The Issue

- Traditional authentication consists of username and password.
- Strong security requires stronger passwords.

How do we get stronger passwords?

- Longer passwords with high entropy = hard to memorize passwords.
- Two-factor authentication.
  1. Password + another (temporary) information shared through secondary channel.

And then, more issues

- We navigate and sign-on to several systems in a day.
- We tend to rely more on mobile devices for access.
- Mobile devices = small touch screens, no hardware keyboards.

How can we combine:

- wireless communications,
- two-factor authentication,
- long passwords,
- into an improved user experience with authentication security?

Enter the Location-Aware Sign-on

- Uses location as an authentication factor.
- Uses the consumer mobile device (smartphone) as an agent to perform location-aware sign-on procedures on behalf of the user.
- Uses Attribute-Based Encryption (ABE) to construct a secure key exchange protocol.
- Uses Bluetooth Low Energy beacons to delimit wireless broadcast zones for indoor location.
- Does not require that the mobile device knows, or reports, its present location.

Case scenario: office

The Location-Aware Sign-On at work

- Wireless-delimited broadcast zones, employing Bluetooth Low-Energy beacons, covers an office floor.
- Beacons broadcast ABE encrypted messages (keys) containing access rules.
- If a mobile device within range is able to decrypt the message, then a key exchange follows between mobile device and backend system.
- This is a sign-on procedure done on behalf of the user.

A second authentication step is performed by the user, utilizing a "simpler" factor (a temporary PIN, pattern, or fingerprint) to the backend system.

Highlights

- Our ABE-based key exchange allows access rules (built on attributes) to be encoded within ciphertext itself.
- The messages containing access rules can be broadcast through insecure medium.
- The primary access decision relies on the capacity, of the user, to decrypt the broadcast message (i.e., the user’s attributes).
- The access rules can be changed on the fly.