Account Recovery – Authentication's Dirty Secret?

Mike Just
University of Edinburgh
28 May 2009
Managing Online Presence

- Many accounts
- Different interfaces
- Too much information
- Too many passwords
- Frequent updates
- A challenge to effectively manage
Managing Online Presence

• Actual presentation included more than a dozen slides demonstrating the online presence of the presenter. For privacy reasons, these have not been posted. Contact the presenter directly to see the full presentation.
Why so many Accounts?

• I do different things with different people
• Used for
  – Storing information
  – Sharing information
  – Receiving information
  – Communicating information
  – Collaborating with others
  – Learning, Teaching, Living
• Used with colleagues, friends, family, ...
What do Accounts want from Me?

• Information, information, information

• Why?
  – Help me store, share, communicate, …
  – Improve my online experience
  – Ensure controlled access to my account
  – Market to me, e.g. advertise
  – Share my information with others
What do Accounts want from Me?

• Information, information, information

• Why?
  – Help me store, share, communicate, …
  – Improve my online experience
  – Ensure controlled access to my account
  – Market to me, e.g. advertise
  – Share my information with others
Account Properties

Security

Usability

Privacy
Account Properties

Security

Stop “bad guys”

Help for yourself

Usability

Privacy

Control “good guys”

Protection vs Control vs Convenience ...
Identification and Authentication

Registration

Identification → Initialize Authentication → Initialize Recovery → Regular Authentication → Account Recovery
Identification and Authentication

Registration

- Identification
- Initialize Authentication
- Initialize Recovery

- If required, user will identify themselves to register
  - Required by banks, work accounts, etc.
  - Identification may rely on shared information, e.g. financial
  - Information might rely upon third-party info, e.g. credit bureaus

- Typical Internet sites don't require identification
  - GoogleMail, Hotmail, Facebook, Twitter
  - Only ensure that only you can authenticate later
Identification and Authentication

Registration

• User chooses 'User Identifier' and authentication credential
  – Typically a password
  – To be used for 'Regular Authentication'
  – Policy often establishes 'password rules'
Identification and Authentication

Registration

- Identification
  - Initialize Authentication
  - Initialize Recovery

  • If needed, user will submit information for later recovery
    - Used in case of forgotten password
    - Often comprised of a set of challenge questions and answers
  • Alternatively, user could be required to (re-)identify
    - Assumes there is shared information for identification
    - Can be costly if initial identification was in-person
Identification and Authentication

Registration

- Identifier and credential (e.g. password) used routinely for authentication
- Policy may require periodic update of credential, e.g., monthly
Identification and Authentication

Registration

- If regular authentication credential is “lost” or “forgotten”, user can still recover their account
  - Often important to retrieve stored information
- User asked to answer one or more of their challenge questions
  - Alternatively, might re-identify
- May also have to follow a re-directed email
Account Recovery with Challenge Questions

Source: http://xkcd.com/565/
Account Recovery with Challenge Questions

• “What is my Mother's Maiden Name?”
• “What was the name of my first pet?”
• “What was the name of my first school?”
• “Who is my favourite actor?”
• “Where did I spend my honeymoon?”
Account Recovery with Challenge Questions

Authentication Credentials

'Something You Have'
- Access card
- Smartcard
- Mobile

'Something You Are'
- Fingerprint
- Iris/retinal scan
- Facial scan

'Something You Know'
- Passwords
- PINs
- Images

'Something You Memorize'

'Something You Already Know'
- Challenge questions
- Images
Account Recovery with Challenge Questions

Sarah Palin Hack an Example of Password Recovery Backfire

By: Brian Prince
2008-09-19

There are 10 user comments on this Security story.

The ease with which Republican vice presidential candidate Sarah Palin’s e-mail was hacked is striking and underscores the importance of improving privacy questions for password recovery. A person claiming responsibility for the hack posted details of what he did Wednesday on a 4chan.org message board. The handle of the poster has been linked to the 20-year-old son of Tennessee Democrat Mike Kornell.

