MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

University of Cyprus

# HUMAN-CENTERED INTELLIGENT USER INTERFACES - MAI648

**Marios Belk**

2022

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

# Adaptive Usable Security

## CONTENTS

- Usable Security
- User Authentication
- Human Interaction Proofs
- Personalized Graphical User Authentication
- Special Topic in Adaptive Usable Security: On Flexible and Personalized User Authentication in Patient-centric Healthcare Systems

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Learning Outcomes

- Know definitions in adaptive usable security
- List the main categories of user authentication
- Evaluate the applicability of human factors in adaptive usable security mechanisms
- Understand the effects of human factors on security aspects of interactive systems

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Usable Security

- Designing security systems that people can use
- One of the 11 hard problems to achieve cyber security [U.S. Dept. of Homeland Security]
- Security policies are reactive and not planned in advance which compromises usability

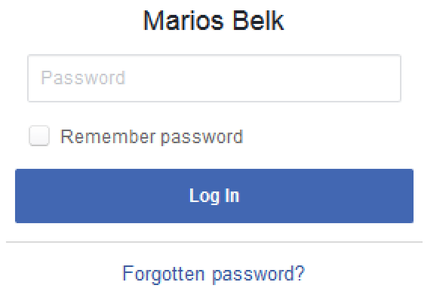


This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

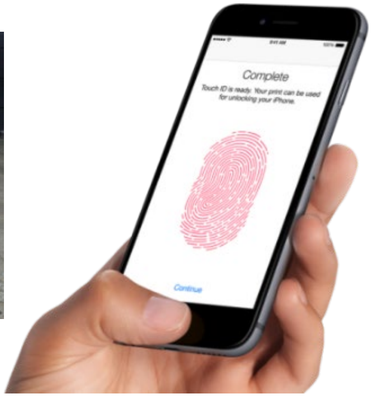
## CONTENT 8

# User Authentication oldest and mostly researched Usable Security topic

- Αὐθεντικός; meaning real or genuine, aims to confirm the authenticity of the user
- One of the most important security mechanisms of any infrastructure today







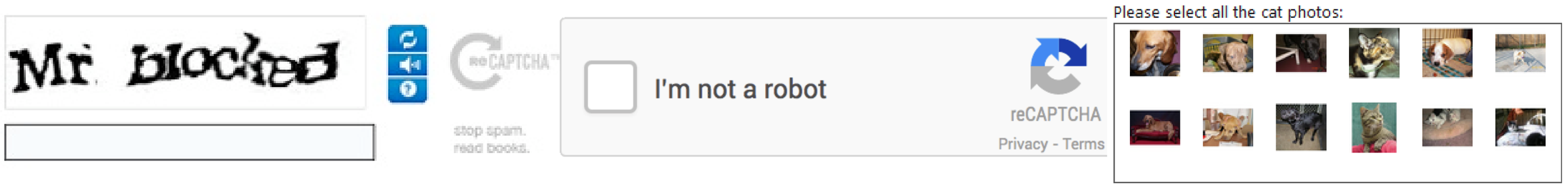



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Human Interaction Proofs highly researched Usable Security topic

- Protect Web systems against automated software agents
- Verifies that the entity interacting with a system is a human being, and not a software agent




*U.S. Department of Homeland Security (2009). A Roadmap for Cybersecurity Research. Available online: https://www.dhs.gov/publication/csd-roadmap*



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# On the Importance of Usable Security in Authentication and CAPTCHA

- Almost **every computer user owns** a password-protected account and **logs in every day** multiple times *[Florencio & Herley]*
- **95% of people reuse** their passwords across accounts *[inc.com]*
- Over **200 million reCAPTCHA** are completed daily *[Bursztein et al.]*
- Over 80% of users are **fed up with unnecessary CAPTCHA challenges** *[Fidas et al.]*
- More than **40% of help desk calls** are customer requests for **password resets** *[Economics of Security]*



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# On the Importance of Usable Security in Authentication and CAPTCHA

- Each password reset request can range from $50 to $150 in labor costs *[Gartner Research]*
- Major companies such as Yahoo, eBay, Sony, Uber faced **password hacks** and data breaches which **affected billions of customer accounts** *[Wired]*
- Sony's password hack in 2011 cost the company over $170M and affected 70M customer accounts *[Wired]*



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Methods on User Authentication

- Knowledge-based
- Token-based
- Biometric-based
- and Multi-factor authentication

[Passfaces, 2009; von Zezschwitz et al., 2015, Winkler et al., 2015; Hajashi et al., 2009; Apple; Google Android]



