9 February 2009
Guest Lecture by Mike Just
Introduction

Who am I?

- Mike Just
- Visiting Research Fellow, School of Informatics
- Researching security and usability of “knowledge-based authentication” with David Aspinall
- Continue to work (part-time, remotely) for Canadian Government investigating innovative technology
- Received Ph.D. from Carleton University in 1998
- Home: Ottawa, Canada
Before beginning today's lecture, we will perform Stage 2 of our Experiment.

Details are provided in the handout.

To participate, you must have completed Stage 1, and have your sealed envelope with you today.

The experiment is voluntary – you can choose to not participate, or to withdraw at any point.

At no time will you be asked to submit any personal information.
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)
- We do know that reduced usability can also reduce security – System designers must find the balance between usability and security
And the design environment isn’t easy ...

- “[These devices] 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 and Usability

- Authentication is the process of confirming someone as authentic

- Three information types for authenticating
  - Something you have
    - Mobiles, smartcards, ...
  - Something you are
    - Biometrics – physical characteristics, involuntary actions
      - Fingerprint, facial recognition, voice recognition, ...
  - Something you know
    - Password, PINs, passphrases, ...
Authentication and Usability (2)

- Authentication information has a “lifecycle”
- Security and usability should be addressed at each stage

Issuance and Maintenance
- Stage at which information is created, issued, updated or retired

Use
- Stage at which information is used to authenticate
Some Security & Usability Principles

- Some Usability Principles
  - Limit amount of physical interaction
  - Limit human processing and learning requirements
  - Limit memorization requirements
  - Limit number of seemingly artificial constraints
  - Limit excessive update requirements
  - Limit requirements for perfect accuracy
- Security should not interfere with the task of the user
- Security often strains these usability limits
  - Especially when using "something you know"
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
  - Dozens of accounts with passwords
- And they're not even considered terribly secure today!
- 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?

Example Questions not necessarily from this class' experiment.
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

- **Observability**
  - The security level is inversely proportional to an attacker’s ability to find the answer to a given question
  - “Attackers” might be strangers, acquaintances, colleagues, friends, family members
(Re-)Consider the following examples

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

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

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

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

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

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Information Available to Attacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blind Guess</td>
<td>Attacker knows alphabet used for answers and its frequency distribution</td>
</tr>
<tr>
<td>Focused Guess</td>
<td>Attacker also knows the questions used and can typically determine possible answers and their frequency distribution</td>
</tr>
<tr>
<td>Site-Specific Guess</td>
<td>Attacker can glean some information from the site which the authentication is protecting</td>
</tr>
<tr>
<td>Personalized Guess</td>
<td>Attacker can determine personal information about the user; either the answers themselves, or information that further reduces the set of likely answers</td>
</tr>
</tbody>
</table>
Challenge Questions – Security Revisited (2)

- **Blind Guess**
  - The *entropy* of $X$ is the amount of information conveyed by $X$, or equivalently, *uncertainty* in $X$
  - Let $X$ take on values $x_1, x_2, ..., x_n$ with respective probabilities $p_1, p_2, ..., p_n$
  - $H(X) = - \sum_{i=1}^{n} p_i \log(p_i) = \sum_{i=1}^{n} p_i \log(1/p_i)$
  - E.g. With $n=8$, and uniformly distributed $x_i$ ($p_i=1/8$), $H(X)=3$
  - E.g. Password consisting of 8 8-bit ASCII characters
    - *Actual* password size of $(2^8)^8 = 2^{64}$. Or 64 bits to encode.
    - *Effective* size of $(62)^8 \sim 2^{48}$. Or 48 bits to guess. (Upper/lowercase, #'s)
    - The 'effective size' is not a minimum! For example, the above calculation assumes a uniform distribution of passwords, which is not the case in reality.
Challenge Questions – Security Revisited (3)

- **Blind Guess (cont'd)**
  - E.g. Answer consisting of 8 8-bit ASCII characters
    - Answers usually normalized to use 26 lowercase characters only
    - *Effective* size of \((26)^8 \sim (2^{4.7})^8 \sim 2^{38}\). Or 38 bits (4.7 bits of entropy per character)
    - But, this assumes uniformly distributed/chosen characters to form answers
    - *Answer space* is the English language, reducing the uncertainty (dictionary attack)
    - *Effective* size of \(2.3(8) = 18.4\) bits of uncertainty (according to Shannon)
  
