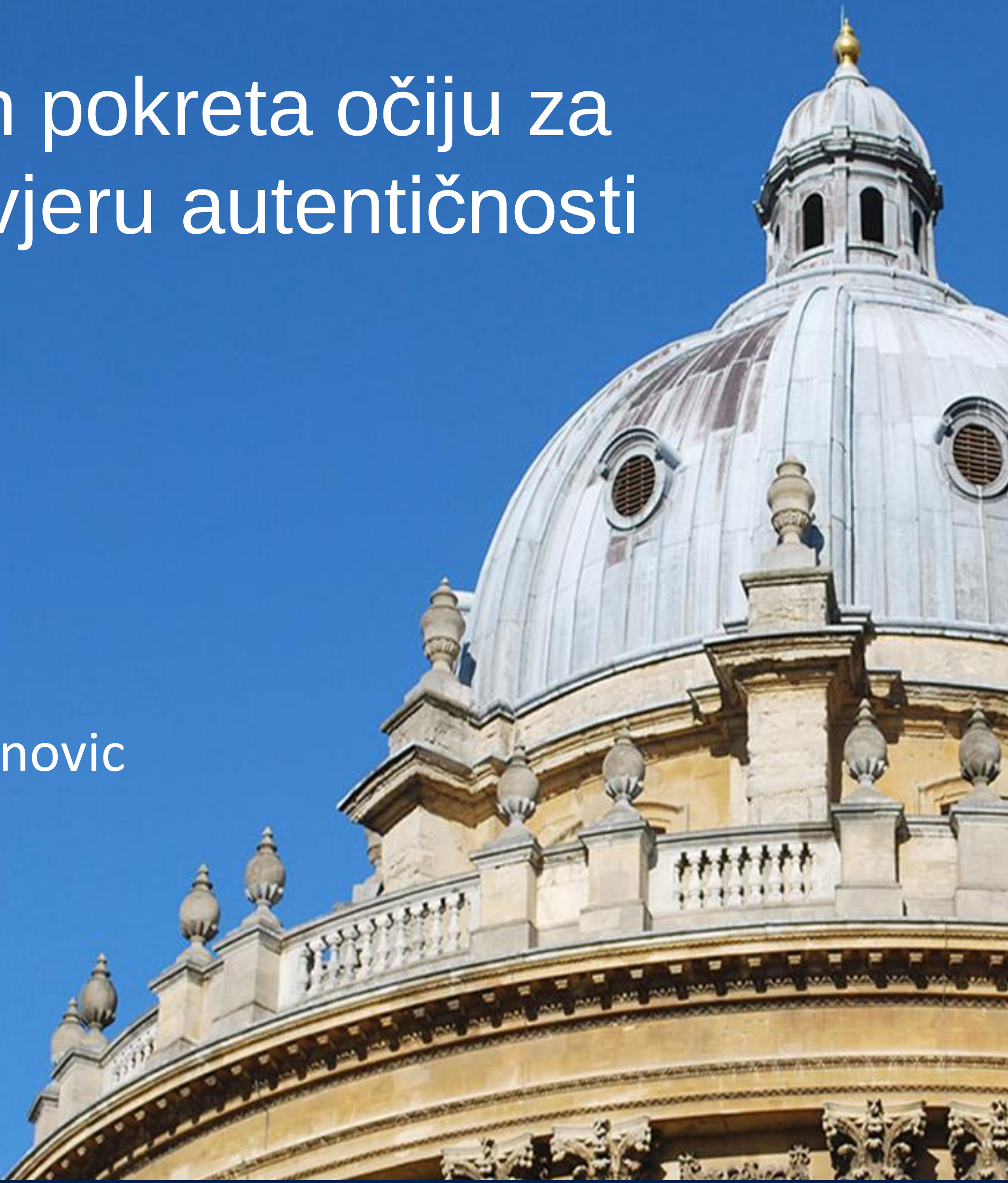
Korištenje refleksivnih pokreta očiju za brzu biometrijsku provjeru autentičnosti

Ivo Sluganovic, Marc Roeschlin,

Kasper B. Rasmussen, Ivan Martinovic

University of Oxford



ZIS, FER Zagreb, Travanj 2017

University of Oxford, Dept. of CS

- Oldest English speaking univ. (est. 1096)
- Consistently ranked in top 6
- Currently 1st worldwide (Times Higher Education ranking)

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

- By subject, **CS** currently ranked 3rd
- 150 academic and research staff
  - Just in: Touring Award to Tim Berners Lee
- 140 PhD (DPhil) students
- Growing fast, esp. in security (CDT!)

Systems Security Lab

- Prof. Ivan Martinovic
- 1 postdoc
  - Martin
- 10 PhD students:
  - Bushra, 2x Simon, Michal, Chris, Vincent, Richard, Matt, Marc, Ivo
- 2 visiting students:
  - Giulio & Kai
- Always looking for enthusiastic and driven researchers!

Systems Security Lab - areas

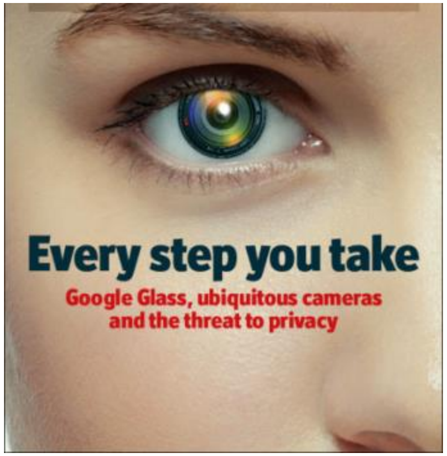
- Location-based Authentication
  - Authentication credentials using PHY-location information
  - Securing next generation **air traffic communication**

- Smartphone/Malware Traffic Analysis
  - Using **smartphone traffic** patterns to identify different smartphone users
  - Traffic based **malware detection**

- Resilient Anti-jamming Communication
  - Security & privacy of **drones** and related communication
  - Communication primitives against **jamming** attacks (intentional interference)
- User (De-)Authentication using Behavioral Biometrics
  - Eye-tracking and gaze-tracking as continuous biometrics
  - Using human bio-signals to authenticate users
  - Attacks on existing systems

Our Latest Collaboration

- **“Observation Resistant User and Device Authentication for Augmented Reality Devices”**
  - doc. dr. sc. Ante Đerek i Matej Šerbec

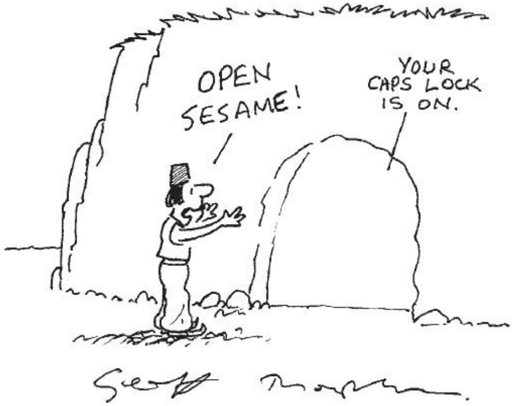


Korištenje refleksivnih pokreta očiju za brzu biometrijsku provjeru autentičnosti

User Authentication

3 main ways to authenticate*:*

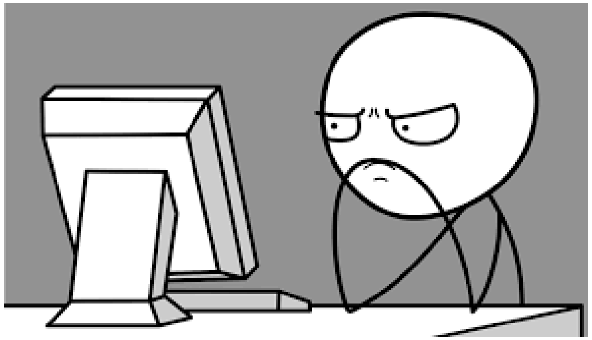
1. *What you **know*** *(e.g. passwords)*
2. *What you **have*** *(possessing the key)*
3. *Who you **are*** *(biometrics)*



"Rules for passwords":

1. A good password should be hard to remember
2. You should never write your password down
3. No password should ever be reused

??!? ☹



Biometric Authentication

- *"…distinctive, measurable characteristics used to label and describe individuals"*

- Authenticate by proving *WHO you are:*
  - Claimed identity proven by generating biometric data on demand
  - Not the same as **identification** (1:1 vs 1:n)

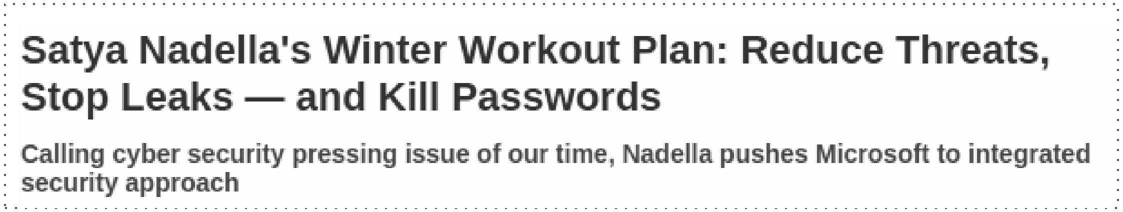
Ivan Vučetić, daktiloskopija

- **Multiple benefits:**
  - Impossible to forget or loose
  - Usually fast(er)
  - Stronger than most users' passwords
  - Less or no cognitive load
  - Non-transferable
    - Prevents phishing & other social engineering
    - Enforces accountability

Biometrics - The Future?

