Security and Usability

“[S]ystems security is one of the last areas in IT in which user-centered design and user training are not regarded as essential.”

“[H]ackers pay more attention to the human link in the security chain than security designers do.”

[Adams and Sasse, 1999] (And still true today!)
Security and Usability (2)

Can usability and security co-exist?

- Does increased security reduce usability?
  - Yes (sometimes)
- Does increased usability reduce security?
  - Yes (sometimes)

- Above examples should not be taken as general responses to questions

- We do know that reduced usability will also reduce security – System designers must find the balance between usability and security
And the design environment isn’t easy ...

- “Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)”

Authentication

Authentication is the process of confirming someone (or something) as authentic

Three information types for authenticating

- **Something you have**
  - Mobiles, smartcards, ...

- **Something you are**
  - Biometrics – physical characteristics, involuntary actions
  - Fingerprints, facial recognition, voice recognition, ...

- **Something you know**
  - Password, PINs, passphrases, ...

- *(Also exists: Someone you know)*
Usability and Authentication

Authentication information has a “lifecycle,” and usability can be addressed at each stage

- Issuance
  - Stage at which information is created or issued
- Use
  - Stage at which information is used to authenticate
- Maintenance
  - Stage at which information is updated or retired

At each stage, one should try to adhere to usability design principles
Something You Have – Usability Considerations

Recall examples: Mobile, smartcard

Issuance

- Require physical interaction (e.g., mail, in-person)

Use

- Some requirements placed on human memory (e.g., Where did I leave my card?)
- Human-card-machine interface issues, e.g., “Which way do I insert the card?”

Maintenance

- See 'Issuance'
- Require periodic replacement due to 'wear-and-tear' and loss
Something You Are – Usability Considerations

Recall examples: Fingerprint, facial recognition

Issuance

- No 'issuance' *per se*, but still need to attend registration
- No everyone is able to successfully register

Use

- No requirements placed on human memory (e.g., choice of finger can be specified at authentication)
- Human-machine interface issues, e.g. not all humans have readable fingerprints, cut finger

Maintenance

- Limited options for renewal due to finite set of biometrics
Something You Know – Usability Considerations

Recall examples: Password, PIN

Issuance

- Ability to follow rules (length, capitalization, ...)
- Ability to create something secure and memorable

Use

- Can I recall my password (with 100% accuracy)?
- If so, which one?

Maintenance

- See 'Issuance'
- Ability to avoid re-using older information
Some ‘Usability Principles’ for Authentication

Issuance

- Limit amount of physical interaction
- Limit human processing and learning requirements
- Limit number of seemingly artificial constraints

Use

- Limit memory requirements
- Limit requirements for perfect accuracy

Maintenance

- See ‘Issuance’
- Limit excessive update requirements
'Something You Know' – Root Causes

Passwords require “100% correct, unaided recall of a non-meaningful item” [Sasse, 2003]

The cause of usability issues are known

- Rules, rules, rules!
  - Length of at least 8 characters ...
  - Must contain one lower and uppercase, one number, ...
  - Monthly updates
- Accurately memorize a non-meaningful item
- Dozens of accounts with passwords

Unfortunately, the solutions to the 'Create-and-Memorize' paradigm/dilemma aren't so obvious
Something You Know – Potential Improvements

Don’t rely upon the *creation* and *memorization* of *new information* for authentication

Use information that is *already known*

**Cognitive passwords**

- Passwords based upon information already known
- Best known example is use of “challenge questions”
- A.k.a. Knowledge-Based Authentication
Challenge Questions – Some Examples

Consider the following examples

- What is your mother’s maiden name?
- What is your favourite colour?
- Who is your favourite actor?
- What was your high school locker combination?
- What was your first pet’s name?

Are these questions secure?
Are these questions usable?
Challenge Questions – Usability Considerations

How might challenge questions, in general, fare against our usability principles?

Issuance

- Limit amount of physical interaction
- Limit human processing and learning requirements
- Limit number of seemingly artificial constraints

Use

- Limit memory requirements
- Limit requirements for accuracy

Maintenance

- See ‘Issuance’
- Limit excessive update requirements
- No new words to learn
- Possible constraints – depends upon questions
- Must still associate answers with questions
- Less concern with memorability
- Accuracy still an issue
- Finite, but seemingly vast, source of information
Challenge Questions – Usability Criteria

Applicability

- Users have sufficient information to provide a relevant answer to a question

Memorability

- Users can consistently recall the original answer to a question over time

Repeatability

- Users can consistently and accurately (syntactically) repeat the original answer to a question over time
Challenge Questions – Security Criteria

Guessability

- Traditional measure in which the security level is directly proportional to the number of possible answers for a given question
- Can consider length of answer (*Blind Guess*) and size of answer space (*Focused Guess*)

Observability

- The security level is inversely proportional to an attacker’s ability to find the answer to a given question (*Observation-Based Guess*)
- Note that “attacker's” might be strangers, acquaintances, colleagues, friends, family members
Challenge Questions – Some Examples Revisited

Consider the following examples

- What is your mother’s maiden name?
- What is your favourite colour?
- Who is your favourite actor?
- What was your high school locker combination?
- What was your first pet’s name?
Challenge Questions – Some Examples Revisited

Consider the following examples *(with my, subjective, assessment)*

- **What is your mother’s maiden name?**
  - Usability **HIGH**  
  - Security **LOW**

- **What is your favourite colour?**
  - Usability **MED**  
  - Security **LOW**

- **Who is your favourite actor?**
  - Usability **MED**  
  - Security **MED**

- **What was your high school locker combination?**
  - Usability **LOW**  
  - Security **HIGH**

- **What was your first pet’s name?**
  - Usability **MED**  
  - Security **MED**
Challenge Questions – Usability and Security Analysis

Did you agree with the usability and security ratings on the previous page?

Security

- 'Observability' levels are often subjective

Usability

- Often depend upon context and environment, e.g. user base, user experience, guidance to users
- Requires empirical evidence
Evaluating Usability

- Typically performed through experiments or on live systems where real data can be analyzed.
- Experiment participants register questions and answers, and are asked to return later to repeat original answers.
- Keys to running a good experiment:
  - Must solicit *real* information from participants.
  - Need at least one week to test long-term memory.
  - Need much longer to test 'favourite' variations over time.
- Recent experiments suggest that the answers to challenge question are not well-recalled by users.
Evaluating Security

- Use experiments to collect real data
- Blind guess
  - Attacker knows no information about the user or question
  - Attack difficulty proportional to answer length
- Focused/Statistical guess
  - Attacker knows the challenge question
  - Attack difficulty proportional to size of answer space
- Observation guess
  - Attacker knows information about the user
  - Attack difficulty proportional to availability of information
Evaluating Security (cont'd)

- Example analysis: Blind guess
  - Entropy of answer can be measured, given its length
  - Used as an estimate of work required to attack answer
  - Count the number of 8-character answers
    - $26^8 \approx 2^{37.6} \rightarrow 37.6$ bits of entropy?
    - But this is all combinations of characters
  - Shannon told us 1.5 bits of entropy (per character), based upon his computations on long strings of text
  - But for strings of 8 characters or less, he suggested 2.3 bits/char
  - Approximate entropy of 8-char answer: $2.3(8) = 18.4$ bits
  - Comparison: A 6-char alphabetic password has $52^6$ possibilities, giving 34.2 bits of entropy per character
Challenge Questions – Practice and Theory

Many implementations exist

Very little academic research performed

Result

- Implementations have various interfaces
- Various functionality
- Likely inconsistent security protection
- Likely inconsistent usability (applicability, memorability, and repeatability)
Challenge Questions – Future Research

Is there an advantage to either administratively chosen or user chosen questions?

- Yes, but only for some people

Are there particular types of questions that are better to use versus others?

- Classes of information
- Different questions for different people
References


**Recommended Reading**: SOUPS paper (available online)