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

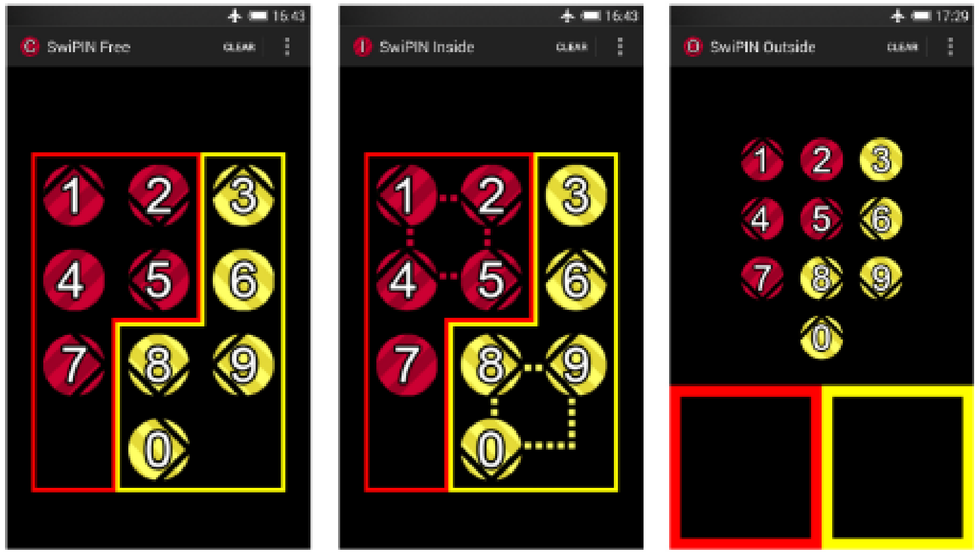
# Methods on User Authentication




This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# SwiPIN: Fast and Secure PIN-Entry on Smartphones

