SCOttish Networking Event (SCONE)

Secure and Usable Authentication

10 September 2009

Mike Just
University of Edinburgh

(joint work with David Aspinall)

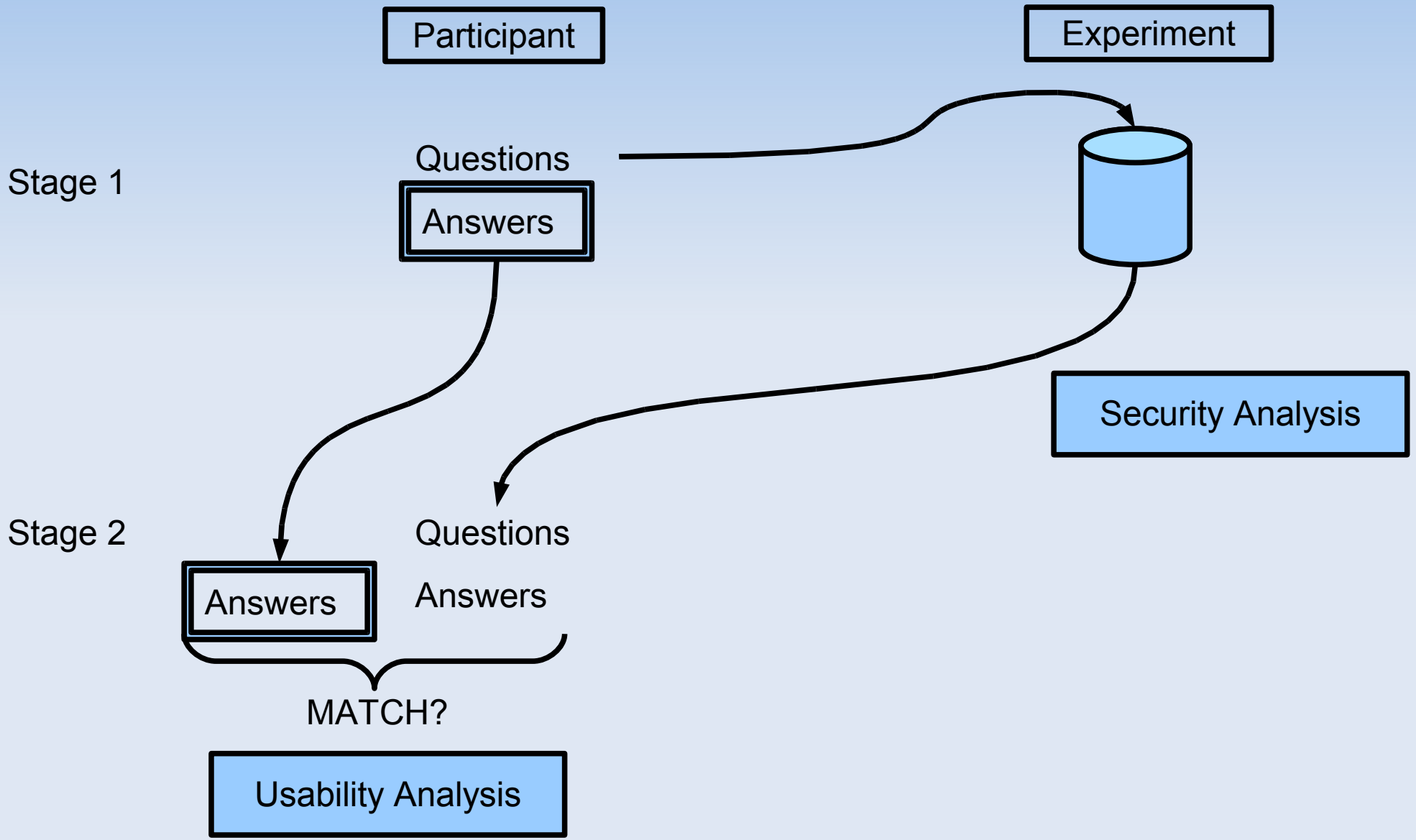
Challenge Question Authentication

- 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”

