Authentication Part 4: Issues and Implications

People and Security

Lecture 8

The great authentication fatigue

(1) 23 knowledge workers asked to keep a diary of all their authentication events for 24 hours registering

i. Name of system
ii. Credentials needed
iii. Memory aids used
iv. Time
v. Frustration level

(2) These records were used as starting point for semi-structured interview

Results

- Frequency: On average, employees authenticated 23 times/day (ranging from 4 to 40)
- Failure rate: 529 authentication events, there were 49 problems (9.3%)
- Most common causes of these problems were:
  - Mistyped passwords (49%)
  - Wrong passwords used (14%)
  - Unknown cause (14%)
  - Forgotten usernames (4%)
- Most authentication events caused mild to moderate frustration

Results

- Memory aids for passwords used by all:
  - Stored in client (browser): 48%
  - Written on paper: 48%
  - Stored in a file: 26%
  - Password manager: 26%
  - Fingerprint reader: 26%

Key insights

- Authentication is a significant drain on productivity
  - not just the time spent, but *disruptiveness* on primary task
  - the more complex the authentication task, the higher the cost of task-switching

Examples of productivity effects

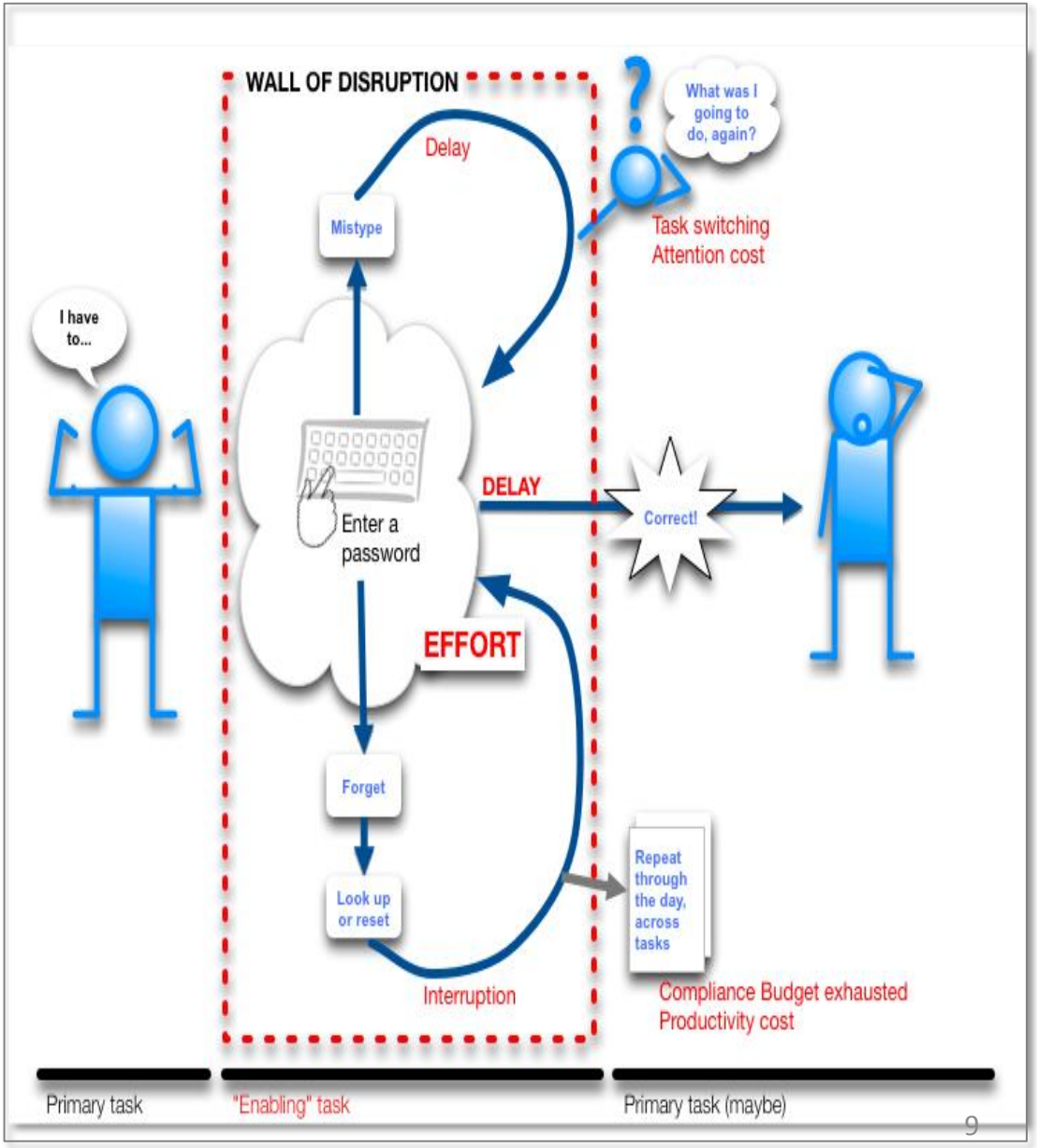
"For the email, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my email. I might do it once every three or four hours instead of every 20 minutes."

