On the Evolution of Digital Authentication

Patricia Arias-Cabarcos
pariasca@mail.uni-mannheim.de
Password Authentication is dominant, despite...

- **Security problems**
  - Offline/Online Cracking
  - Bad Usage: reuse, common words...
  - Bad Deployments: unprotected storage
  - Phishing, social engineering, spyware, etc.

- **Poor usability**
  - memorize, type, follow complex policies
  - users can’t cope well with passwords

Why?

- Inertia
- Failure of research on convincingly better alternatives

---


The alternatives

- **Implicit AuthN**
  - Continuous AuthN
  - Voice
  - Gait
  - Typing Dynamics
  - App usage patterns
  - Heartbeat
  - Eye-tracking
  - Brain waves

- **Password Managers**
  - Federated AuthN
  - Password
  - PIN
  - Pattern
  - Questions

- **Multifactor AuthN**
  - USB key
  - Smart Card

+ **Usability**

- **Implicit AuthN**

  - Face
  - Iris
  - Fingerprint

+ **Security**

- **Physiological**
  - Biometrics
- **Behavioral**
  - Something you are
  - Something you know
  - Something you have
Which is the best alternative to passwords?
It’s all about context

1. **Location**: Home
2. **Application**: Low Risk
3. **Beacons**: Familiar Device
4. **Light**: Dark

---

1. **Location**: Public Place
2. **Application**: Sensitive, e.g., online banking
Adaptive Authentication: very brief state-of-the-art survey

1 Arias-Cabarcos, P., and Krupitzer, C. "On the design of distributed Adaptive Authentication Systems." WAY Workshop@SOUPS'17.
Adaptive Authentication: very brief state-of-the-art survey

**Observations**

- Variety of authenticators and contexts
- Different metrics/algorithms for selection
- Ad-hoc designs:
  - Hard to extend, re-configure
  - Difficult to reproduce, to compare

---

1 Arias-Cabarcos, P., and Krupitzer, C. "On the design of distributed Adaptive Authentication Systems." WAY Workshop@SOUPS’17.
We need a **Brain** for Adaptive Authentication

Flexible, easy to reconfigure for:
- authenticators
- contexts
- selection algorithms
How to design a **Brain** for Adaptive Authentication

---

How to design a Brain for Adaptive Authentication

How to design a Brain for Adaptive Authentication

How to design a Brain for Adaptive Authentication

Potential benefits

• Independent research on different parts can be merged
  • Authentication mechanisms
  • Decision making algorithms
  • Context fusion

• Faster testing of different configurations for research studies, e.g.:
  • Which combinations of authenticators are more usable?
  • Which configurations are more efficient?

• Easy deployment of adaptive authentication
  • Break “Silos of Authentication”
Challenges & open questions

- SECURITY
- PRIVACY
- USABILITY
Challenges & open questions

- How to improve behavioral biometrics accuracy?
- How to compute contextual risk?
- Analyze new attack vectors, e.g.: simulating lower risk contexts
- Security of distributed components
Challenges & open questions

**SECURITY**
- How to improve **behavioral biometrics accuracy**?
- How to compute **contextual risk**?
- Analyze new **attack vectors**, e.g.: simulating lower risk contexts
- **Security** of **distributed** components

**PRIVACY**
**Orwellian scenarios:**
- Unobtrusive user authentication is privacy intrusive
- Who collects behavioral data and how are they handled?

**USABILITY**
Challenges & open questions

**SECURITY**
- How to improve behavioral biometrics accuracy?
- How to compute contextual risk?
- Analyze new attack vectors, e.g.: simulating lower risk contexts
- Security of distributed components

**PRIVACY**
Orwellian scenarios:
- Unobtrusive user authentication is privacy intrusive
- Who collects behavioral data and how are they handled?

**USABILITY**
- Acceptance: will users trust highly unobtrusive (invisible) authentication systems?
- Trade-offs privacy/usability
Challenges & open questions

- How to improve **behavioral biometrics accuracy**?
- How to compute **contextual risk**?
- Analyze new **attack vectors**, e.g.: simulating lower risk contexts
- **Security** of **distributed** components

**Orwellian scenarios:**
- Unobtrusive user authentication is privacy intrusive
- Who collects behavioral data and how are they handled?
- **Acceptance**: will users trust highly unobtrusive (invisible) authentication systems?
- **Trade-offs** privacy/usability

- How can we measure, fuse, and reason about authenticators’ strength?
- Which are the suitable math constructions for authenticators to operate on data without leaking personal information?
- Which optimization algorithms are suitable for Authenticator selection?
References


On the Evolution of Digital Authentication