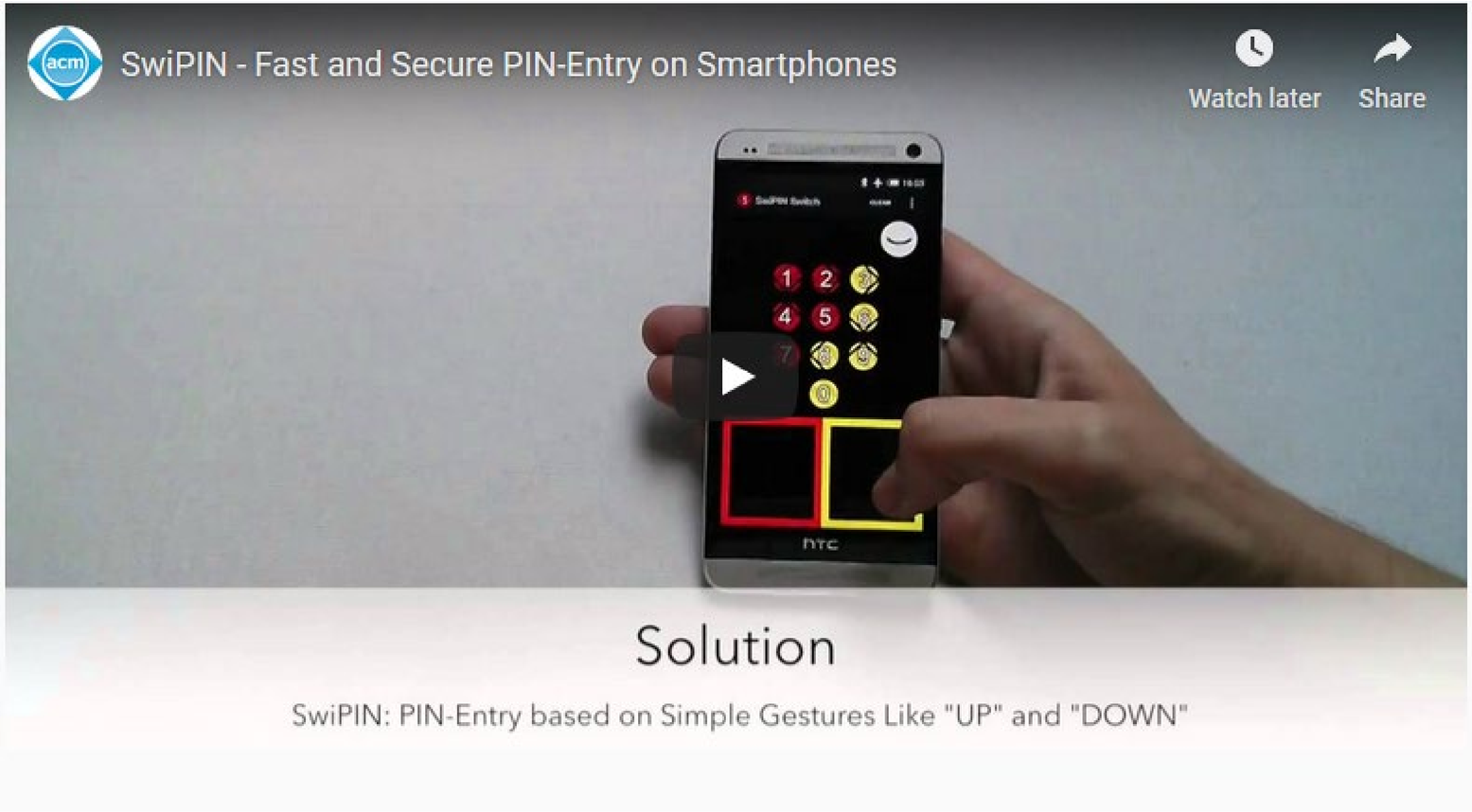



*Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). Association for Computing Machinery, New York, NY, USA, 1403–1406. DOI:https://doi.org/10.1145/2702123.2702212*



