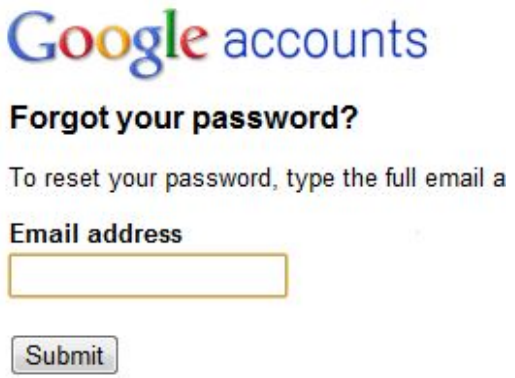
ActivPass: Your Daily Activity is Your Password

Thomas Finelli, Artian Kica,
Evan Gilgenbach

Introduction

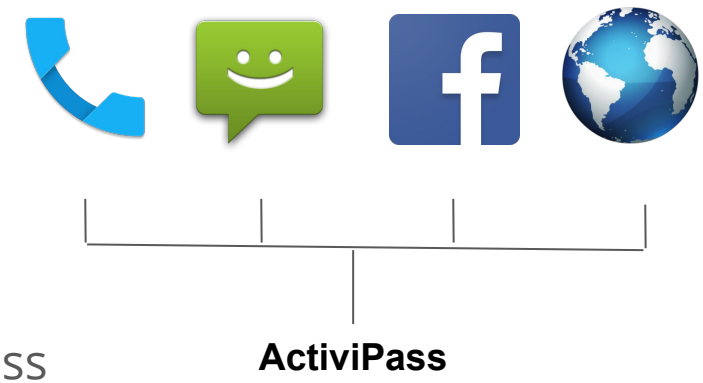
- Authentication through passwords
  - Pros:
    - Secure
    - Simple
  - Cons:
    - Secure passwords are hard
    - Password reuse is common and dangerous
    - Easy to share; also security risk



- Create new authentication method
  - Simple and easy to use
  - Resistant to sharing

Vision

- Authenticate based on user's activity
- Ask user questions about their activity
  - What is the caller's name from the first call you received today?
  - Which news site did you not visit today? (CNN, CBS, BBC, ABC)
- Question generation
  - Call logs
  - SMS logs
  - Facebook activities
  - Browser history
- Use outlier events
  - Typically easy to remember hard to guess

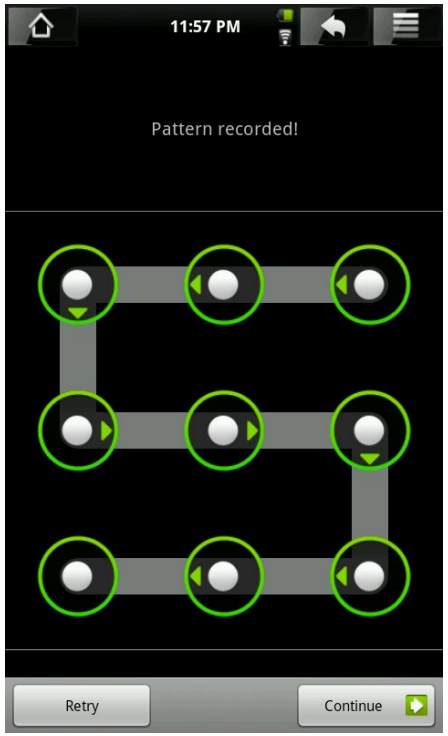


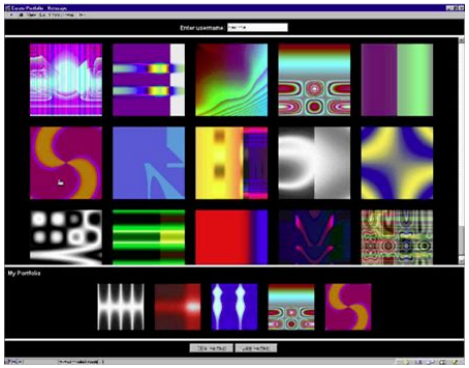
Vision

- Applications
  - Password sharing prevention (Netflix, HBO Go, etc.)
  - Replacement for password hints
  - In addition to regular password
- User can customize
  - Number of questions
  - Question format
  - Activity permissions
- Perform user studies

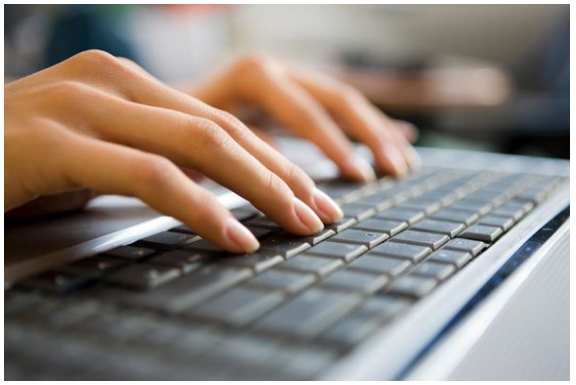
Other Forms of Authentication

- Text Password
  - Easily sharable
  - Security risks if leaked
- Physical Biometric Authentication
  - Face, Fingerprint, Iris, Audio, Gait
  - Security risks if leaked
- Graphical Password
  - Touch predetermined areas or sequences of images





Other Forms of Authentication

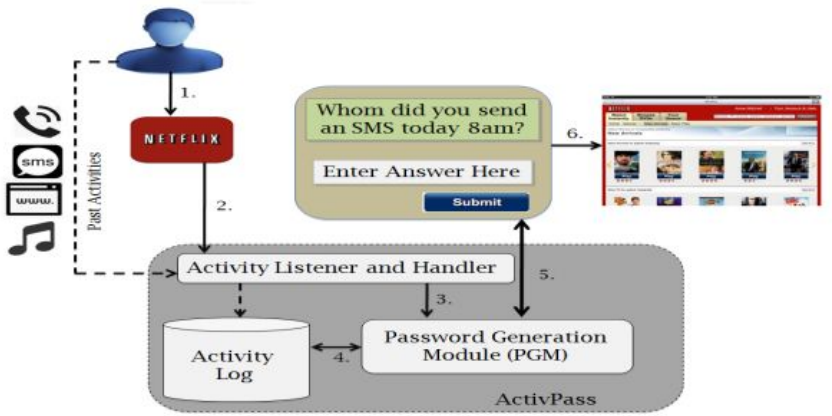


- HCI-based Biometric
  - Input Device Interaction Based
    - Keystroke, Mouse, Haptic
  - Software Interaction Based
    - Email behavior, typing style, game strategy
  - Keystroke pattern based authentication had 50% false acceptance rate
- One Time Password
  - Only works for one session
  - Dynamically Changing password which is based on "*something you have*"
  - Mitigates password sharing by being dynamic

How does ActivPass work?

- Activity Listener runs in the background and logs metadata
  - SMS, calls, web pages, etc.

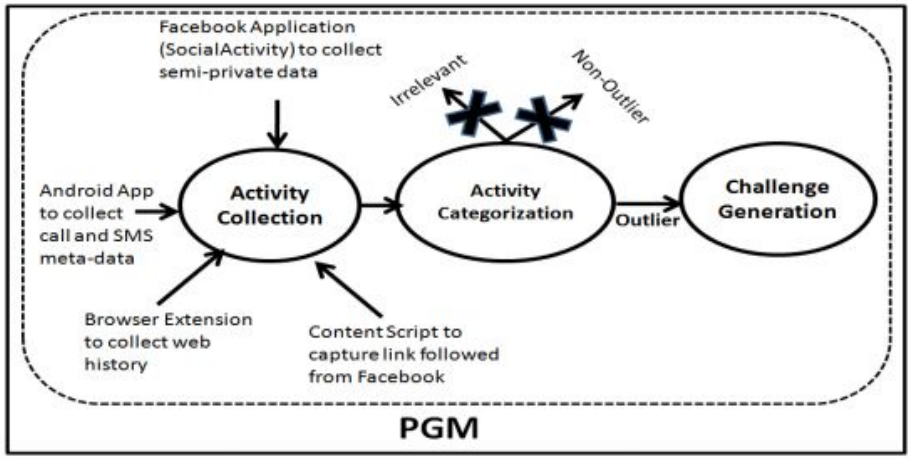
- When user invokes an application:
  - Password Generation Module (PGM) creates *n* password questions based on collected metadata
  - If user can answer *k* correctly, the application is launched



How does ActivPass work?

- Periodically draws logs in order to classify them with an Activity Categorization Module.
  - Attempts to determine “outliers”
    - e.g. Browser homepage vs

      infrequently visited webpage
  - Erases any “irrelevant” logs
    - e.g. Unk



What sort of questions are asked?

	Range of questions asked
Facebook	1) Profiles visited by the user. 2) Groups the user is a member of. 3) A person with whom user had a chat.
Web	1) Titles of the web-pages visited by the user.
Call	1) A person whom the user called. 2) A person who called the user.
SMS	1) A person whom the user sent an SMS. 2) A person who sent an SMS to the user.
Audio	1) The tune/tone used by the user as an alarm. 2) The tune/tone used by the user as her ring-tone. 3) The audio files downloaded by the user.

Source	**Details of data collected**
SMS	Time, Receiver/Sender Name
Call	Time, Type (incoming, outgoing), Name of other person, Duration
Audio	Title of Music added in this week, Alarm tone, Ring tone
Web	URL, Time of visit
Link visited from Facebook	URL, Time of visit
Facebook Group	Name of Private (secret and closed) groups
Facebook Pages	Name of pages created by user
Facebook Profile	Name of Facebook friends of user
Facebook Message	Time (in milliseconds from epoch), Name of other person, Msg Id, Thread Id

Results

- Results came in three stages
- Stage 0 determined feasibility using user-created questions
- Stage 1 determined first-pass numbers from the initial design
- Stage 2 was a re-design that eliminated poorly-performing activities and questions.

Results (cont.)

- Over 50 volunteers given 20 questions:
  - average recall rate: 86.3% ± 9.5
  - average guessability: 14.6% ± 5.7

- Devised Bayesian estimate of challenge given *n* questions where *k* are required

- 95% success rate with 5.5% guessability over 15 volunteers

n	k	Authentic user	Impostor
4	4	0.554	0.0004
4	3	0.906	0.011
4	2	0.989	0.1043
4	1	0.998	0.468
3	3	0.642	0.0031
3	2	0.948	0.0577
3	1	0.996	0.3771
2	2	0.745	0.0213
2	1	0.981	0.2707

Discussion

- Password sharing in a secure threat-model
- Tests against dedicated attackers
- Three Factor Model
- Compares favorably to other non-biometric “something you are” solutions (keystroke)
- Prior Art: Facebook security verification