Authentication Frequency (and Continuous Authentication)

Mike Just
Interactive and Trustworthy Technologies Group
Glasgow Caledonian University

SOUPS 2014 – WAY Workshop
9 July 2014
Outline

• Authentication frequency

• Continuous authentication (on mobile devices)
  • Implicit, transparent, data-driven, …
Authentication Frequency

• Typical authentication issues
  • Credential number, size, complexity
  • Duration of each authentication attempt

• Authentication frequency
  • Number of authentication attempts with same credential
  • At one or more accounts
  • Explicit vs. implicit use

• Trade-offs for increased/decreased authentication frequency
Authentication Frequency – Highs and Lows

• High(er) frequency
  • Higher frequency would seem to increase recall
  • SSO: Reduce number of credentials
  • Security
    • Model behaviour \(\rightarrow\) reduce explicit use (e.g., continuous authentication)

• Low(er) frequency
  • Lower frequency (explicit use) would seem to reduce use burden (e.g., saved passwords)
    • But also seems to negatively impact recall (leading to recovery)
  • Continuous authentication supports lower explicit use of credential
Continuous, Data-Driven Authentication

- On mobile devices
- Reduce explicit unlocks
- Multiple sensor input
- More than just location
  - Insider attacks
  - Environment change

See MoST 2014
Time to Train

![Graph showing distance over days for different categories]

- app
- wifi
- light
- magnetic
- rotation
- noise
- sys-load
- usr-load
- global

![Graph showing distance over days for another category]

- app
- bocm
- active
- cal
- charge
- global
Threshold Setting
Usability

- Current activity: usability study
Security

- Initial attacks, based on physical access, and known information
Efficiency

- Adaptive: Based on score changes over time (or other “trigger”)
- Weight and use of sensors in different contexts (time, location)
Final thoughts

• Authentication frequency
  • Increasing/decreasing frequency options
  • Infrequent account access

• Continuous, data-driven authentication
  • Plausible, but further investigation required
  • Current: Further usability and security studies, resource consumption
  • Will users (who currently use PIN/pattern) like a reduction of the number of explicit unlocks?
  • Will users (who DON’T currently use PIN/pattern) now use a solution with a smaller number of unlocks?
  • Will it be sufficiently secure?
  • Will lower frequency of explicit authentication impact memorability?
Email: mike.just@gcu.ac.uk

Joint with Gunes Kayacik, Nicholas Micallef, Lynne Baillie, and David Aspinall (Edinburgh)