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

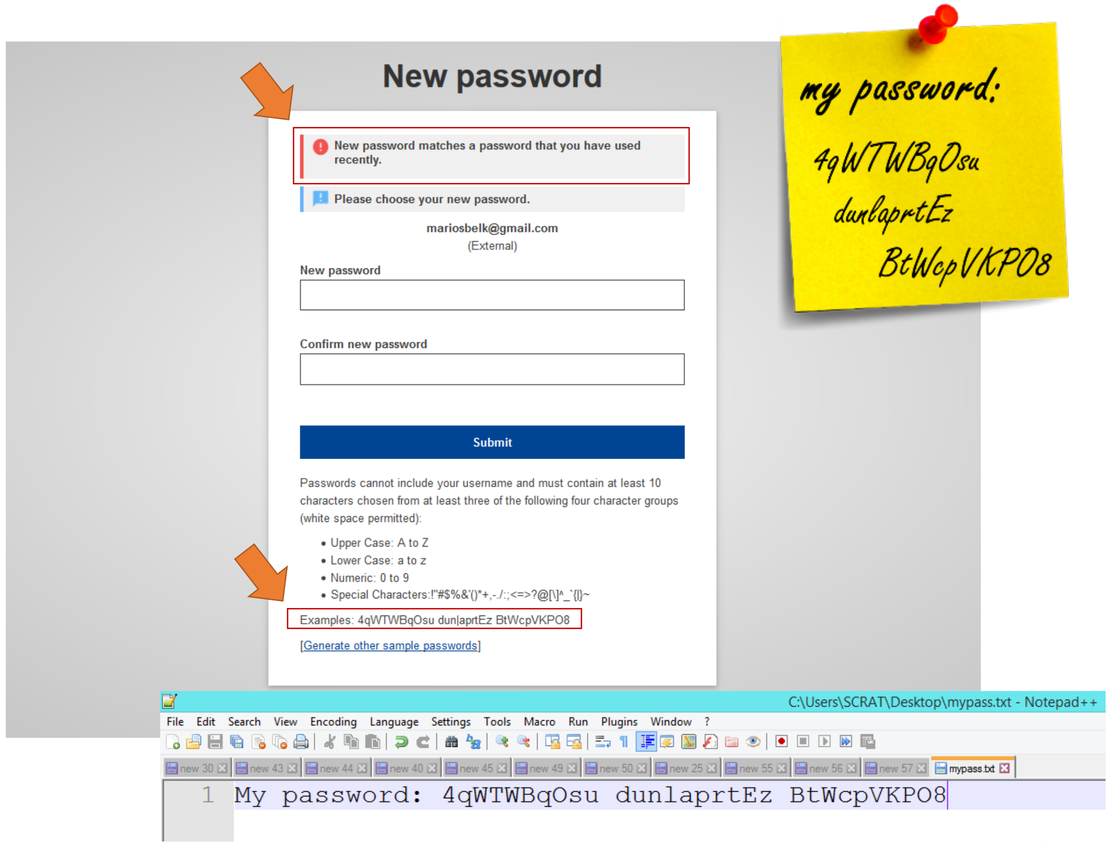



https://www.youtube.com/watch?v=5gKjcFwb55c


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Security vs. Memorability



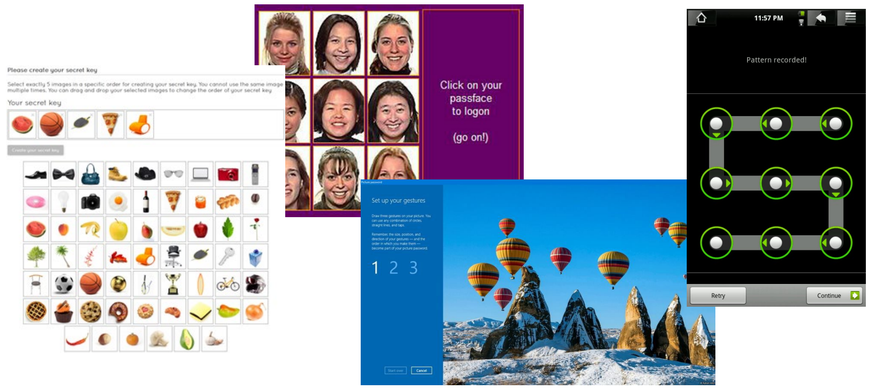



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Graphical User Authentication

- Require users to recognize or recall images or draw patterns on a grid as their authentication key
- Scaffold natural human-computer interaction and adapt easier to nowadays mobile and immersive user interaction realms





This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Recall-based Graphical Authentication

- Users draw gestures on a background image to login
  - Combination of tabs, circles, straight lines



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

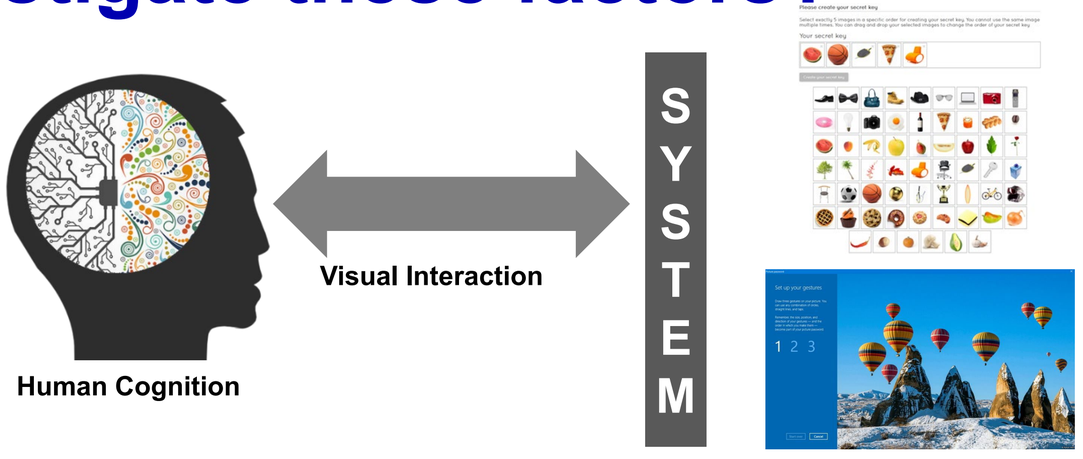

*Windows™ Picture Gesture Authentication*



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Why do we investigate these factors?




- A. Gain new knowledge by studying the interplay between human cognition, visual behavior and security
- B. Apply the gained knowledge to design innovative approaches
- C. Evaluate the added value of the new approaches in the context of user studies


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Case Study

- **Effects of human cognition and visual behavior on password security**
  - Katsini, C., Fidas, C., Raptis, G., Belk, M., Samaras, G., Avouris, N. (2018). Influences of human cognition and visual behavior on password security during picture password composition. ACM SIGCHI Human Factors in Computing Systems (CHI 2018), ACM Press, paper 87



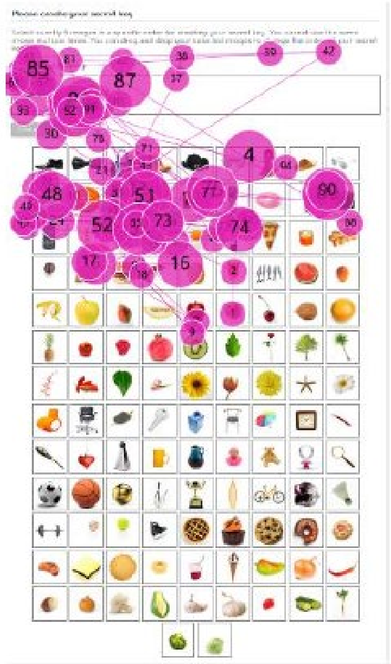
This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

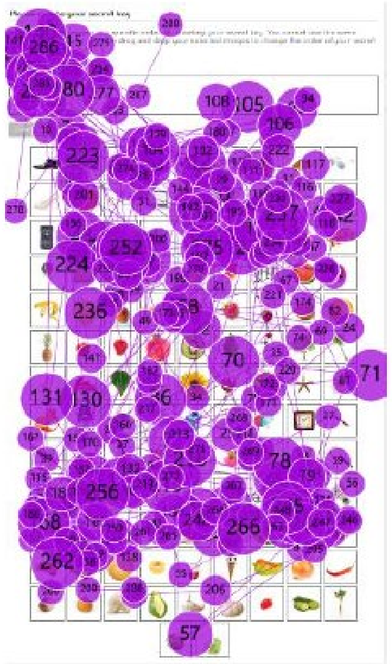
CONTENT 8

# Influences of Human Cognition and Visual Behavior on Password Strength

- **Graphical password composition embraces visual information processing and determines security**

- We adopt a cognitive psychology perspective and investigate how users react to stimuli, through analyzing their visual behavior, aiming to understand how they decide on the graphical passwords they create







This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Field Dependence-Independence

- Field Dependence-Independence is a cognitive theory interrelated with the visual behavior of users
- Reflects how individuals retrieve, recall, process and store graphical information



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Field Dependence-Independence

**Field dependent**

Follow a more holistic approach to process visual information

They have difficulties in identifying details in complex visual scenes

**Field independent**

Follow a more analytical approach to process visual information

Pay attention to details

Easily separate simple structures from the surrounding visual context

Co-financed by the European Union
Connecting Europe Facility

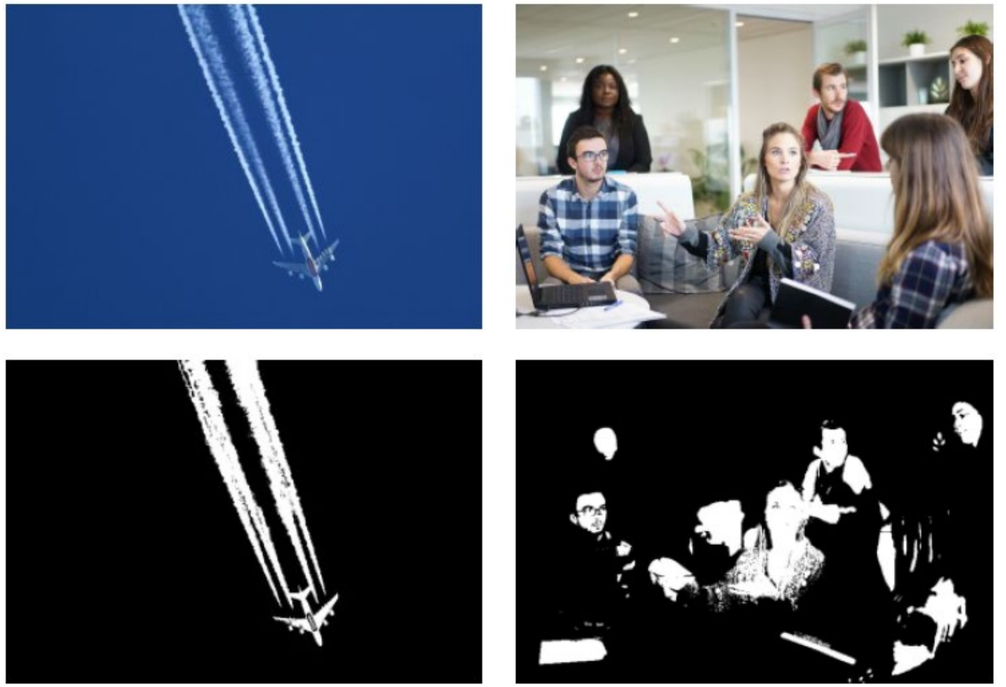


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Image Complexity – Attention Points

- Image complexity is known to affect password strength and gesture combinations
- We intentionally decided to provide two images of different complexity (in terms of number of attention points)
- Images of different complexity used in the study, a simple image showing a jet (left), and a complex image showing a workplace (right). At the bottom, the saliency maps of the images are depicted





This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Hypotheses

- **$H_{01}$**. There is no significant difference on the strength of the created graphical passwords between field-dependent (FD) and field-independent (FI) individuals across background images of varying complexity

- **$H_{02}$**. There is no correlation between the strength of the created graphical passwords and the visual behavior of field-dependent (FD) and field-independent (FI) individuals across background images of varying complexity