- **How many bits are needed to prevent attacks?**
  - That depends upon which attacks (risks) you're trying to mitigate
    - *Online attacks* can be mitigated by limiting the number of authentication attempts. However, *offline attacks* allow for many, many more guesses.
    - *Random attacks* (compromise any account) allow many guesses spread across multiple accounts. *Targetted attacks* focus on a specific user account so are limited by online/offline constraints (but introduce personalization to attack)
    - But 20 bits is not enough ...
Challenge Questions – Security Revisited (4)

- Focused Guess
  - Knowing question gives further reduction in uncertainty (and questions are effectively public)
  - E.g. ”What was my first pet's name?”
    - http://www.babynames.com/Names/Pets/ gives the top 200 names for dogs and cats
  - Some questions simply suggest very low entropy answers, e.g. ”What religion is my father?”, ”Favourite colour?”

- Site-Specific Guess
  - Dependent upon the site, one can sometimes learn the likely gender, age range, interests, place of residence of users
  - E.g. ”First album bought?”, ”Who is my favourite actor?”

- Personalized Guess
  - Only necessary once previous attacks have been exhausted
  - ”Mother's Maiden Name” is often easy to determine from public records

Example Questions not necessarily from this class' experiment.
There's been very little study of the memorability of authentication credentials, especially challenge questions.

We hope to learn more from our experiments.

Some observations:
- Older users have difficulty remember "first time" events.
- "Favourites" can change over long-term.
- Questions that are "disguised" to be more secure, can also be less memorable.
Other Options for Authentication

- Graphical text passwords
- Consider familiar password process, where temporal order is tied to position
  - password: G _ _ _ _
  - password: G o _ _ _
  - password: G o p _ _
  - password: G o p h _
  - password: G o p h e
  - password: G o p h e r
- No link input position to temporal order
  - password: _ _ G _ _ _
  - password: _ _ G o _ _
  - password: _ p G o _ _
  - password: _ p G o h _
  - password: e p G o h _
  - password: e p G o h r
- Other memorable passwords possible
  - E.g. reverse, rotation, even-then-odd, outside-in
- Secure? Usable?
Other Options for Authentication (2)

- Password is (2,2)(3,2)(3,3)(2,3)(2,2)(2,1)(5,5)
- '(5,5)' is 'pen up'
Other Options for Authentication (3)
Other Options for Authentication (4)
Security and Usability – Final Thoughts

- Security authentication with information (passwords, challenge questions) requires
  - Sufficient information – But this impacts memory
  - Minimal constraints – But this impacts processing
  - Accuracy – But this impacts memory & processing

- Seems daunting!
  - Current solutions simply don't have a sufficient balance between security and usability
References

- SOUPS, CHI and HCI conferences for peer-reviewed papers
- Questions?
  - mike.just@ed.ac.uk
'Something You Have' – Security and Usability Considerations

- Issuance and Maintenance
  - Often requires physical interaction (e.g. In-person, mail)
  - Security: In-person registration, using 'physical' credentials for identification
  - Usability: Physical interaction required, but little processing or memory

- Use
  - Security: Prevent duplication or impersonation
  - Usability: No requirements placed on human memory, but human-card-machine interface issues, e.g. “Which way do I insert the card?”
'Something You Are' – Security and Usability Considerations

- **Issuance and Maintenance**
  - Requires physical interaction to collect biometrics
  - Security: In-person registration, using 'physical' credentials for identification
  - Usability: Physical interaction required, but little processing or memory
  - Limited options for renewal due to finite set of biometrics

- **Use**
  - Security: Prevent duplication or impersonation
  - Usability: No requirements placed on human memory, but human-machine interface issues, e.g. Not all have readable fingerprints
'Something You Know' – Security and Usability Considerations

- **Issuance and Maintenance**
  - Can (and typically do) perform online
  - Security: Relies upon online identification information
  - Usability: Ability to follow rules (length, capitalization, ...), and create something secure and memorable
  - Security/Usability: Typically prevent re-use of previously-used information

- **Use**
  - Security: Very dependent upon user memory capabilities
  - Usability: Memory recall of credentials