Perhaps the most unsettling thing about the hack on Republican vice presidential
Account Recovery with Challenge Questions

Whowroteit? Mystery advertisement has readers and netizens fascinated
Tracks appear to lead back to a Russian businessman with plenty of money to spare

By
Account Recovery with Challenge Questions

Twitter porn-name game sparks privacy warning

May 15, 2009 04:30 AM

Comments on this story (5)

NICOLE BAUTE
STAFF REPORTER

Twitterers twittering into the great abyss should be careful about the games they play, Canada’s privacy commissioner warned this week after catching on to a new trend.
Account Recovery with Challenge Questions

• Ubiquitous use of challenge question authentication
• Very little published research as to whether it's
  – Usable
  – Secure
  – Privacy-friendly
• For remainder of this presentation
  – Recent research results
  – Best practices for challenge question authentication
Challenge Question – Recent Research

- Rabkin (2008)
- Schechter et al. (2009)
- Just & Aspinall (2009)
Challenge Question – Recent Research


• Security analysis of challenge questions used by 20 US banks
• Result
  – Many questions found to provide low security
Challenge Question – Recent Research

- Security and usability analysis of challenge questions used by Microsoft, Yahoo!, Google

- Results
  - High rates of successful guessing by friends, acquaintances
  - High rate of users unable to recall their answers
Challenge Question – Recent Research

- Security and usability analysis of 500 user-chosen challenge questions

- Results
  - Most questions were insecure
  - High rate of users unable to recall their answers
Challenge Question – Recent Research

• What does these results mean?
  – There are serious questions for the security and usability of authentication with challenge questions
  – Partially due to increased information availability

• However,
  – This verdict is for current implementations
  – Some improvement possible with improved guidance and tools

• And the research continues ...
Challenge Questions – Usability

Three criteria to assess usability

• Applicability
  – How widely applicable is the given question?

• Memorability
  – How easy is it for the user to recall the answer?

• Repeatability
  – How accurately can the answer be replayed, without syntactic or semantic ambiguity?

**What was your first pet's name?**

**What was my high school locker combination?**

**Street vs Avenue**

**Favourites**
Challenge Questions – Security

Increasing Information for Attacker

Answer alphabet and distribution, common answer sets

Questions, distributions of likely answers

User account, published data, social networks, friends, family, ...

Attack Modes

Blind Guess

Focused Guess

Observation

Answer Guess
Challenge Questions – Security

Three criteria to assess security

• Length of answers
  – Helpful when dynamically assessing user answers
  – Can't force longer answers, but can ask multiple questions

• Size of answer space
  – Can “filter out” obviously small questions
  – Can measure others

What's my favourite colour?
Too few possibilities!

What's my best friend's last name?

Only $10^5$ in US (2000)
Challenge Questions – Security

• Observability of answers
  – Subjective assessment
  – Known to friends or family?
  – Obtainable by strangers?
    • Public records, social networks, physically observable, ...

Recall earlier web examples
Challenge Questions – Privacy

• Is the information being asked, too sensitive?
  – Does it reveal overly personal beliefs, preferences, ...

• Some questions might be particularly sensitive to one culture, more than others
  – Religion, politics, relationships, …

• Can be difficult to balance between information that is private (known only to a user), personal (memorable to user), but not sensitive
Other Considerations

• Number of questions to ask
  – Recent research suggests more than one question/answer required
  – More 'entropy' for an attacker to have to guess
  – Can also help to increase difficulty of Observation attack
  – User might register 3-4 questions and answers, and is required to answer at least 2 questions at authentication
  – For Government of Canada solution, users registered 3 questions and answers, and were asked all 3 at recovery
Other Considerations ...

• To '*' or not to '*'
  – What was my first school's name? ************
  – What was my first school's name? St. James IV

• Use of '*' can limit effectiveness of “shoulder surfing” attacks

• But, use of '*' can make entering of answer difficult

• If we assume that questions are rarely used (only for recovery), then shoulder surfing may be less of a concern
  – For Government of Canada solution, we did not use '*''s, and thus opted for improved usability whereby users see what they type
Other Considerations ...

- Normalization of answers
  - Is the answer “John Carter” = “john carter” = “johncarter”? 
  - Is the answer “St. James” = “St James”?

- Unlike with passwords, capitalization and punctuation locations are very predictable with answers
  - Thus offering little to improve security
  - Recent research shows users have difficulty with consistent capitalization

- For Government of Canada solution, answers were normalized to remove capitalization and punctuation
Other Considerations ...

- System-generated versus user-generated questions
  - Users can choose unique, secure questions
  - However, users will also often choose very insecure questions
  - For Government of Canada solution, we used one system-generated question, and two user-generated questions

- Complementary security measures
  - Email a recovery link to the user
Conclusion

• When passwords are forgotten, we rely upon known information to authenticate
• A risky proposition, since this information is often more widely known than we would like
• Usability – Security – Privacy
• Improved practices and further research are required
Further Information

• Other presentations, research publications, at

• Email: mike.just@ed.ac.uk