"… there are lots of things that harm productivity, such as the inconvenience associated with working from home. I would probably do more work from home if there weren't so many security issues associated with that."

Multiple authentications required

"You have to put in name and password three times before you're fully hooked up. If something goes screwy without luck, you have to do it four times because you have to do it once to decrypt, once to enter in, and then once to connect to the wireless."

- Authentication as a ‘wall of disruption’



Authentication hate list

1. Repeated authentication to the same system (e.g. because of 15 min time-outs)
2. Authenticating to infrequently used systems
   - Difficulty to recall previous password
   - Password could have expired in the meantime
   - Resetting a password is not easy
3. Creating a valid password (different rules for each system)

"Well, I think that if I just logged in, then it should be able to understand that I just logged in and not ask me for the password again. […] That's too much, because you shouldn't have to do extra work to authenticate. Because yeah, it can just pick up what you do."

http://humourspot.com/wp-content/uploads/2013/04/Sorry-but-your-password-must-contain....jpg

Authentication Hate List

4. Managing a high number of different credentials
   - Different policies means strategies for creating & recalling pws don't work
   - Which credentials to use for which system
5. Use of RSA tokens
   - *"It's this extra, again, effortful stuff. I have to dig around in my bag and get the RSA ID token out and then set it on my laptop and then type out the number, make sure that you're not typing it right before changes or as it's changing or whatever."*

Employees' coping strategies

1. Batching and planning of activities to limit the number of logins
2. Storing passwords or writing them down
3. Resetting passwords to the same one
4. Creating passwords to be memorable
5. Creating passwords that are easy to type on mobile devices
6. Folder of email reminders sent by the system – a lo-fi password manager

Maladaptive coping strategies

- Giving up devices:
  - *"If I had a company laptop I would have to log in twice, once when you turn it on because the hard drive's encrypted, and then again to actually get into Windows or the operating system. […] So I never wanted a company laptop for that reason. I don't want to have to log in more times than I need to."*
- So many employees stop taking laptop when travelling – or give it back altogether

Maladaptive coping strategies

"I have research collaborations with people in other institutions, but it is just extremely difficult to share files with them, to transfer software you're writing, and that sort of thing. To me, the way that security impacts work is not that I waste a few seconds typing in a password, but it is these things that you just can't do because of the limitations of security policy. […] I can think of cases when I have thought it would be really nice to include some person at another university on a software development project, but then I realize it is going to be such a tremendous pain to organize that."

What most coping strategies have in common

1. Users want to be in control of their effort postponing authentication to when it's convenient to them
2. Physical effort (e.g. copying and pasting of passwords from a file) is preferred over cognitive effort as employees want to stay mentally focussed on their work
3. Password managers are preferred as they can save approx. 10s per login and save users from the cognitive effort of recalling a password and the physical effort of typing them in
4. Users have a *compliance budget* and if the effort is too great they might give up trying or in some cases circumvent a policy to get their work done

Final thoughts on Authentication

- Identification: Who are you?
- Authentication/Verification: Prove it!
- Authorisation: What are you allowed to do?

> ***"Conflating the three – running them together, failing to distinguish each from the others – can lead to serious security problems."***
>
> - Schneier: Beyond Fear, 2003

Problems

- Confusing authentication with identification
  - Last 4 numbers of social security number
  - Mother's maiden name, …
- Confusing authentication with authorization
  - Keeping password written down locked in safe is good if you are away and manager needs to get to your files

Making authentication work

- Authentication is a system
- More than deciding how to authenticate
  - Who does registration?
  - Where is the information stored?
  - How is that information guarded?
  - What carries authentication?
  - How easy is to authenticate the authentication?

Key issues

1. Signatures easy to forge with scanners and copiers
2. Token expiry – how easy/reliably can they be revoked?
3. How easy is it to fake, or illegally obtain a token?

Do you need ID?

- Identification can lead to privacy issues.
- Can be avoided by implementing authentication/authorisation only.
- But: identification is essential to establish audit trails, which are often required for security of other processes

User IDs and accounts

- Different user IDs for different systems increase memory load
- Reduce number of user IDs (standardise user IDs within organisation) to improve usability
- But: may disclose information about organisation: random user IDs may provide additional security

Example user ID policy

"User identification names shall consist of the 5-digit employee identification number assigned by the Human Resources Department and prefixed by a single letter."

- Barman, *Writing Information Security Policies*

Default accounts

- Default usernames (e.g. set by manufacturer) must be removed
- Default passwords must be changed
  - Sometimes simply forgotten
  - Often not changed because of worries about availability "locking out"
  - Need backup mechanism for such accounts

Default settings

[Feynman goes to see Los Alamos locksmith, who opened a safe of the base captain, who had forgotten the combination - without drilling into it – and asked him]

"You must know how to crack safes?"

"Yeah – I know the locks come from the factory set at 25-0-25 or 50-25-50, so I thought: who knows, maybe the guy didn't bother to change the combination, and the second one worked."

This big shot captain had to have a super, super safe, and had people go through all the effort of hoisting the thing up into his office, and then he didn't even bother to change the combination.

I went from office to office in my building, trying those two factory combination, and I opened about 1 safe in 5."

From: *Surely you're joking, Mr Feynman?*

Still the same problem today

- Many enterprises have more administrative passwords than those attached to ordinary user accounts. About half of those are never changed, especially enterprise software admin applications.
- Privileged routers and servers never changed in 13% cases.
- Hardwired passwords in software – see Stuxnet
  - http://www.schneier.com/blog/archives/2010/10/stuxnet.html
- Other PAS issue: someone inserted USB in system
- The SHODAN search engine revealed 1000's of connected systems still with the default password
  - http://money.cnn.com/2013/04/08/technology/security/shodan/index.html

Distress codes

- Code that user transmit to indicate that they are in distress
  - Hostage situation
  - Being forced to withdraw money at ATM
- Can be
  - Special PIN, e.g. burglar alarm, ATM
  - Code word in voice call
- Key: Must “look normal” to attacker

Example: burglar alarm

- A distress code can be programmed into system
- If legitimate user is forced to disarm the alarm, can enter distress code instead
- System simulates normal functioning (e.g. seems to disarm alarm) but sends signal to monitoring company.

Issues with distress codes

- Rarely used, so memorability is a problem
  - For PINs and PWs, best to use "distress variant" on normal one
  - For burglar alarms, Matthew Francis advises to write distress code on inside of alarm pad
    - Does not need to be remembered
    - To attackers, it looks as if it is the "real" PIN
    - They will trigger the alarm even if user is not present