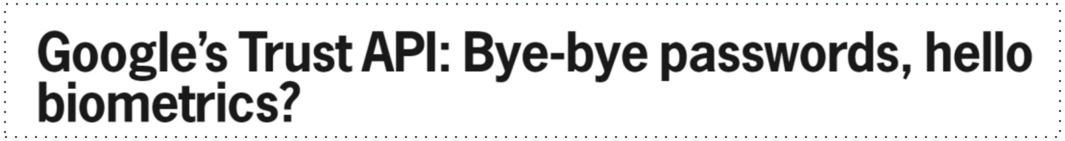
AADHAAR

- over 99% (1.133 billion) of Indians aged 18 and above had been enrolled
- world's largest biometric ID system



Satya Nadella's Winter Workout Plan: Reduce Threats, Stop Leaks — and Kill Passwords

Calling cyber security pressing issue of our time, Nadella pushes Microsoft to integrated security approach



Google's Trust API: Bye-bye passwords, hello biometrics?

Reuse of Biometric Data

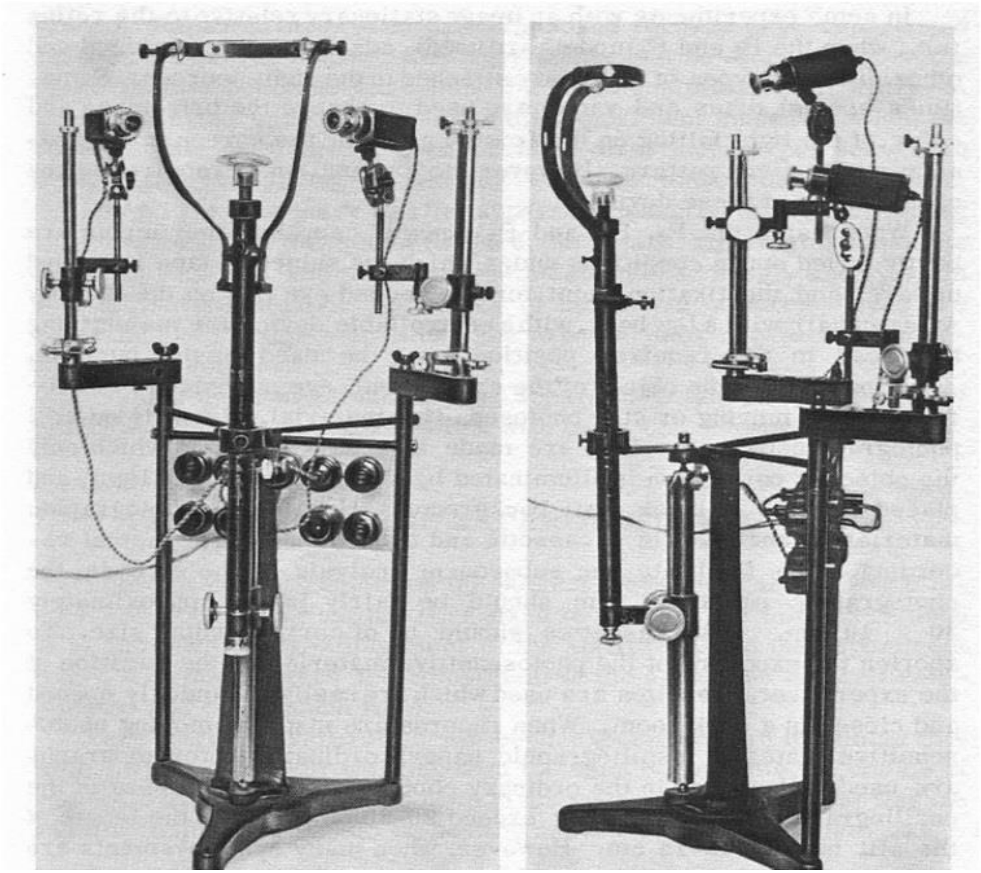
Biometrics seem to be everywhere recently

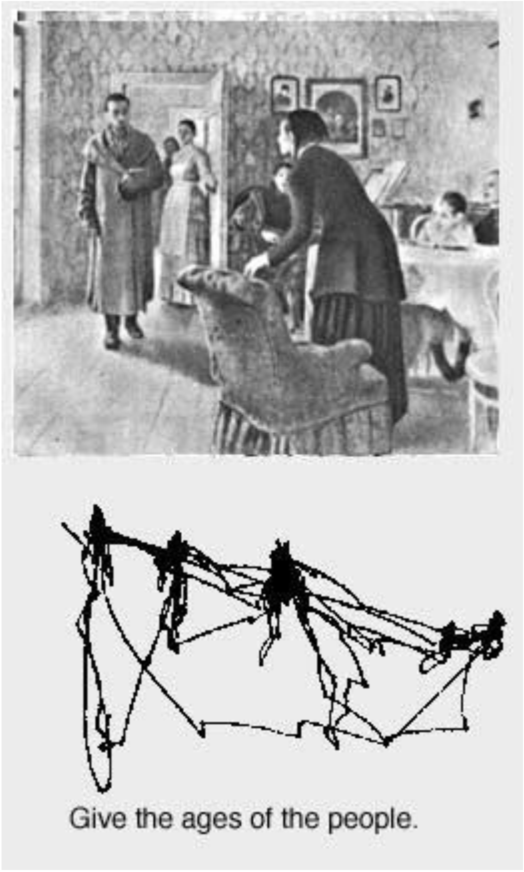
***…** however:*

How can we ***prevent the reuse*** *of eye movement biometric data?*

- Biometrics mostly implement *liveness detection* as a proxy
- Protocols typically prevent reuse by verification of freshness

Eye Tracking then…





Yarbus, 1967

… as a result of

Over 100 years:

- **Research:** visual perception, cognition, language comprehension
- **Medical**: detecting autism, concussions, depression
- **Interface:** disabled, design & marketing, gaming laptops

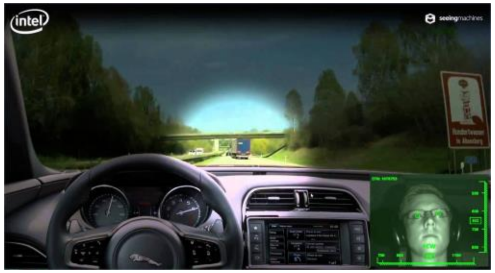
… now coming to …

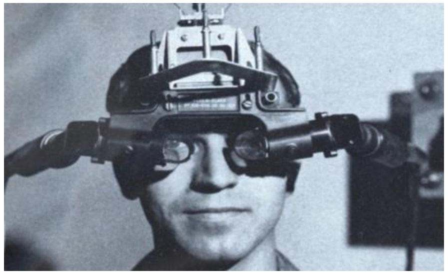
Mobile devices

- EyeScroll (Samsung S4, …, S7)
- Eye Tracking using commodity cameras (Krafka & Khosla, CVPR 2016)

Cars

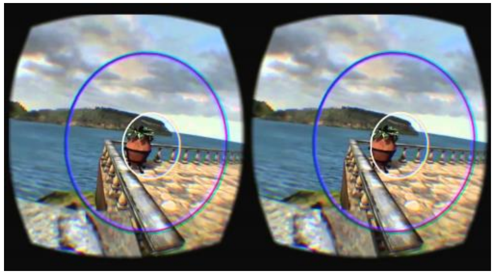
- Detecting drowsiness, focus
- GM, Cadillac in 2017



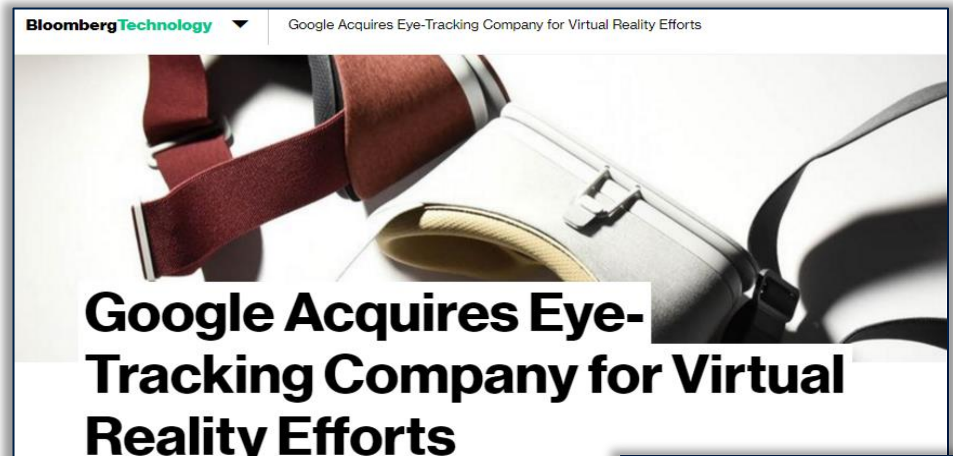


AR / VR systems

- New input channel
- Foveated rendering



...recently

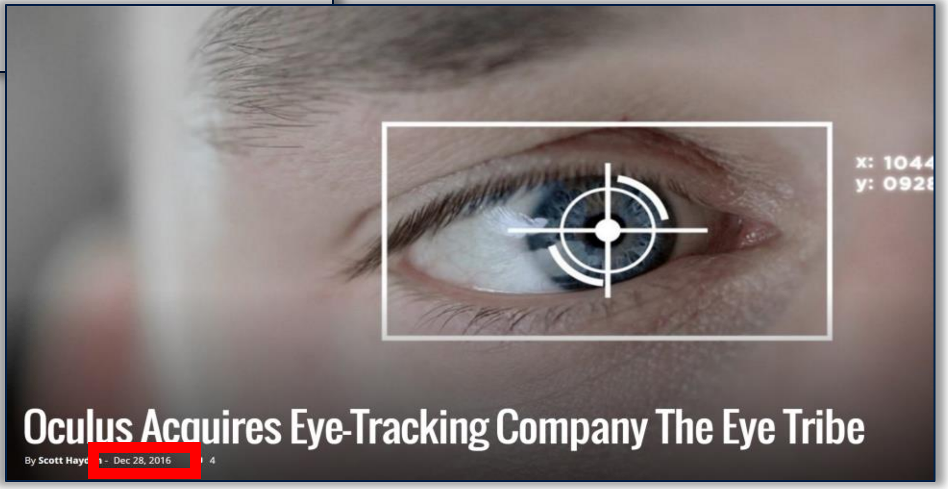


BloombergTechnology ▼ Google Acquires Eye-Tracking Company for Virtual Reality Efforts

Google Acquires Eye-Tracking Company for Virtual Reality Efforts

by Mark Bergen

October 24, 2016 — 9:40 PM EDT *Updated on* October 24, 2016 — 9:40 PM EDT



Oculus Acquires Eye-Tracking Company The Eye Tribe

By Scott Hay - Dec 28, 2016 4

Eye Movements

- 100 000 movements per day
- Responses in under 80 ms
- Fastest rotational movement in human body (900 deg/s)
- Can be both voluntary and reflexive
- Exhibit individual traits

Def: "An action that is performed without conscious thought, as a response to a stimulus."

In Authentication?

Use of eye movements

- As a control channel
  - Users input passwords or secret patterns

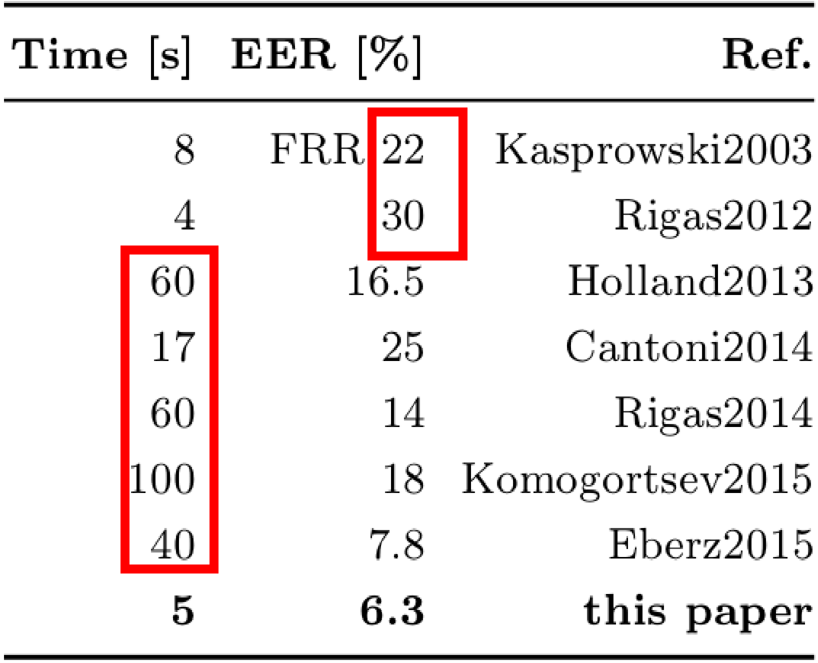
- **As a biometric**
  - Analyze characteristics of recorded eye movements
    - usually while showing a visual stimulus

1. “***what***” is one looking at
  - analysis of scan paths, areas of interest …

2. “***how***” do one’s eye movements look
  - speed, acceleration, latencies, curvatures & angles …

Eye Movement Biometrics

- Remains a **challenging problem**:



Time [s]	EER [%]	Ref.
8	FRR 22	Kasprowski2003
4	30	Rigas2012
60	16.5	Holland2013
17	25	Cantoni2014
60	14	Rigas2014
100	18	Komogortsev2015
40	7.8	Eberz2015
5	**6.3**	**this paper**

Visual stimulus …

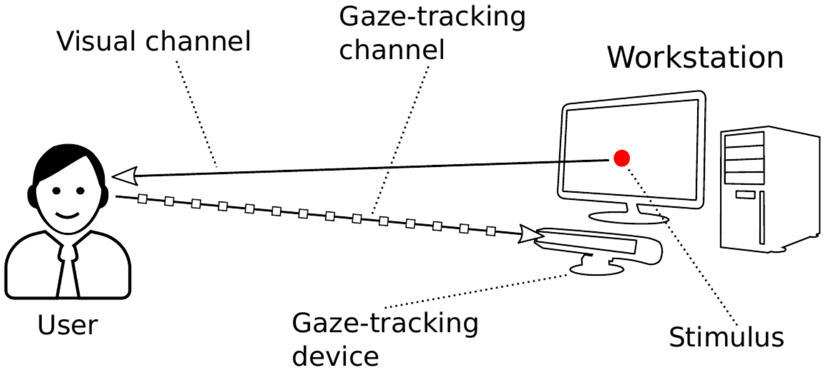
- *“Read the text”*
- *“Watch 30s of a movie trailer”*
- *“Look at the face”*
- <u>*“Look at the dot along these 9 positions”*</u>

Results in:

- Response depends on cognitive state
- Long authentication times
- User habituation

Our Assumptions

System Model



Threat Model

1. **Impersonation attack** ✓
   - Internal attacker
   - External attacker

2. **Replay attack** ✓
   - Attacker **observes** and directly replays legitimate authentication attempts
   - Not usually considered

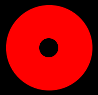
3. **Targeted attacks** ✓/ X
   - Very strong adversary: nothing is secret
   - Build an generative interactive model

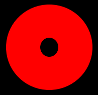
Design Goals

- General authentication goals:
  - Low error rates
  - Short authentication time
  - Low cognitive load
  - **Resistance against replay attacks**

