbjJCn
imKzKxhmxVxRyvS2c/MWd16yRykMkJxF2QD65OCxml6C4v98s3jW8Mo7irWxuArkTCG
ZPPwsUdH+z6bdm4QYDNAaPw5d4dfT334pKh3K552t8a4w0cSGYKRSKTU3ECT912

END PGP MESSAGE

Public GPG Key
The takeaway from the password caution should be: use memorable, long, strong passwords.

"I hateses all kinds of YELLOW # 5" is memorable and would req 65,53 trillion trillion trillion centuries to attack via brute force.

Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.

"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.
Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.

"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.
The takeaway from the password caution should be: use memorable, long, strong passwords.

"I hateses all kinds of YELLOW # 5" is memorable and would req 65.53 trillion trillion trillion centuries to attack via brute force.
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
Whatsapp

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

This is not a first from WhatsApp.
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
Verifying you have the right key
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