

# Observation-Resistant Multifactor Multimodal Authentication

Aleksander F. Mallasvik

Gjøvik University College, Norway  
Norwegian Information Security Laboratory  
Department of Computer Science

## Motivation

- An increasing amount of sensitive data is stored on handheld devices.
- Vulnerable authentication protocols are being used to protect valuable information
- Loss of information may involve loss of revenue and financial obligations
- Modern smart phones allow for more elaborate schemes utilizing accelerometers etc.

## This thesis concentrated on the following areas:

- Analysis of the accelerometer signals produced by hand gestures
- The modulation, recognition and separation of hand gestures
- Incorporating hand gestures as an additional modality in authentication schemes, to increase **observation resistance**

## Overall goal

Increase observation resistance by the usage of **hand gestures** in direct, and **challenge-response** combinations

# Gesture analysis and recognition

We gathered a total of 1140 samples divided on 6 different gestures (RF, LF, BF, FF, CR, CL) and 38 people, which consists of three pairs of identical but inverted gestures.

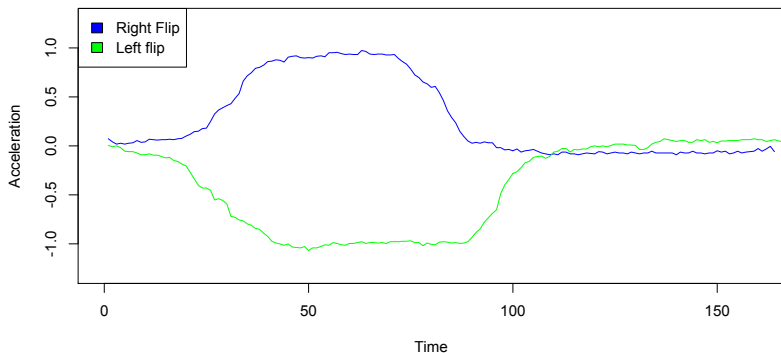
- Performed a distinctiveness investigation, where we achieved an EER of 27-28% - our focus was not on biometrics
- This indicates high intra-class variances - raw hand gestures are not very distinctive
- Generated templates, representative for all users, based on a median calculation.
- Utilizing more sophisticated distance metrics and template generation methods might lower the EER.

The general templates lowered our EER to 8% and 5%, with and without circular gestures respectively.

# General templates

Even gestures from the same pair provided us with clearly distinctive results in at least one axis.

Right and left flip, general templates X-plot



# PIN-code placement based authentication scheme

In this scheme, gestures was used to place the PIN digits entered by the user into a predefined position in the PIN-code.

- Each PIN entry consist of the 2-tuple PIN digit and gesture.
- Each gesture statically corresponds to a specific placement in the PIN-code (e.g, back flip - first position).
- Allows for obfuscated logins - the user can change login sequence each time
- The scheme uses a 4-digit PIN, but allows for unlimited digit entrances due to the **overwrite mechanism**

**Overwrite mechanism** A user can overwrite a previously entered PIN digit by performing the same placement gesture twice.



# PIN-code placement based authentication scheme cont.

We enforced the worst case attack scenario; **full observability**, meaning that the attacker could observe the login sequence however he wanted.

- We evaluated the observation resistance of the scheme with and without applying the *overwrite mechanism*.
- Gesture recognition delay gives attackers time to think - fixed in newer devices
- Overwrite mechanism increases resistance

Combined observation resistance rate of 85% (normal PIN entry scheme: 1.25%). Good considering the recognition delay and attack scenario



# Elaborate challenge-response scheme

Previous scheme is, like all simple CR schemes without randomness, viable against direct replay attacks.

- This scheme introduces additional human and device randomness to thwart this threat
- Attack scenario; **full observation on video**

Experiment specific research questions;

- How hard is it to obtain video footage clearly showing all challenges and gestures performed?
- How resilient is the scheme when an attacker has access to multiple login sequences of the same person?

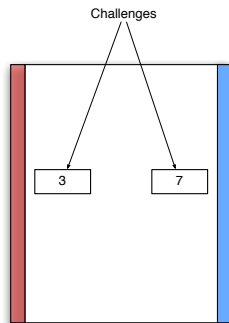
# Elaborate challenge-response scheme - Protocol description

Secrets shared between device and user;

- 8-digit long PIN
- Gesture-color associations

Protocol:

- User presented with 4 unique challenges
- The **digits** correspond to indices in the users PIN
- The user *chooses* which one of the indices to enter, by performing **either** the gesture corresponding to the *red* or *blue* color.



# Elaborate challenge-response scheme - Security assessment

## Summary of findings;

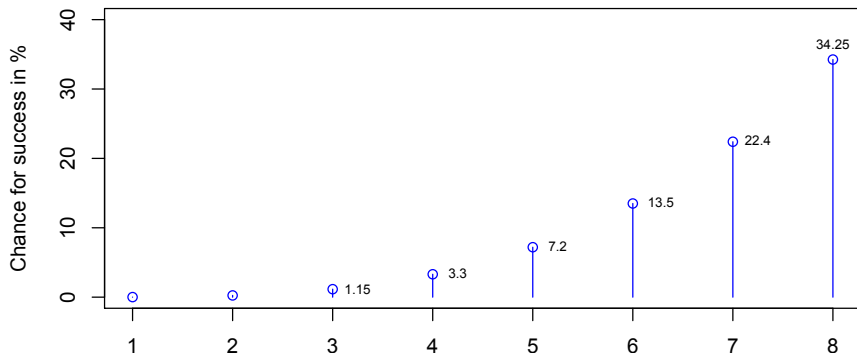
- $\approx 0\%$  chance of a replay attack succeeding, as each challenge is unique.
- Extremely difficult to obtain video footage clearly showing both indices, colors and gestures, even in a perfect environment with external lighting.
- An attacker can never deduce more than two gesture-color associations.
- The scheme's resilience depends on the amount of PIN digits the attacker has deduced.
- Statistically highly unlikely that an adversary can decode more than 4 PIN-index relationships after videotaping 2 sequences from the same person. Thus giving him a 3.3% chance.



# Elaborate challenge-response scheme - Security assessment cont.

Shows the relationship between decoded PIN-digits and the attackers chance of successfully attacking the protocol.

**An attackers chance of successfully attacking the scheme**



## Gesture recognition

- Achieved adequate recognition rates for authentication usage
- Newer devices will remove recognition delay, and allow for the inclusion of pre-processing steps

## PIN-code placement based authentication scheme

- Easy to use and increases observation resistance significantly, even with delay
- Extensions can further improve security, e.g, let the user decide gesture-placement assignment

## Elaborate challenge-response scheme

- $\approx 100\%$  replay resistant
- Offers an significant amount of resistance even against video observation attacks
- A bit more complicated to use - security tradeoff

## To lower the EER;

- Remove noise (at start and end) by using sliding windows
- Curve fitting - normalize all sequences to one length before comparison
- Implement more sophisticated distance metrics and template generation methods
- Personalization of templates

## Authentication schemes;

- Retest the *PIN-code placement based authentication scheme* under more realistic scenarios, and on a more powerful device - hence removing the delay.