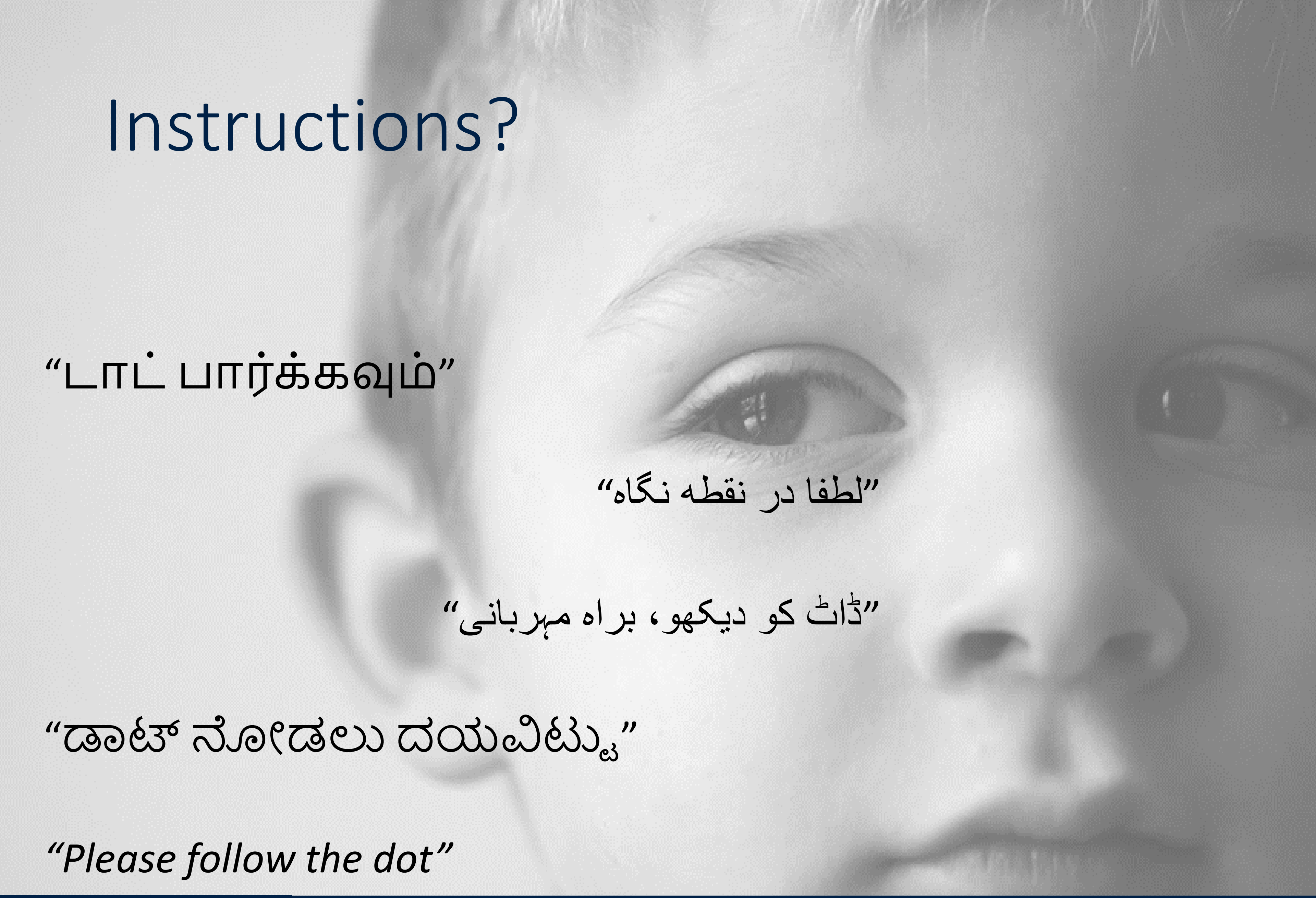
- Characteristics of an *ideal* visual stimulus?
  - Extracts predominately **physiological** responses
  - Requires **short**, **simple** interaction
  - **Fresh** every time and allows verification of the **response**

- **Core idea**: specific stimuli can elicit **reflexive** eye movements





Wasn’t that easy?



Instructions?

“டாட் பார்க்கவும்”

“لطفا در نقطه نگاه”

“ڈاٹ کو دیکھو، براہ مہربانی”

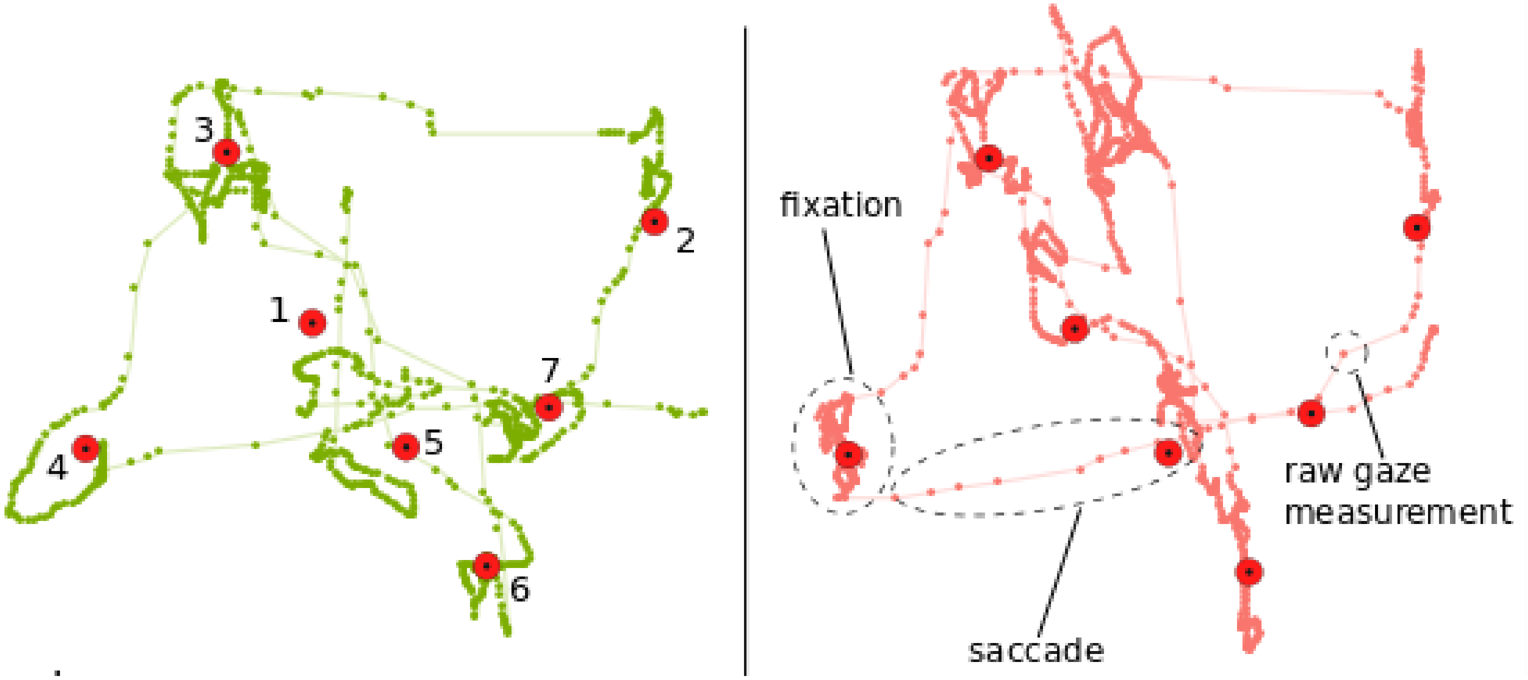
“ಡಾಟ್ ನೋಡಲು ದಯವಿಟ್ಟು”

“Please follow the dot”

Reflexive & Predictable Response

Core idea:

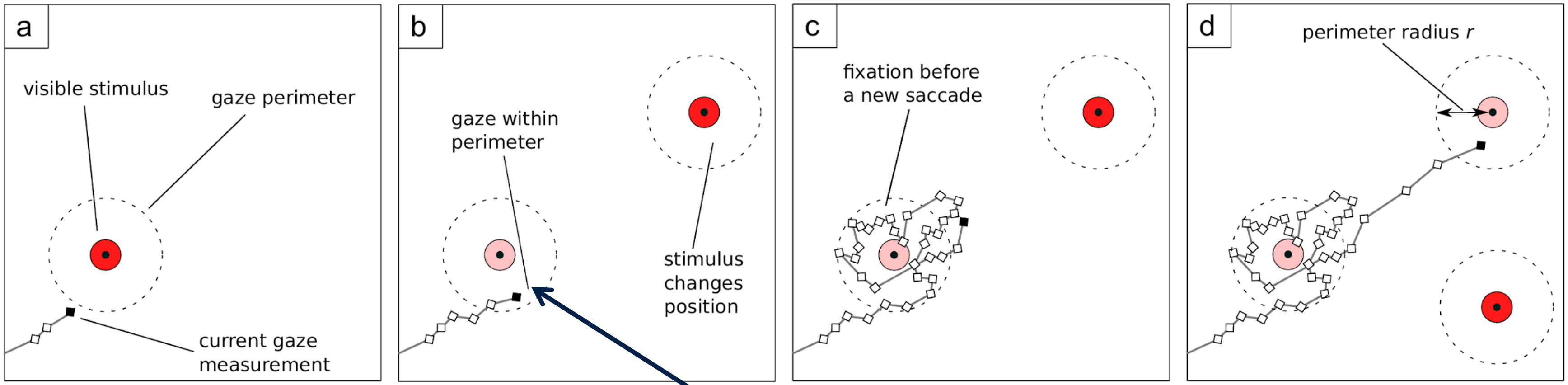
- While most are conscious, some eye movements can be **reflexively triggered** to elicit a **predictable response**



Sluganovic et al. - *Using Reflexive Eye Movements for Fast Challenge-Response Authentication*

Stimulus for Reflexive Saccades

How often should the position change?

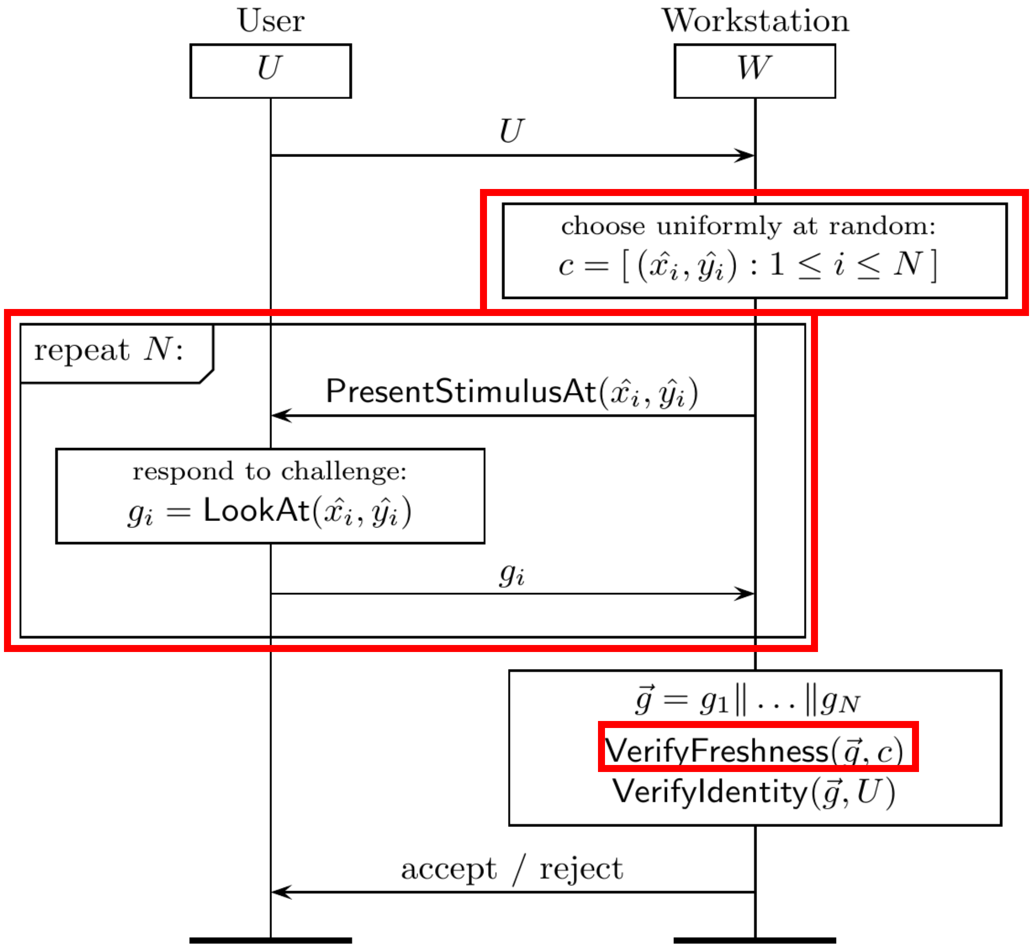


Successfully “gazed”

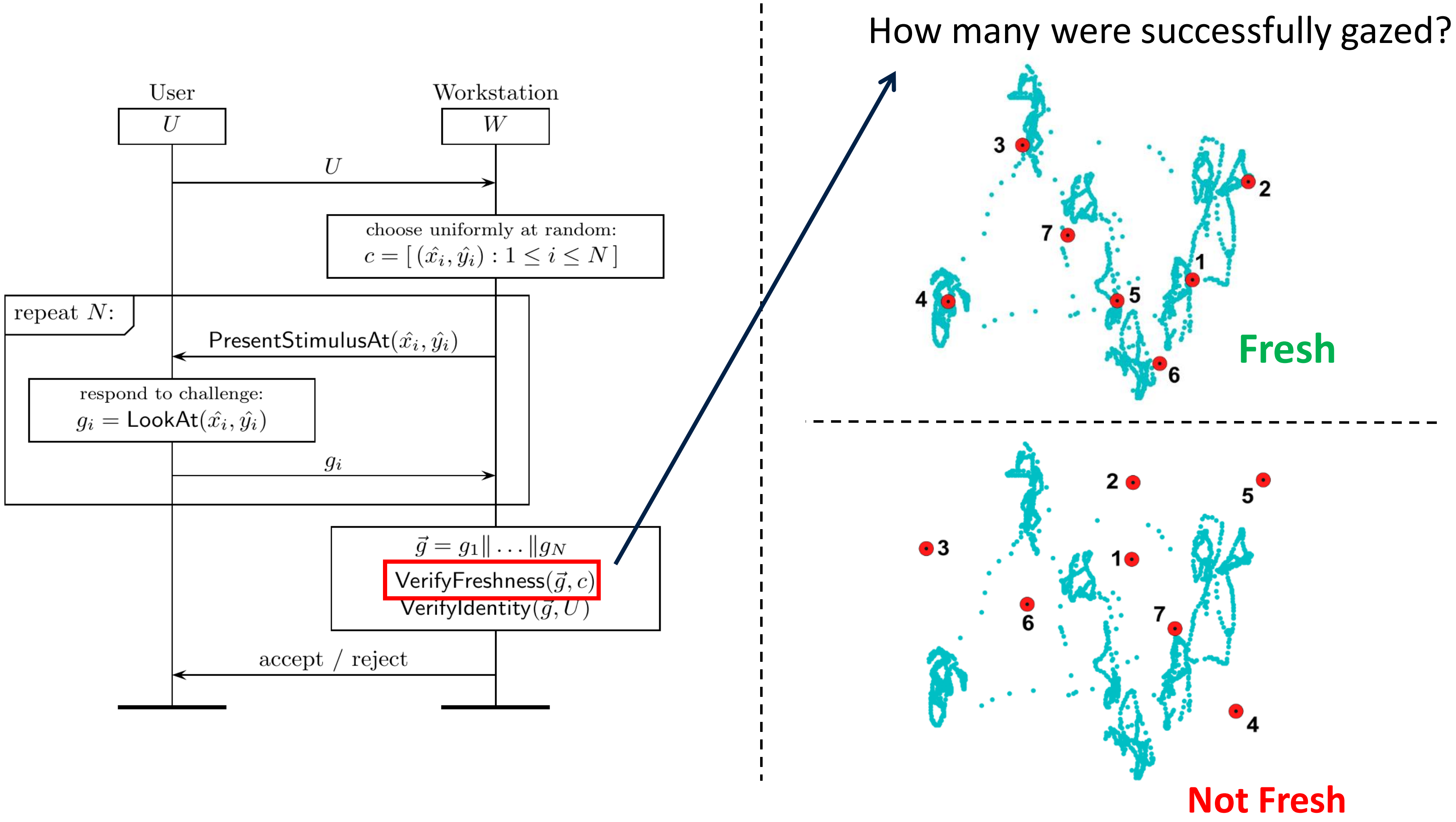
Making the stimulus **interactive**:

- Minimizes dwell time, maximizes number of extracted saccades
- Reduces habituation (unpredictable), increases reflexiveness
- Increases required effort for an attacker!

Biometric Authentication Protocol


User
U
Workstation
W
U
choose uniformly at random:
$c = [\,(\hat{x}_i, \hat{y}_i) : 1 \leq i \leq N\,]$
repeat N:
$\mathsf{PresentStimulusAt}(\hat{x}_i, \hat{y}_i)$
respond to challenge:
$g_i = \mathsf{LookAt}(\hat{x}_i, \hat{y}_i)$
g_i
$\vec{g} = g_1 \| \ldots \| g_N$
$\mathsf{VerifyFreshness}(\vec{g}, c)$
$\mathsf{VerifyIdentity}(\vec{g}, U)$
accept / reject

Biometric Authentication Protocol



User

U

Workstation

W

U

choose uniformly at random:
$c = [\,(\hat{x}_i, \hat{y}_i) : 1 \leq i \leq N\,]$

repeat N:

$\mathsf{PresentStimulusAt}(\hat{x}_i, \hat{y}_i)$

respond to challenge:
$g_i = \mathsf{LookAt}(\hat{x}_i, \hat{y}_i)$

g_i

$\vec{g} = g_1 \| \ldots \| g_N$

$\mathsf{VerifyFreshness}(\vec{g}, c)$

$\mathsf{VerifyIdentity}(\vec{g}, U)$

accept / reject

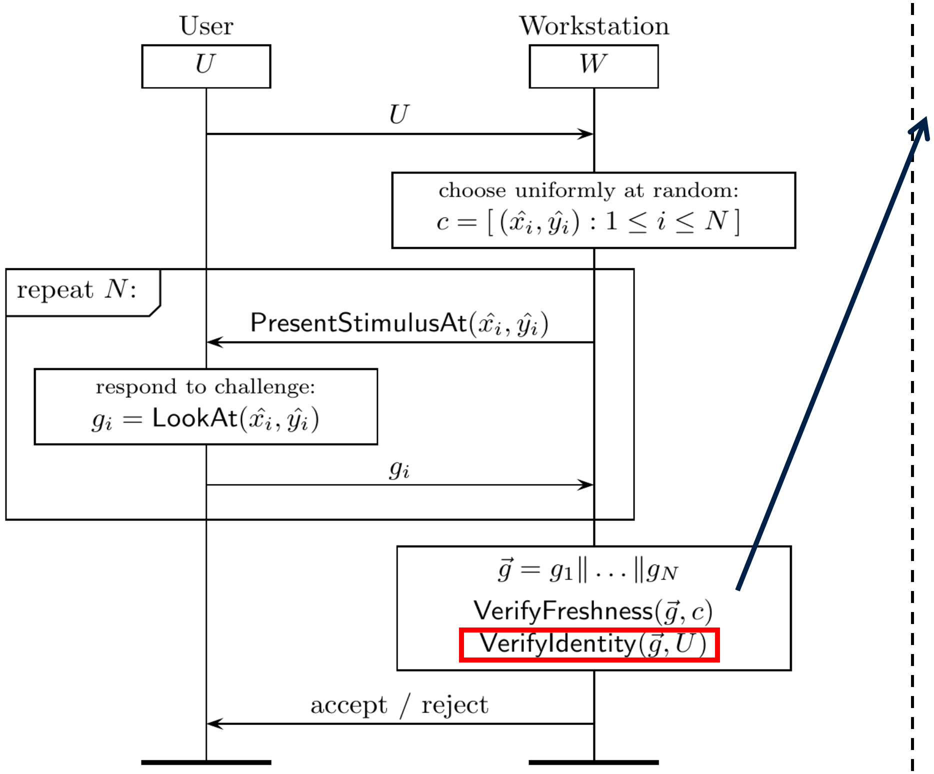
How many were successfully gazed?

Fresh

Not Fresh

Sluganovic et al. - *Using Reflexive Eye Movements for Fast Challenge-Response Authentication*

Biometric Authentication Protocol



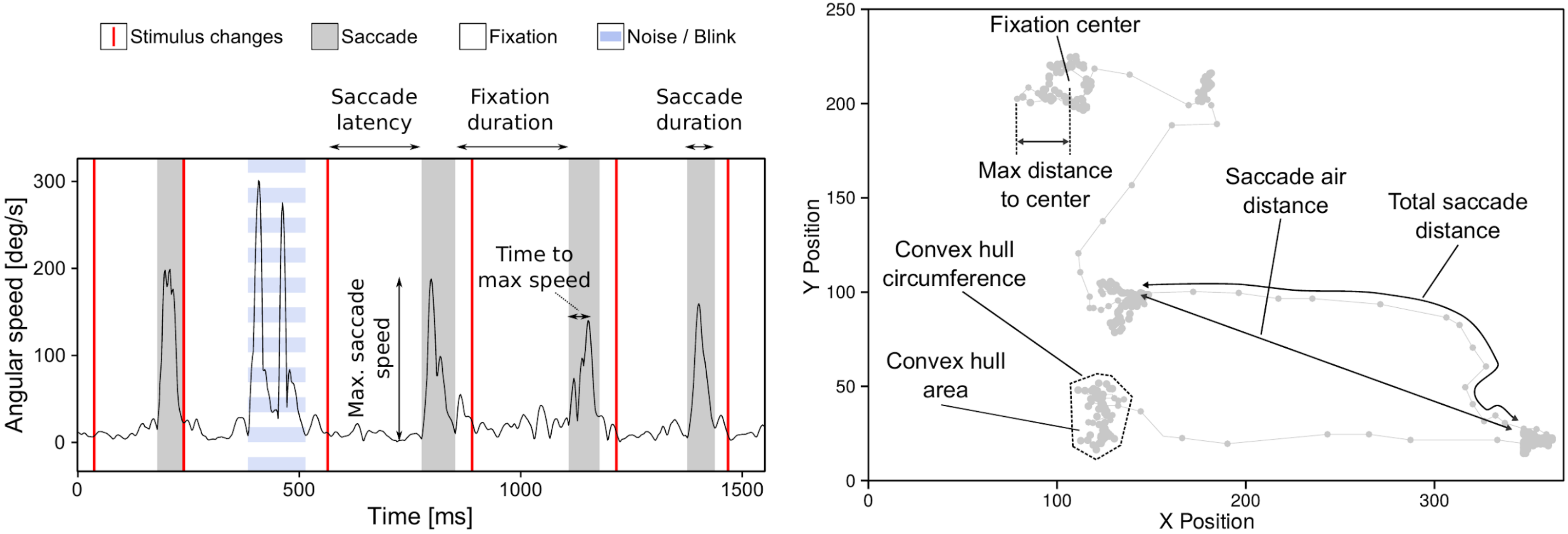
User
Workstation
U
W
U
choose uniformly at random:
$c = [\,(\hat{x}_i, \hat{y}_i) : 1 \le i \le N\,]$
repeat N:
$\mathsf{PresentStimulusAt}(\hat{x}_i, \hat{y}_i)$
respond to challenge:
$g_i = \mathsf{LookAt}(\hat{x}_i, \hat{y}_i)$
g_i
$\vec{g} = g_1 \| \ldots \| g_N$
$\mathsf{VerifyFreshness}(\vec{g}, c)$
$\mathsf{VerifyIdentity}(\vec{g}, U)$
accept / reject

Do observed gaze characteristics correspond to the claimed identity?

1. Extract multiple temporal and spatial features

2. Train/use a binary classifier for each user (SVM)

Features for Classification



(a) Temporal Features

(b) Spatial Features

- No physiological features (pupil sizes, distance between eyes, etc.)

