An Exploration of Geographic Authentication Schemes

Abstract:

We design and explore the usability and security of two geographic authentication schemes: GeoPass and GeoPass-Notes. GeoPass requires users to choose a place on a digital map to authenticate with (a location password). GeoPassNotes—an extension of GeoPass—requires users to annotate their location password with a sequence of words that they can associate with the location (an annotated location password). In GeoPassNotes, users are authenticated by correctly entering both a location and an annotation. We conducted user studies to test the usability and assess the security of location passwords and annotated location passwords. The results indicate that both variants are highly memorable, and that annotated location passwords may be more advantageous than location passwords alone due to their increased security and the minimal usability impact introduced by the annotation.

Existing system:

In Existing system we use GeoPass, in which a user chooses a single place on a digital map as their password. We perform a multi-session in-lab/at-home user...
study of GeoPass involving 35 users over 8-9 days. Our results suggest that GeoPass is highly memorable: none of the returning participants forgot their location passwords after one day. Of the 30 participants who returned to login one week later, only one participant failed to enter their password. There were very few failed login attempts throughout the entire study. Our security results suggest that GeoPass provides enough security to protect against online attacks under simple system-enforced policies. GeoPass may also be useful as a building block for future geographic authentication systems.

**Disadvantage:**

- GeoPass is certainly vulnerable to offline guessing attacks.
- Additionally, GeoPass may offer weak security against online guessing attacks in some circumstances (e.g., if it is deployed in a small city or if the adversary had a method of effectively prioritizing guesses). Thus, prudent implementations of GeoPass should find another way to increase security.

**Proposed system:**

We propose, implement, and evaluate two systems for geographic authentication: GeoPass and GeoPassNotes. We evaluate the systems’ security and usability through two user studies, finding that they both exhibit very strong memorability.
(over the span of 8-9 days, there were only two resets for GeoPass and none for GeoPassNotes). Usability was high in terms of there being few failed logins and user perceptions of the system. Although 67% of the GeoPass users and 80% of the GeoPassNotes users indicated that they could easily use the system every day, we must be cautious about recommending their use on frequently used accounts. Given that the login times for both systems are longer than text passwords, we suggest they would be most appropriate in contexts where logins occur infrequently. For example, it might be useful for infrequently used online accounts or possibly fallback authentication. We found that annotated location passwords have the potential to be stronger than text passwords against guessing attacks when proper policies are applied, thus they may be more desirable for higher-security environments.

Advantages:

- The geographic authentication schemes we explored appear to be highly memorable.
- It would be interesting to explore other ways to harness this memorability while enhancing security. One interesting direction is to explore the extent that the presentation effect can improve security in geographic authentication systems. Another future direction includes
exploring whether the memorability of geographic locations might translate if used in mnemonics for text passwords.

The GeoPass system. The “X” marker represents the user’s password.

Snapshot of the GeoPassNotes interface during note entry.
Hardware Specification:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech
- Ram: 512 Mb.
- MOBILE: ANDROID

Software Specification:

- Coding Language: Java 1.7
- Tool Kit: Android 2.3 ABOVE
- IDE: Android Studio
Reference:


