Contextual Security
Secure Systems Group

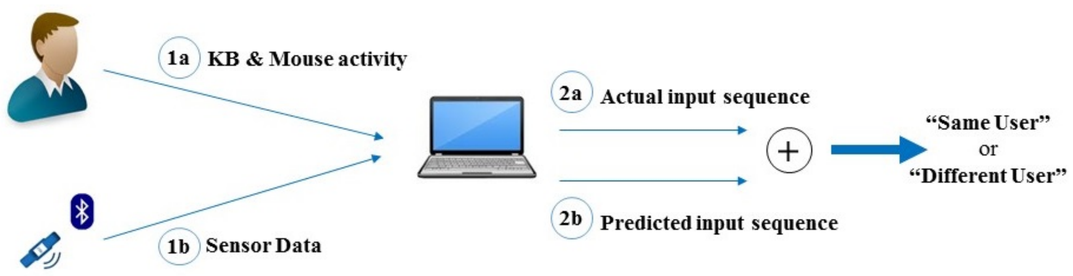
Swapnil Udar, Otto Huhta, Prakash Shrestha, Nitesh Saxena, N. Asokan

Perils in Designing Zero-Effort Deauthentication

- Prompt deauthentication a challenge on multi-user terminals
- ZEBRA correlates wrist-movements with observed I/O activity to determine if legitimate user is still interacting with a given terminal

Zero-Effort Bilateral Re-Authentication[1]

- Allow seamless recurring authentication for logged in users
- Prompt deauthentication in case user has moved away from terminal
- User-agnostic, cheap to deploy

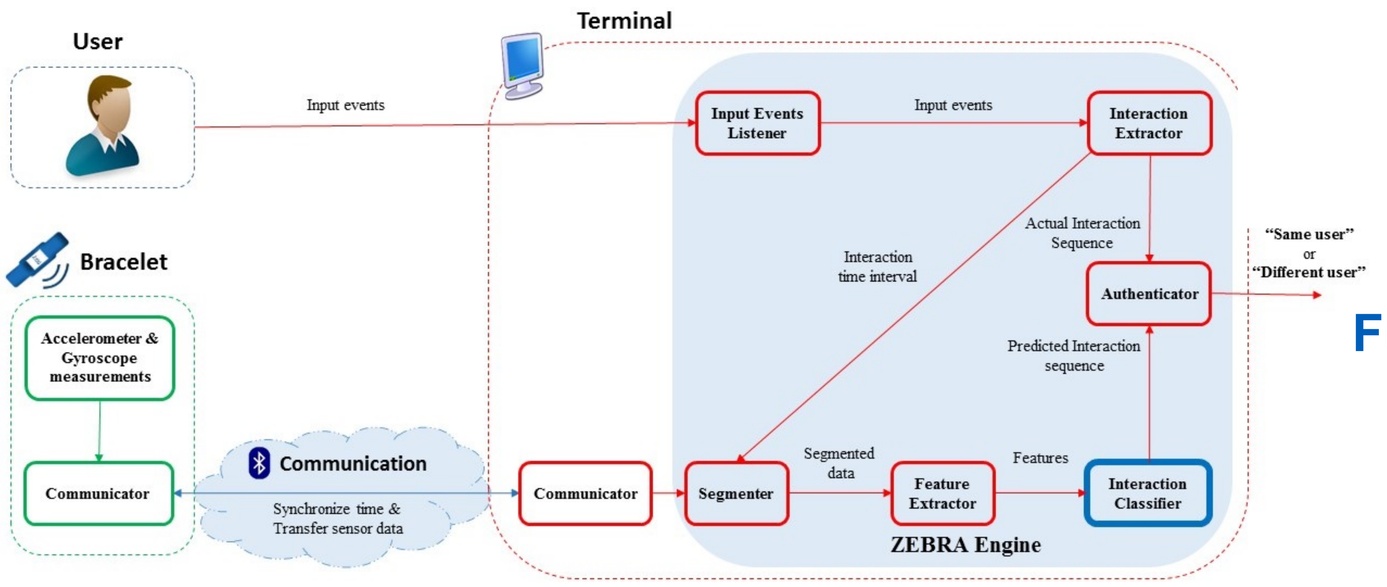


(1a) keyboard and mouse interactions on a PC

(1b) sensor data from personal wrist-worn bracelet

(2) Use machine learning to predict PC interactions from sensor data

Compare known and predicted interaction sequences: log user out if they don't match



Vulnerabilities

- Authentication triggered only by PC interaction

→ No interaction, no deauthentication

→ An attacker can select type, timing of activities

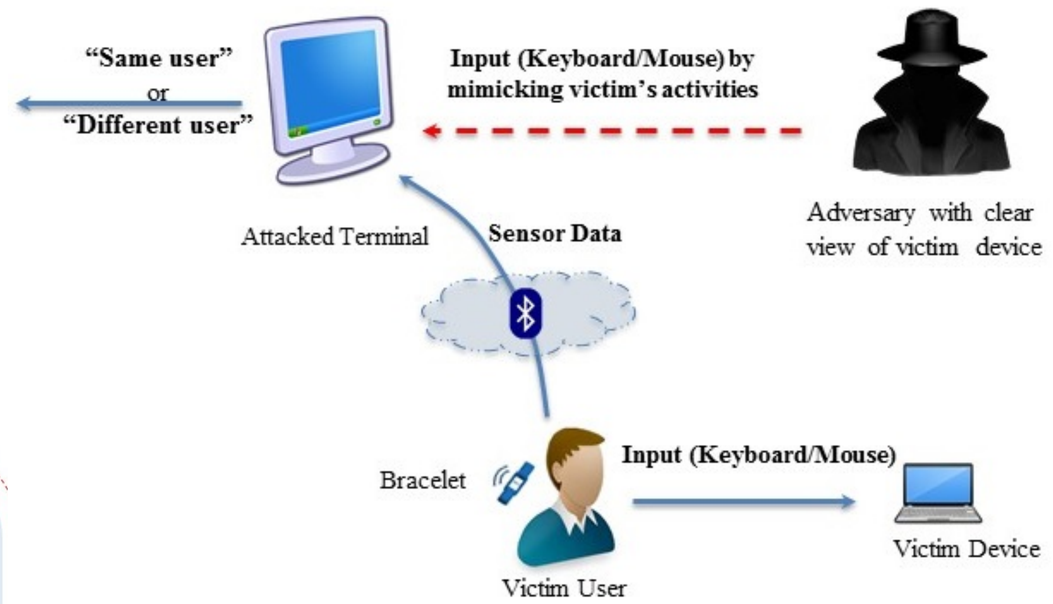
- Some interactions easier to mimic than others

Attack

- Attacker opportunistically mimics activities
- Focuses only on the keyboard

→ Sophisticated attacker can cheat ZEBRA

→ Still secure against innocent misuse



Further development

- Trigger authentication based on bracelet
- Integrate with proximity-systems
- Improve classifier by using training data from broader range of input devices

1) http://thaw.org/2014/04/02/zebra-zero-effort-bilateral-recurring-authentication/

Aalto University

Academy of Finland

UAB

http://arxiv.org/abs/1505.05779