Experimental Evaluation

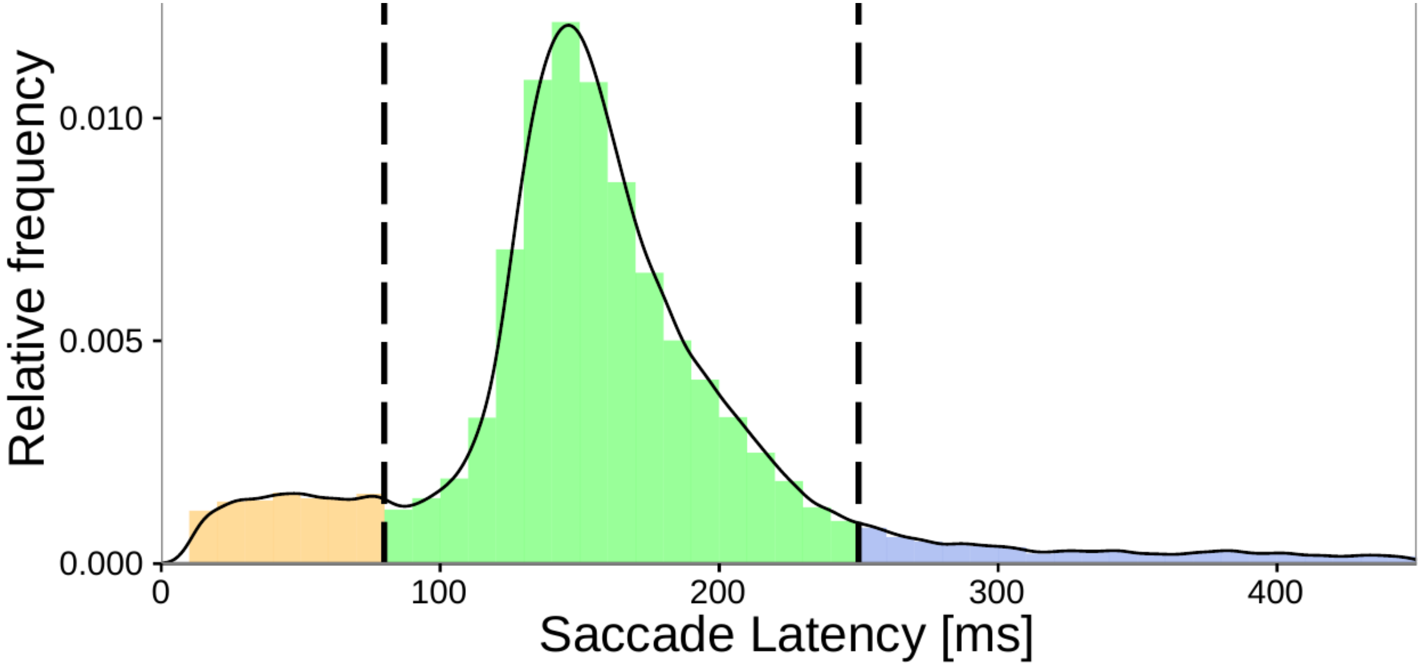
- Main questions:
  - Responses **predominately reflexive?**
  - Influence of challenge complexity on **errors** and **authentication times?**
  - Resistance against **impersonation attacks?**
  - Resistance against **replay attacks?**

- 4 sessions
  - Each with 15 authentication attempts
- 30 participants
- Total of 1 602 authentication attempts

Cognitive Effort

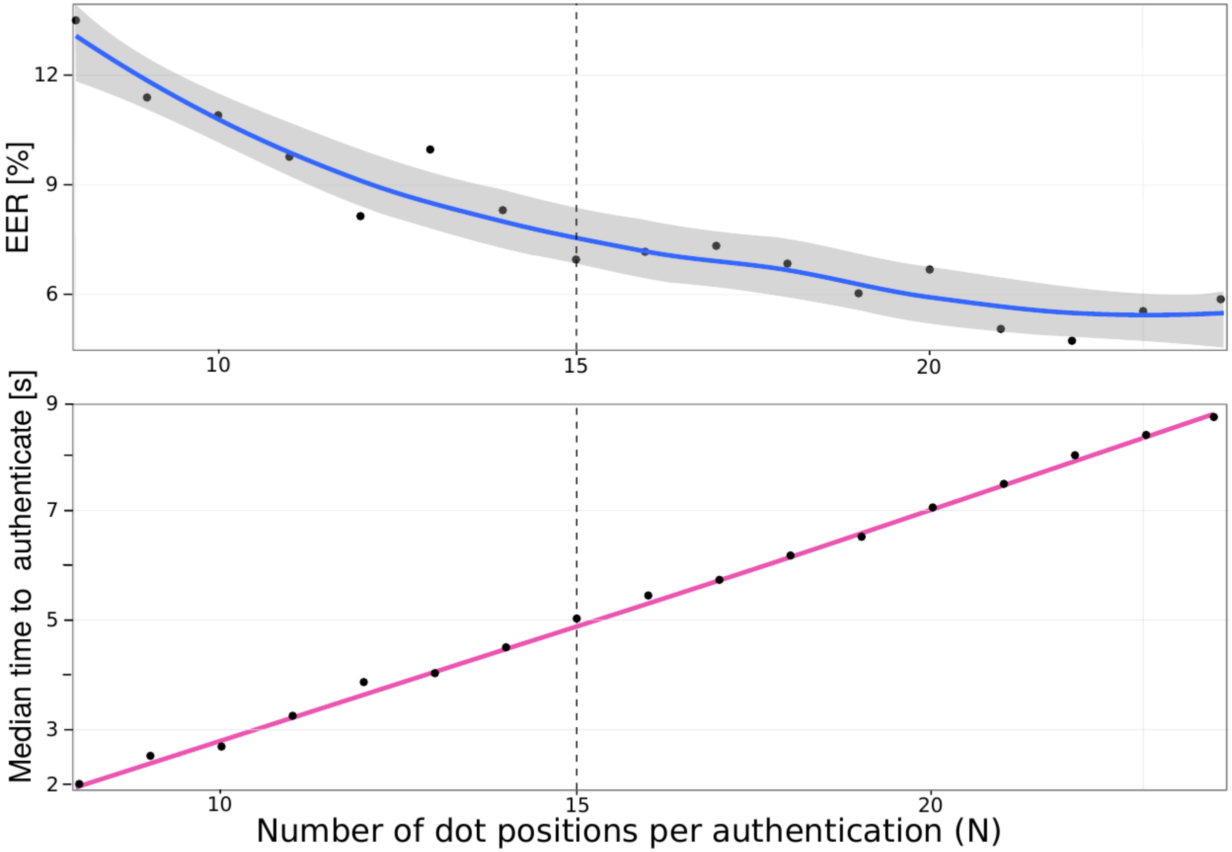
- *Are elicited saccades indeed reflexive?*
- Distinguished by their latencies:

noise < 80ms < **reflexive** < 250ms < **voluntary**



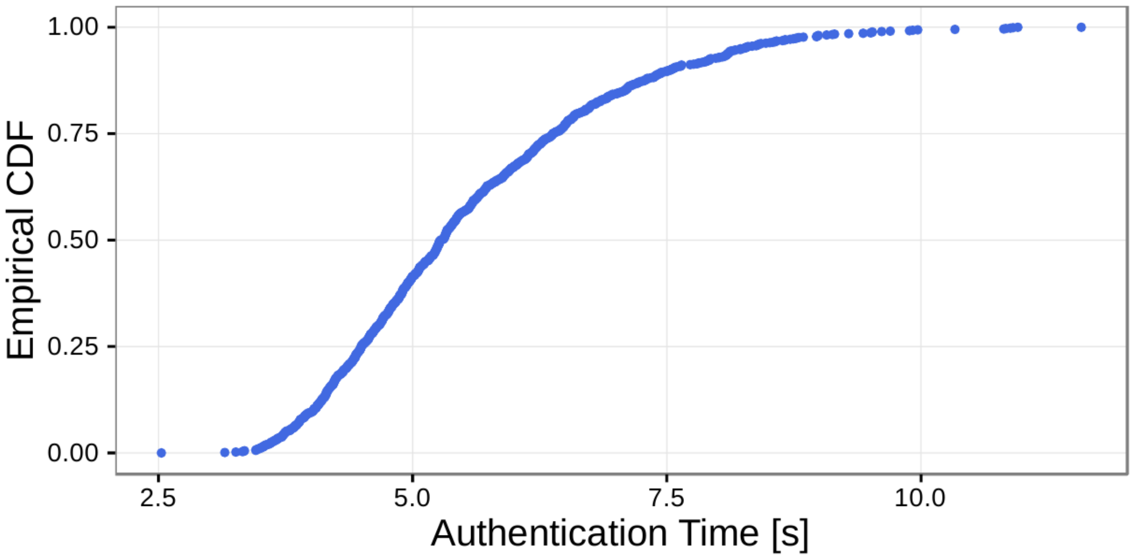
Stimulus complexity

- *How do errors and auth. times depend on stimulus complexity?*



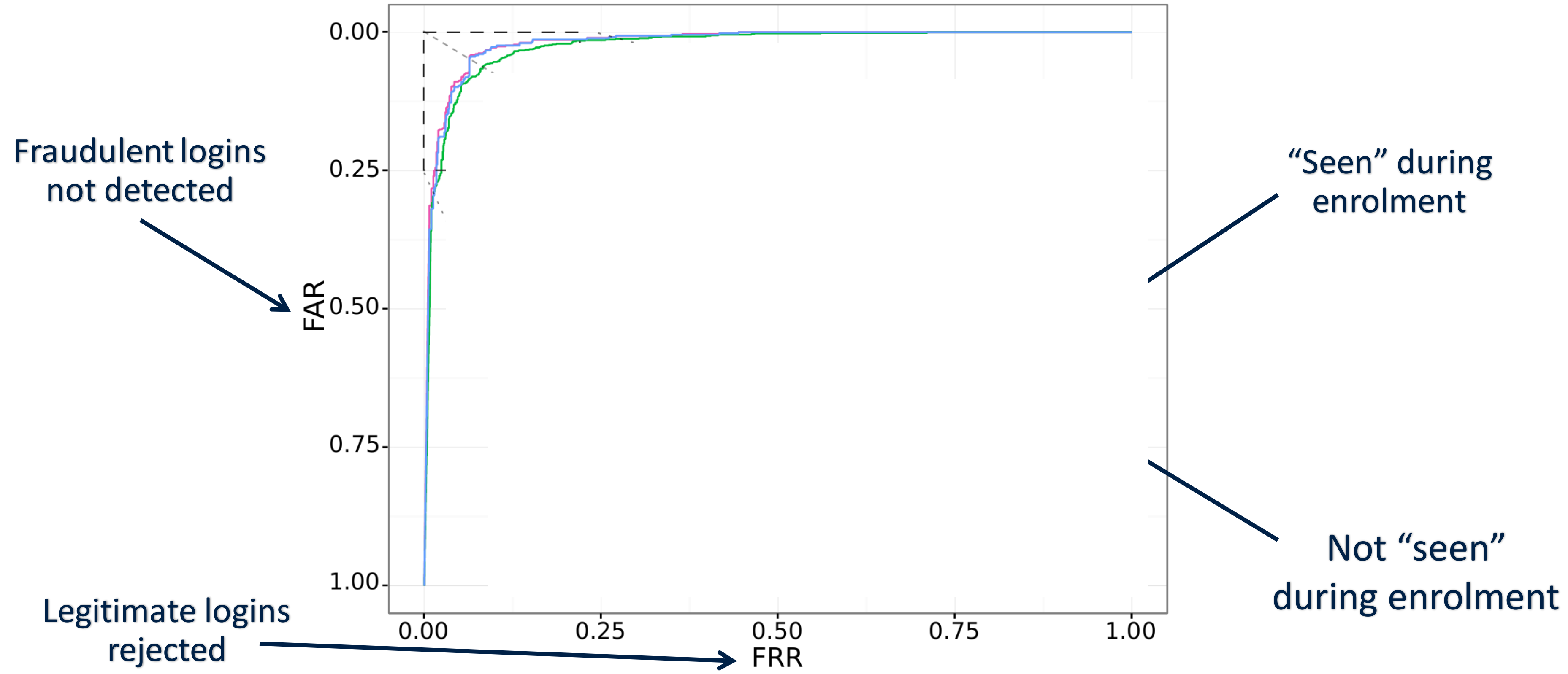
Authentication Time

- Distribution of auth. times when ***N = 15:***
  - *50% in under 5s, 90% in under 7.5s*
- *How fast is fast enough?* For passwords (Shay, ACM CHI 2014)
  - Authentication times: 11.6 – 16.2s
  - Input errors: 4-7%
  - 20% had problems recalling; 35% said "*remembering was hard*"



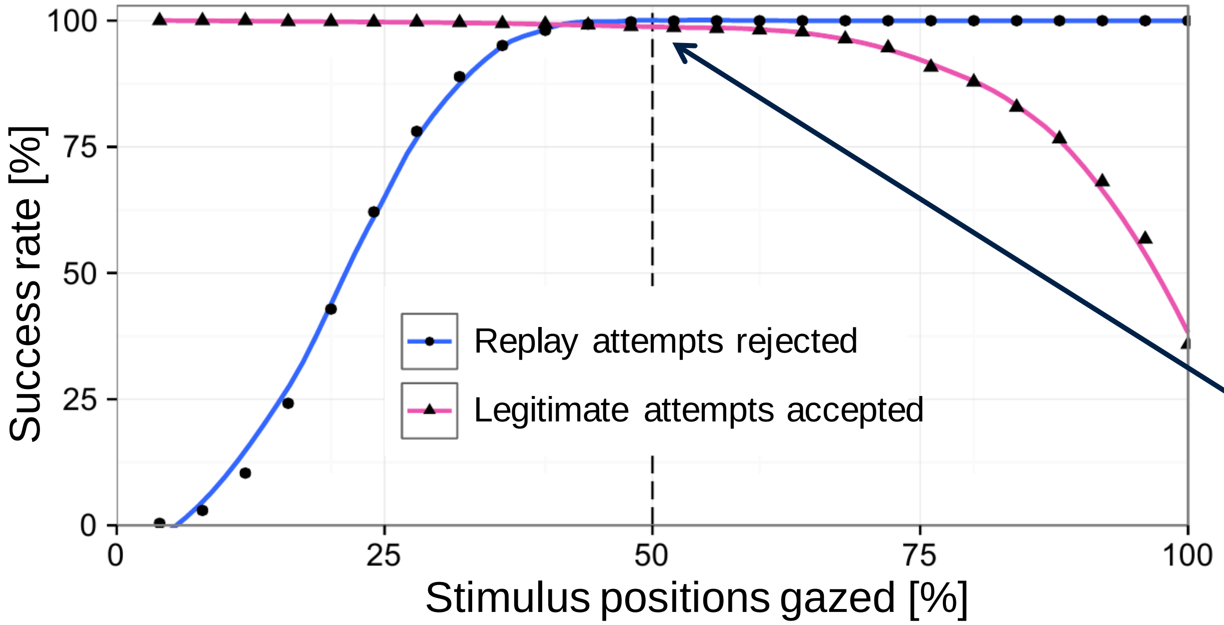
Impersonation Attacks

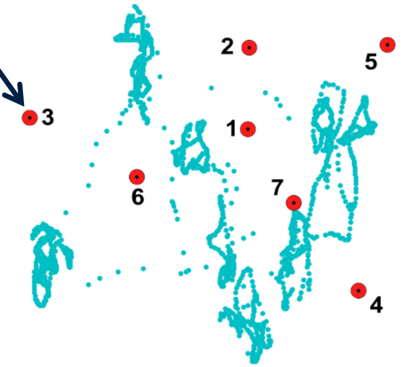
- Binary classifier trained for each user
- Varying decision threshold yields the ROC curve:



Replay Attacks

- Evaluated replay attempts for 10^6 pairs (*challenge*, *response*)





0.06% FAR

1.47% FRR

Conclusion

- **Reflexive eye movements** enable fast biometric user authentication
- Improved **authentication time** and **error rates**
  - **Median of 5 seconds**
  - **6-7% EER**
- Implemented challenge-response protocol to **prevent biometric replay**
  - **FAR of 0.06%**
- Applicability to systems which allow eye tracking

Future Work

- Evaluation on other devices
  - Mobile eye trackers (glasses)
  - Consumer devices
- Impact of different stimuli configurations
- Use of “static” features
  - pupil size, face
- Stability over time
- Evaluation of generative attacks

- Application of reflexiveness to other biometrics?

Other Recent Work

- *“Using **EEG-Based BCI** Devices to **Subliminally** Probe for Private Information”*
- *“Generating **Secret Keys from Biometric** Body Impedance Measurements”*
- “STASH: Securing **transparent authentication** schemes using prover-side **proximity verification**”
- **Security & privacy of AR devices (FER Zagreb)**

Hvala na pažnji!

Pitanja? ☺

ivo.sluganovic@cs.ox.ac.uk