Personal Choice and Challenge Questions: A Security and Usability Assessment

16 July 2009

Mike Just
University of Edinburgh
(joint work with David Aspinall)

Challenge Question Authentication

- Authentication credential is answer from a question-answer pair
- Common questions
  - *”What is my Mother's Maiden Name?”*
  - *”What was my first pet's name?”*
  - *”What was the name of my primary school?”*
- Often, though not always, used for secondary authentication
- Answers rely upon information that is *already known*, as opposed to *memorized*
- A.k.a. ”Personal Verification Questions,” ”Recovery Questions”

Recent Research Results

- Rabkin, *SOUPS 2008*
  - Subjective assessment of 20 banks with ~200 challenge questions
  - Security: Guessable (33%), Auto. Attackable (12%), Attackable (-)
  - Usability: Inapplicable (50%), Ambiguous (32%), Not memorable (13%)
- Just and Aspinall, *Trust 2009*
  - Pilot experiment (paper-based) collecting questions and answer lengths
  - Security: Answers susceptible to brute-force attack (based upon length)
  - Usability: Not memorable (25%) including Ambiguous (5%)
- Schechter, Berheim Brush and Egelman, *IEEE Oakland 2009*
  - Experiment to study questions from AOL, Google, Microsoft and Yahoo!
  - Security: 17% of answers guessable by arms-length acquaintances
  - Usability: 20% of users forget their answers within 6 months

Our Research (1 of 2)

- Research suggests significant problems with both the security and usability of challenge question authentication systems
  - How can we begin to improve?
- A systematic and repeatable way to analyze the security and usability of challenge questions
  - To continue to assess current systems, and suggest improvements
  - To allow assessment of future systems
- Our focus was on user-chosen questions
  - Does personal choice encourage increased security and usability?

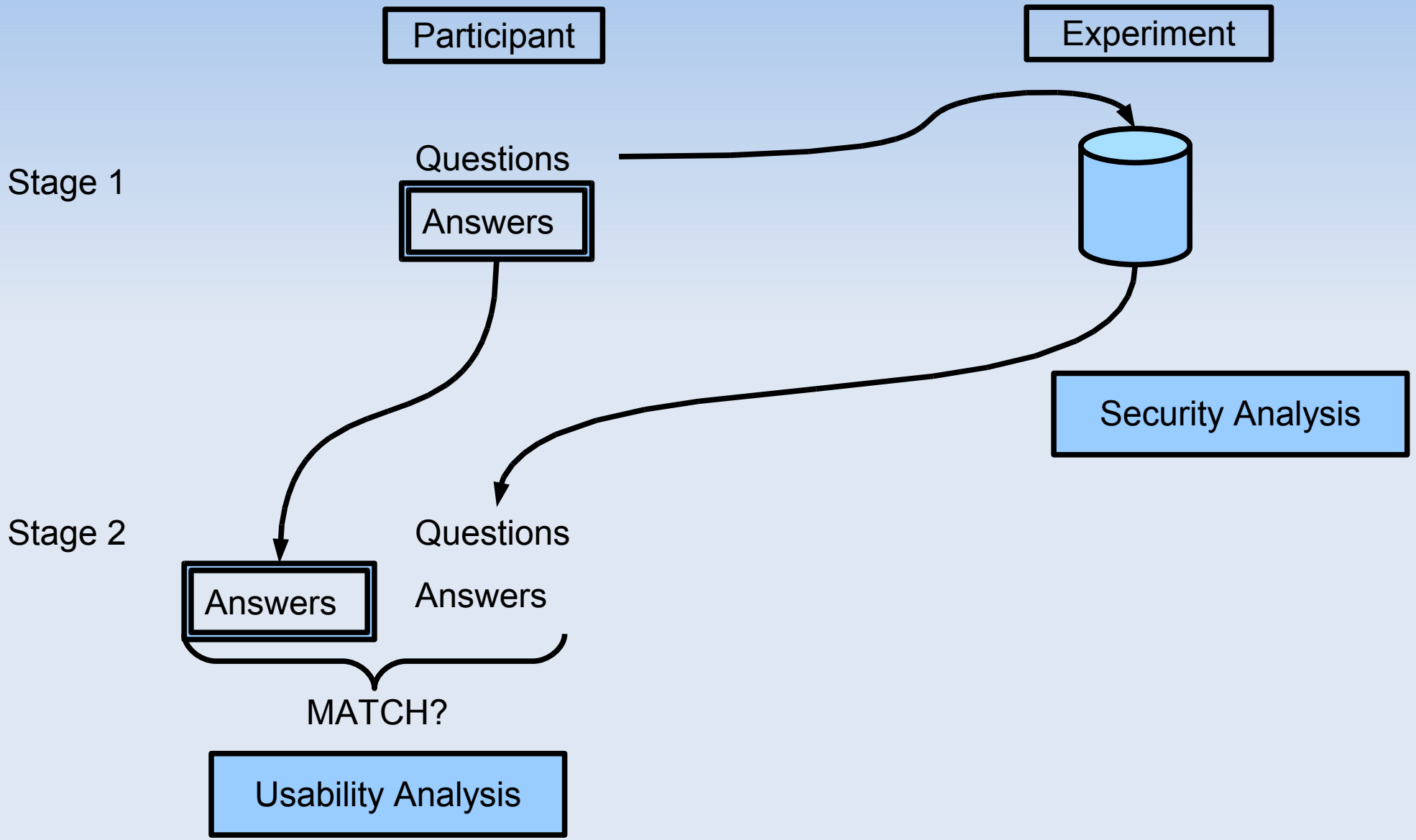
Our Research (2 of 2)

