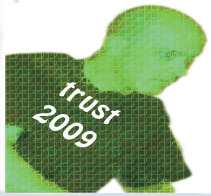
Challenging Challenge Questions

Mike Just and David Aspinall
School of Informatics
University of Edinburgh

Presentation at Trust 2009
8 April 2009
Oxford, UK

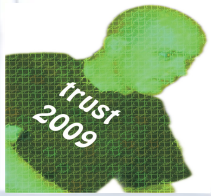
Challenge Question Authentication

- Question-Answer pairs
- Answer is *authentication credential*
- Common questions
  - *"What is my Mother's Maiden Name?"*
  - *"What was the name of my first pet?"*
  - *"What was the name of my primary school?"*
- Typically used for secondary authentication



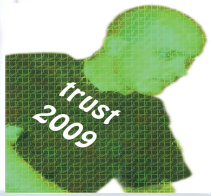
Challenge Question Research

- Interdisciplinary research
  - Security (Attacker's Point-of-View)
  - Usability (User's Point-of-View)
- Very little published research in this area
  - Haga/Zviran (1991), Pond et al. (2000) looked at security, usability of 'word associations'
  - Just (2004) provided security, usability criteria
  - Rabkin (2008) analyzed 20 bank web sites



Our Contributions

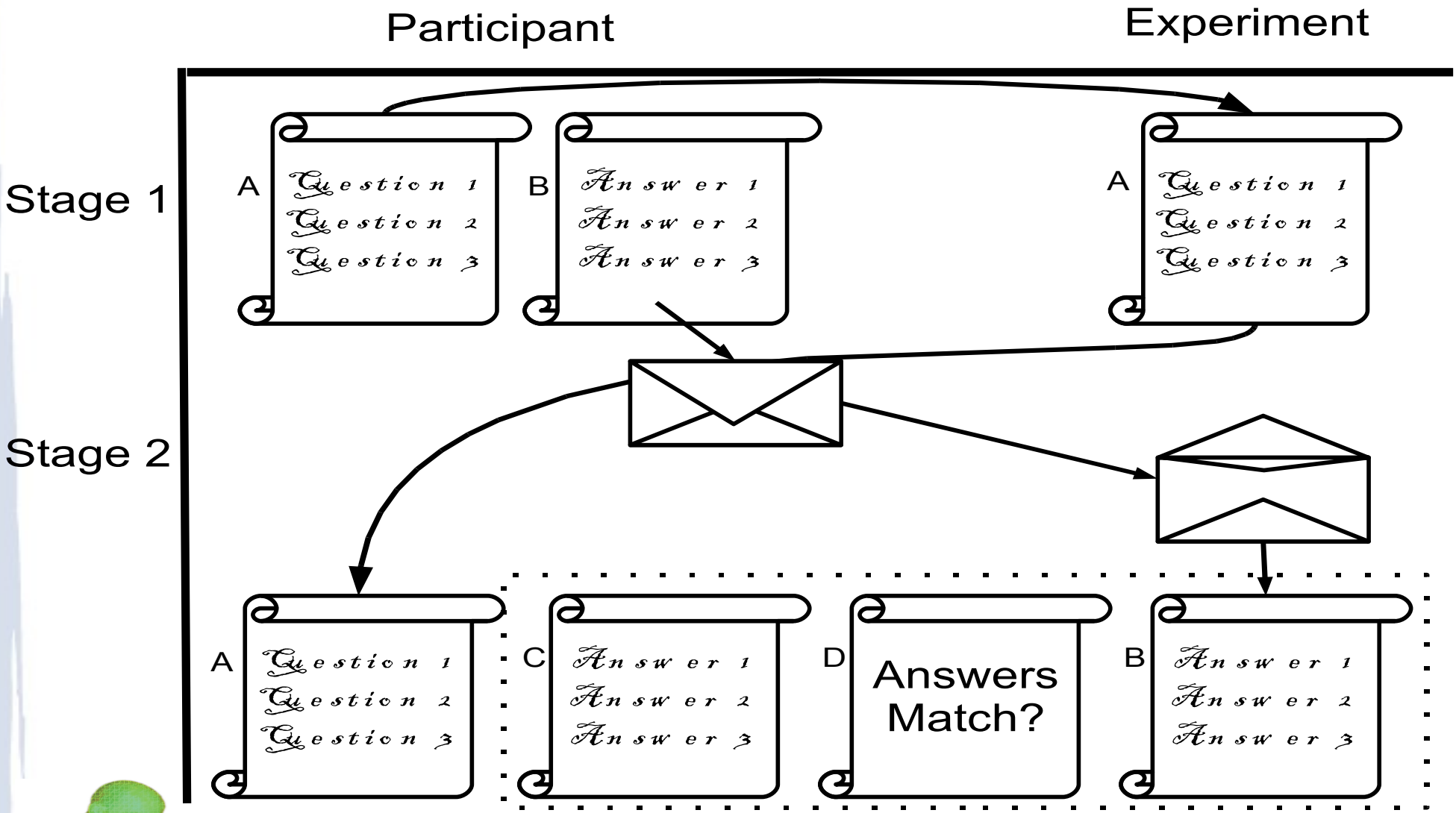
- Experiment and analysis of **user-chosen questions**
- Experiment that **engenders trust** in participants
- Evidence that single-question systems are **susceptible to brute force attack**
- Evidence that user **perception of security does not align** with actual security provided
- Evidence that **answers aren't suitably memorable**



Collecting Private Data

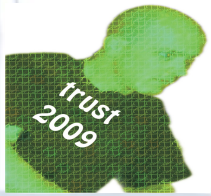
- Ethically challenging, but users readily submit information
- Issues regarding participant behaviour
  - Equate credentials with other private info?
  - Contribute *real* information?
  - Degree of freedom with user-chosen questions
- Opportunities for improved Data Collector behaviour
  - Challenge to ourselves – don't collect
  - Avoid having to maintain information
  - Consistent message – keep credentials to yourselves!

Our Experiment



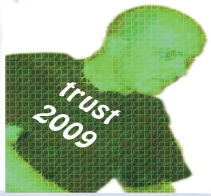
Experiment Results

- Two experiments on University students
  - Stage 1 – 73 participants, 218 questions
  - Stage 2 – 28 days later, 40 participants
- Limited size and demographics, but we can still draw *negative implications*
  - If not memorable for students then likely not memorable for others as well



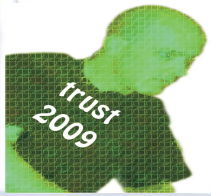
Results – Trustworthy Experiment?

- Likelihood of question re-use
  - 42% Very likely
  - 49% Somewhat likely
  - 9% Not likely
- Did non-submission of answers contribute?
  - 15% Very much
  - 48% Somewhat
  - 37% Not at all
- Tsai et al. (2007) – More privacy emphasis → less sharing
- Our method may contribute to more real input – more research req'd



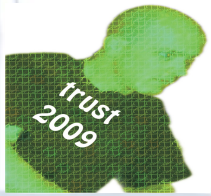
Results – Question Security

- Average answer length: 7.95 characters (Median = 7)
- 8-char answer has only 18.4 bits of entropy
  - Assumes 26 character alphabet, 2.3 bits/char
- Comparison: 8-char password has 45.6 bits of entropy
  - Assumes 52 character alphabet, 4.7 bits/char
- Florêncio and Herley (2007) found that even the weakest sites have passwords of at least 20 bits of entropy
- More than 50% asked for a Proper Name or number



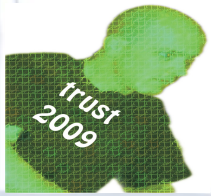
Results – Security Perceptions

- Difficult for stranger to determine answer?
  - 46% Very difficult
  - 42% Somewhat difficult
  - 11% Not difficult at all
- Users overestimate difficulty for attacker
- Might reflect limited 'attack model' for users
  - Users may not understand attacker capabilities



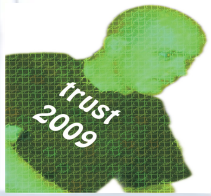
Results – Usability

- Answer recall (by question)
  - 75% recalled exactly
  - 18% with different capitalization, punctuation
  - 7% were different (18% of participants)
    - 3 completely different
    - 5 with 'repeatability' mistakes
- Florêncio and Herley (2007) found that 4.28% of Yahoo! users forget their passwords
- Our results were after 28 days, with young students



Conclusion

- Summary of results
  - New method for collecting data
  - Security of single questions is very limited
  - Security perception of users is misaligned
  - Perfect recall of answers appears problematic
- Future work
  - Potential benefits of multiple questions
  - Alternatives to 'free-form' answers
  - Dynamic assessments of questions and answers



Conclusion (2)

- Related papers
  - Just, Aspinall, “Choosing Better Challenge Questions” (submitted)
  - Schechter, Brush, Egelman, “It's no secret. Measuring the security and reliability of authentication via 'secret' questions.” (IEEE Security & Privacy, May 2009)
- More information
  - http://homepages.inf.ed.ac.uk/mjust/KBA.html