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Hypotheses

FD ↔ FI

FD ↔ FI

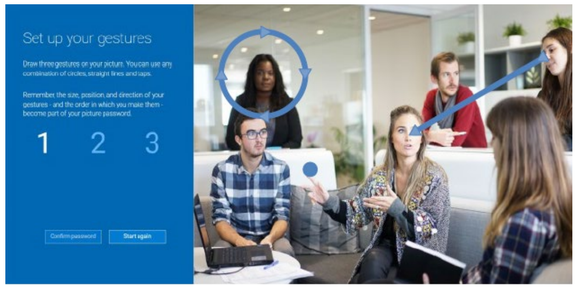
Between-subjects analysis with security as a dependent variable



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Study Instruments




- Graphical User Authentication Scheme
  - We used Windows™ Picture Gesture Authentication
  - Draw a combination of tabs, circles, straight lines to login


- Equipment
  - Tobii Pro Glasses 2
  - Fixations were extracted using a velocity threshold identification (I-VT) algorithm by Tobii

Co-financed by the European Union
Connecting Europe Facility

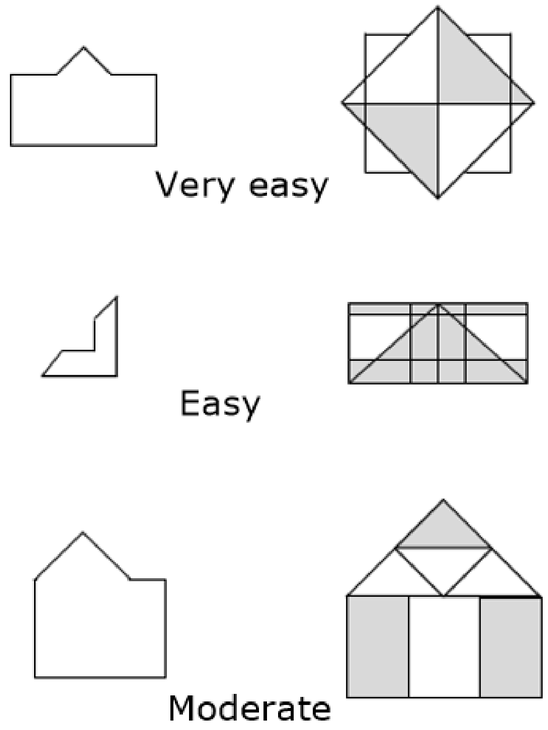


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Study Instruments

- Cognitive Style Elicitation Test
  - Group Embedded Figures Test (GEFT)
  - Consists of 18 pattern-recognition tasks
  - Identify a given pattern within a complex context
  - The higher the score, the more field independent you are




Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Eye-Gaze Metrics

- Fixation duration: total duration of fixations of an individual within an area of interest (AOI), considering visits and revisits to the AOI
  - sum, mean, max, and std.
- Fixation count: total number of fixations of an individual within each AOI, considering visits and revisits to the AOI
- Saccade length: distance between rapid eye movements from one fixation to another
  - sum, mean, max, and std.

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Password Strength Metric

- We adopted **password guessability**, a widely used metric for measuring password strength
- We used a brute-force approach based on the attention points of each background image
- Our brute-force algorithm started from the segments covering the attention points, next checked the neighboring segments, and finally checked the rest of the image segments
- The password strength was measured in number of guesses required to crack each password

Co-financed by the European Union
Connecting Europe Facility

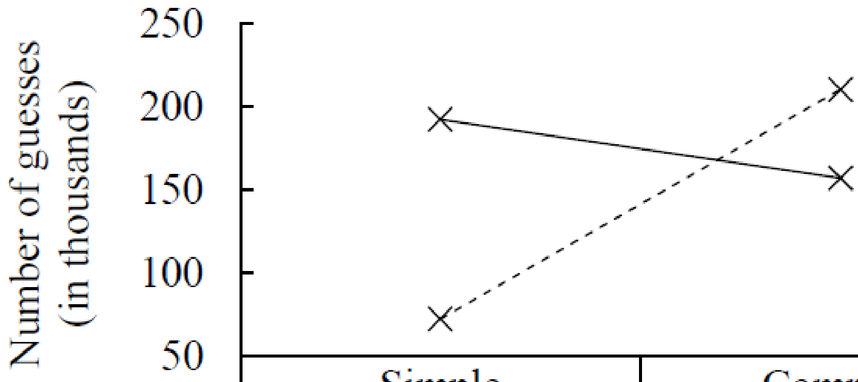


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results: Password Strength Differences among FD/FI

- Mixed ANOVA revealed a significant interaction between the effects of the FD-I cognitive style and the image complexity on the strength of the created passwords, $F = 4.183$, $p = .041$, $\eta 2 = .166$




| | Simple | Complex |
|---|---|---|
| FD | 192.345 | 157.124 |
| FI | 72.305 | 210.526 |


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results: Password Strength Differences among FD/FI

- Pairwise comparisons revealed that 120K fewer guesses were required to crack the passwords of the FIs when using the simple back-ground image compared to the FDs when using the simple background image (p = .042)
- FD: no significant differences were revealed between the passwords created using the two images
- FI: 138K more guesses were required to crack the passwords created using the complex background image compared to those created using the simple background image (p = .028)

Co-financed by the European Union
Connecting Europe Facility



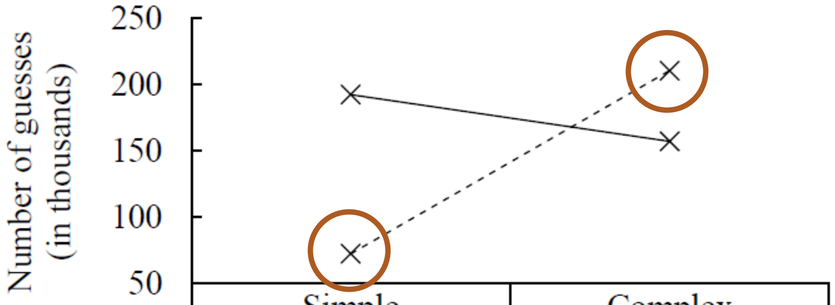
This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Main Findings

## FI Users

- **In low complex images**, FI users cannot create secure passwords due to their inherent visual behavior attitudes to focus on the attention points of the image
- **In high complex images**, there is a significant increase of security which also highlights the interplay between human cognitive attributes in visual search and image complexity towards security

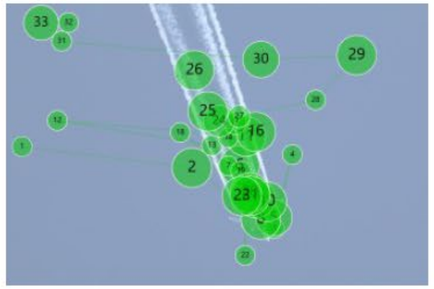
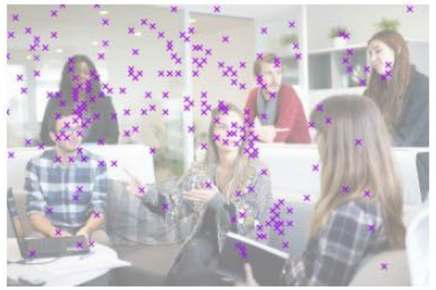



| | Simple | Complex |
|---|---|---|
| FD | 192.345 | 157.124 |
| FI | 72.305 | 210.526 |


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Interpretation of Results

| FIXATION DURATION | | FIXATION COUNT | |
|---|---|---|---|
|  |  |  |  |
|  |  |  |  |
| Field Dependent | Field Independent | Field Dependent | Field Independent |



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Interpretation of Results

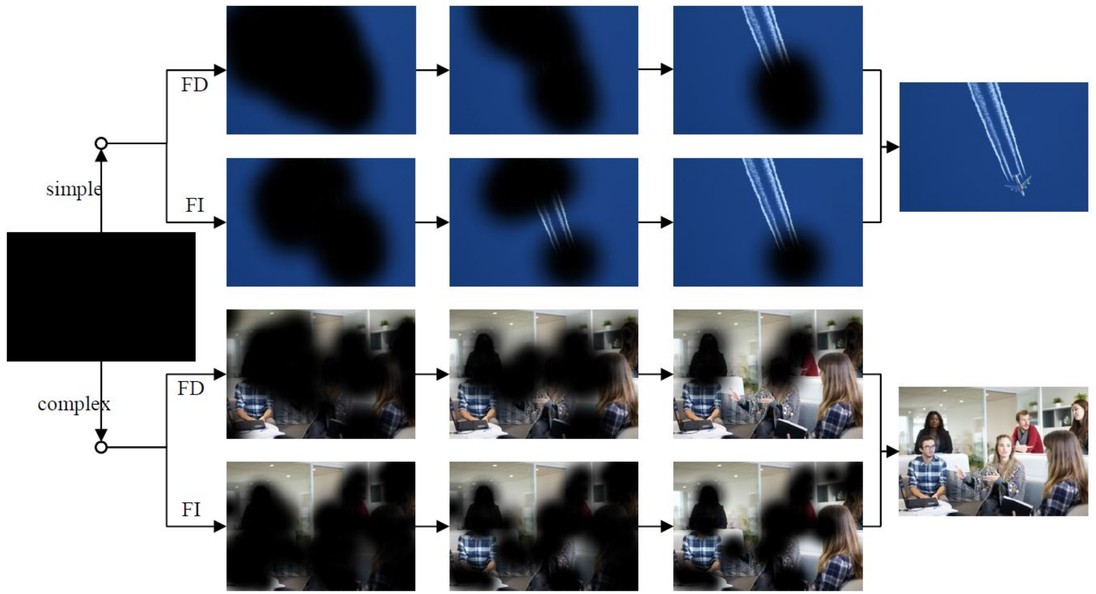
- Main effects of FD-I on visual behavior: Statistically significant effect for the number of fixated segments ($F = 5.358$, $p = .031$, partial $\eta 2 = .203$), the number of fixations ($F = 5.859$, $p = .025$, partial $\eta 2 = .218$), fixation duration ($F = 4.694$, $p = .042$, partial $\eta 2 = .183$)
  - FDs produced 22.085 (95% CI, -.384 to 44.553, $p = .041$) more fixations than FIs on the simple background image
  - FDs fixated for 11.442 (95% CI, 3.559 to 17.194, $p = .037$) more seconds on the simple background image than the FIs
  - FDs fixated on 26.910 (95% CI, -1.725 to 55.545, $p = .043$) more segments in the simple background image than FIs