1. Novel experiment for collecting authentication information
2. Security model for question assessment
3. Assessment of the security and usability of 180 user-chosen challenge questions
   - Experiment with 60 first-year Biology students at the University of Edinburgh

Collecting Data (1 of 3)

- Ethically challenging, but users readily submit
- Issues regarding participant behaviour
  - Sensitivity to challenge question answers?
  - Contribute *real* information?
  - Degree of freedom with user-chosen questions
- Opportunities for improved Collector behaviour
  - Challenge to ourselves: Don't collect!
  - Avoid having to maintain information
  - Consistent message: Keep credentials to yourself!

Collecting Data (2 of 3)



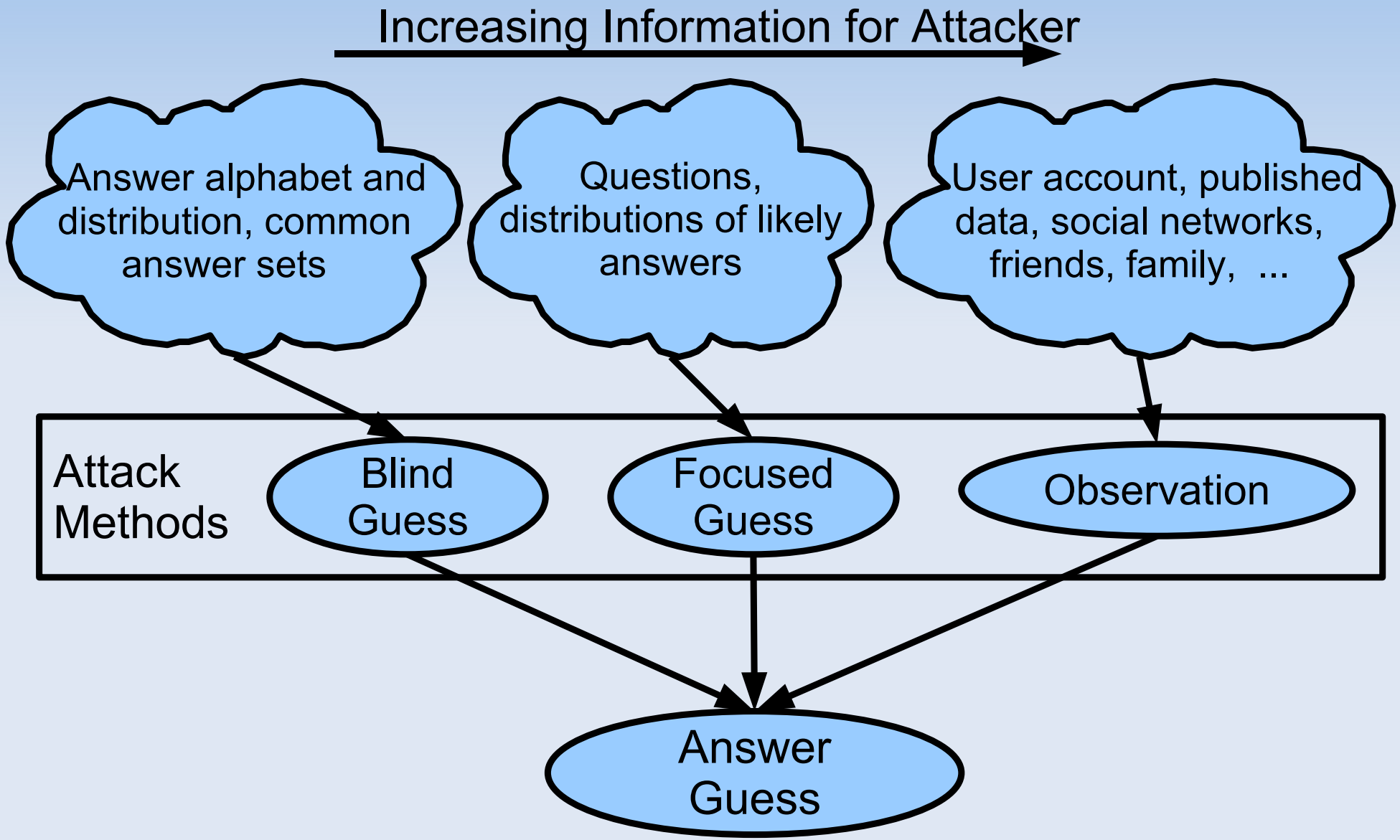
Collecting Data (3 of 3)

- Participants use of 'real' Questions and Answers
  - We asked if participants would use same Questions and Answers in real applications (e.g. Banking)
  - Of the respondents (94%) indicating that they would likely re-use their questions, 45% indicated some influence from not submitting their answers
- Participants and personal privacy
  - We asked participants if they would be concerned if their friends or family members knew their Questions and Answers
  - More than two-thirds of the questions raised 'no concern' at all for participants with < 10% meriting strong concern
- Results are similar to our earlier pilot experiment (*Trust 2009*)

Security Model (1 of 2)

- Existing security analysis of Challenge Questions is ad hoc
- There are no clear guidelines for choosing 'good' questions and answers
- We wanted a more systematic and repeatable approach that would
  - Provide some guidance for secure design
  - Allow continued assessment of new solutions
- We encourage further refinement of our model
- Assessment results depend upon context

Security Model (2 of 2)



Security Analysis – Blind Guess (1 of 5)

- Brute force attack
- Security Levels based on equivalence to passwords
  - 6-char alphabetic password (2^{34})
  - 8-char alphanumeric password (2^{48})

Low (2^{34}) Med (2^{48}) High

- Answer entropy: 2.3 bits (1st 8 chars), then 1.5 bits
- Results (by question)
  - Average answer length: 7.5 characters
  - 174 Low, 4 Medium, 2 High
- Results (by user)
  - Q1 – 59 Low, 1 Medium, 0 High
  - Q1, Q2 – 38 Low, 13 Medium, 9 High
  - Q1, Q2, Q3 – 5 Low, 19 Medium, 36 High

Security Analysis – Focused Guess (2 of 5)