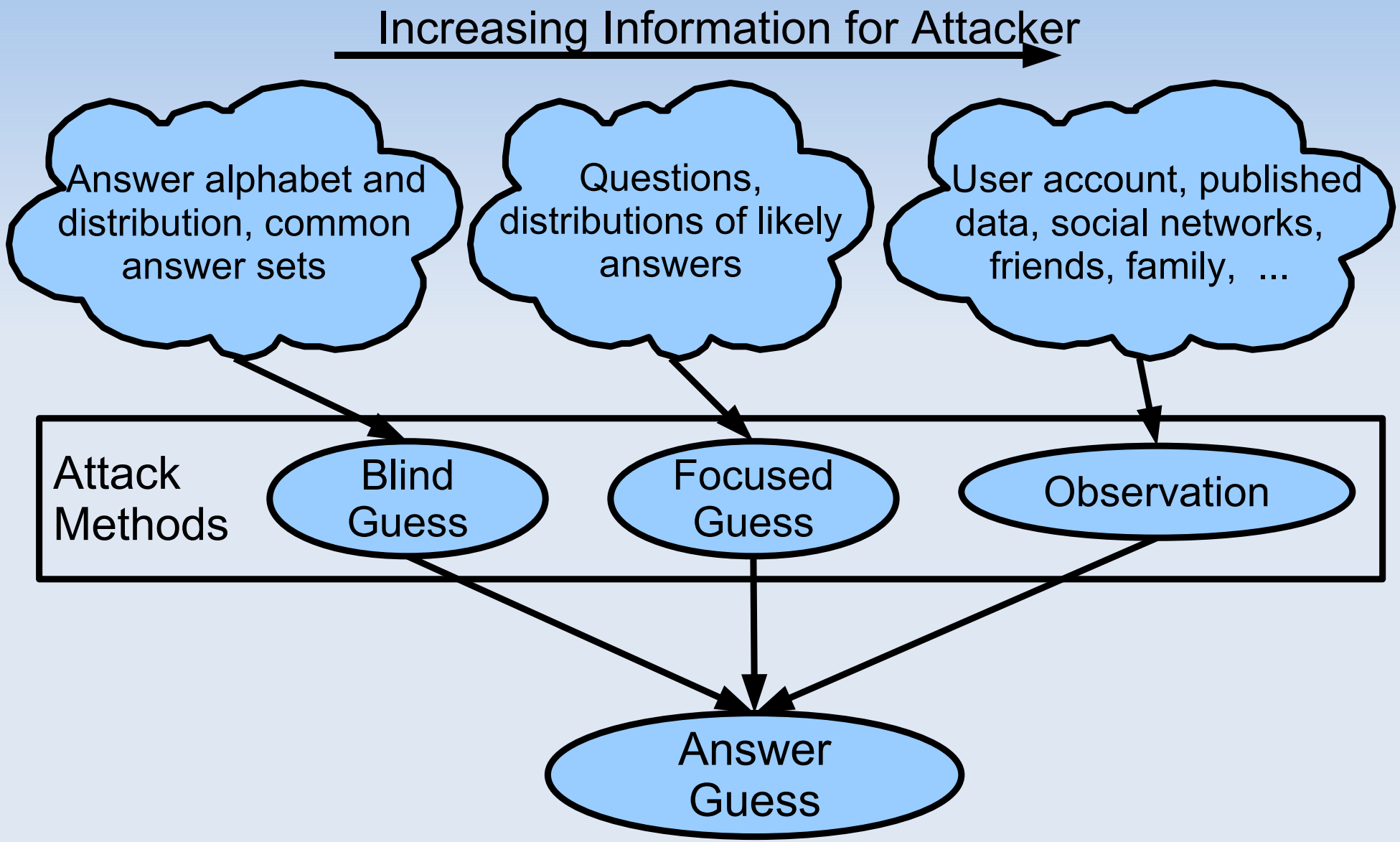
Our Research

- Multi-disciplinary
  - Security (Attacker's Point-of-View)
  - Usability (User's Point-of-View)
- Previous analysis of challenge question authentication has been ad hoc
  - We wanted a systematic and repeatable process
- Lead experiments to collect 500 user-chosen questions
  - Three each from 167 participants
  - Subsequent analysis considers a subset of these questions (180 questions from 60 users)

Collecting Data



Security Model



Security Analysis – Blind Guess (1 of 4)

- 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 4)

- 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 4)

- 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 4)

- 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

Discussion

- Security (and usability) concerns with *current* implementations
- Assessment model can be applied to new proposals
- Two key observations
  - Small variety of questions used
  - User doesn't receive any feedback
- Next steps
  - Tool for Interactive Question Generation
  - Tool for Automated Assessments

Further Information

- Project web site
  - http://homepages.inf.ed.ac.uk/mjust/KBA.html
- Email
  - mike.just@ed.ac.uk
- Interested in connecting with other security researchers