- Attacker knows the Challenge Questions
- Security Levels same as for Blind Guess
- Answer types and space →
- Results (by question)
  - 167 Low, 0 Medium, 13 High
- Results (by user)
  - Q1 – 58 Low, 0 Medium, 2 High
  - Q1, Q2 – 46 Low, 11 Medium, 3 High
  - Q1, Q2, Q3 – 5 Low, 28 Medium, 27 High
- Much room for refinement of 'Space'

Q Type	%	$\log_{10}$Space
Proper Name	50%	4 – 5
Place	20%	2 – 5
Name	18%	3 – 7
Number	3%	1 – 4
Time/Date	3%	2 – 5
Ambiguous	6%	8 – 15

Security Analysis – Observation (3 of 5)

- Attacker tries to obtain or observe the answer
- Security Levels defined qualitatively
  - Low – Answer publicly available
  - Medium – Answer not public, but known to F&F
  - High – Neither
- Levels assigned to questions by
  - Subjective analysis, and
  - Participant input (provided upper bound only)
- Results (by question)
  - 124 Low, 54 Medium, 2 High
- Results (by user)
  - 24 Low, 34 Medium, 2 High
  - Did not ”sum” levels (used max)
- Much room for refinement of levels and analysis

Security Analysis – Overall (4 of 5)

- Overall rating is a 3-tuple (Blind, Focused, Observation)
- Results
  - All Low – 1 participant
  - All High – 0 participants
  - No Lows – 31 participants (50%)
  - (H,M,M) or (M,H,M) – 15 participants (25%)
  - (H,H,M) – 11 participants (20%)
- Dependencies not (yet) considered
- Ability to perform observation attacks in parallel, and offline, is a significant advantage for attackers

Security Analysis – Overall (5 of 5)

- Perceived effort of Stranger to Discover Answers
  - Very difficult (47%)
  - Somewhat difficult (42%)
  - Not difficult at all (11%)
  - Users overestimate the difficulty of attack
- Perceived effort of Friend/Family to Discover Answers
  - Very difficult (11%)
  - Somewhat difficult (36%)
  - Not difficult at all (53%)
  - Users surprisingly aware of this risk

Usability Analysis

- Criteria: Applicability, Memorability, Repeatability
- Answer recall (180 questions)
  - 15 errors (8%)
  - Reduces to 7 errors (4%) if we exclude 'capitalization' errors
- Answer recall (60 users)
  - 11 users (18%) made at least one error
  - Reduces to 7 users (12%) if we exclude 'capitalization' errors
- Comments suggest that 'complicated answers' and allowance of free-form answers may be culprit
- Florêncio & Herley (2007) found that 4.28% of Yahoo! users forget their passwords
- Our results were after 23 days, with young students

What Does it All Mean? (1 of 3)

- Serious concerns regarding the security and usability of (user-chosen) challenge questions
  - Questions were similar to system-chosen
- But, before we write-off challenge questions
  - Multiple questions seem to help (security at least), though security challenges remain
  - How do the users who forget their answers relate to those forgetting their passwords (same users?)
  - Are we reducing help-desk costs, relative to not having challenge questions at all?

What Does it All Mean? (2 of 3)

- Current implementations are terribly boring
  - Little research of challenge question authentication
  - Most has been to assess security and usability
  - Less research into new designs
- Potential paths forward
  - Dynamic assessments of security and usability
  - New types of information for authentication (e.g., 5 W's)
  - Other methods: who you know, what you have access to, …
  - Users are different – customize to meet their strengths (no 'one-size-fits-all')

What Does it All Mean? (3 of 3)

- But, how to improve usability ...
  - Fixed-form answers
  - Tolerance for < 100% accuracy
- At the very least, let's properly evaluate new proposals
  - Avoid 'neat technology ideas' that improve security/usability only
  - Cf. yesterday's tutorial
  - Usability: Applicability, Memorability, Repeatability
  - Security: Blind Guess, Focussed Guess, Observation
  - Observation attacks by friends, family, acquaintances, strangers
  - Analysis of answer entropy

Further Information

- Project web site
  - http://homepages.inf.ed.ac.uk/mjust/KBA.html
- Email
  - mike.just@ed.ac.uk