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Adaptive GUA Scheme based on Saliency Masks




- The image is totally covered at the beginning, and then the successive saliency levels based on the eye-tracking data of each cognitive group fade-out within 20 seconds


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

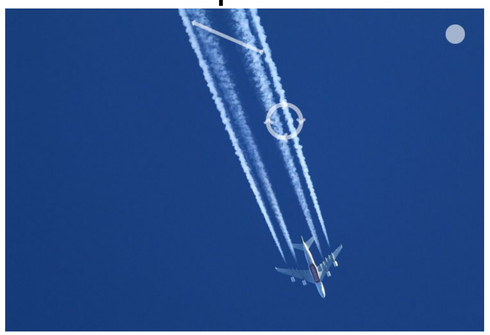
# FI: Password Selections Without vs. With Adaptive Masks

Without Adaptive Masks

72K guesses to crack

210K guesses to crack

With Adaptive Masks



137K guesses to crack

291K guesses to crack

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Special Topic in Adaptive Usable Security: On Flexible and Personalized User Authentication in Patient-centric Healthcare Systems

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

# Serums: Securing Medical Data in Smart Patient-Centric Healthcare Systems

- 3-year EU H2020 Project (€4.47M)
  - Started on 1st January 2019
  - https://www.serums-h2020.org
- The goal: Build a personalized patient-centric healthcare system, enhancing the personal care of patients, and maximizing the quality of treatment they can receive, while ensuring trust in the security and privacy of their medical data.



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

# Serums: Securing Medical Data in Smart Patient-Centric Healthcare Systems

- Project partners

University of St Andrews
zuyderland
IBM
sopra steria
FUNDACIÓ CLÍNIC BARCELONA
accenture
scch software competence center hagenberg
Πανεπιστήμιο Κύπρου University of Cyprus
UCL Université catholique de Louvain
University of Dundee



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Serums Aims

- Aim 1: Integrate out-of-hospital personal medical care with centralised hospital systems, including general practitioner and special consultant provision, into a new form of smart, patient-centric healthcare
- Aim 2: Establish trust in the correct operation of smart, patient-centric healthcare systems by developing techniques for safe, secure and anonymous sharing of data
- Aim 3: Ensure the patient has full control over their personal data in accordance to GDPR and other regulatory frameworks
- Aim 4: Demonstrate effectiveness and generality of Serums techniques on multiple disparate use cases

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Serums Technologies

- Smart Patient Records for representation of distributed medical data
- Blockchain Technology for controlling access to sensitive data
- Distributed Privacy-Preserving Learning for distributed data analytics
- Flexible User Authentication for secure, personalised and usable authentication and authorisation
- Data Fabrication for Medical Data for generating synthetic but realistic patient record
- Data Cloaking for Medical Data for masking the data to allow safe transmission over untrusted networks
- Semantic-Preserving Encryption to allow advanced data analytics while preserving data privacy


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Serums Technologies

- Smart Patient Records for representation of distributed medical data
- Blockchain Technology for controlling access to sensitive data
- Distributed Privacy-Preserving Learning for distributed data analytics
- **Flexible User Authentication for secure, personalised and usable authentication and authorisation**
- Data Fabrication for Medical Data for generating synthetic but realistic patient record
- Data Cloaking for Medical Data for masking the data to allow safe transmission over untrusted networks
- Semantic-Preserving Encryption to allow advanced data analytics while preserving data privacy


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

# Develop new authentication and trust mechanisms for medical data

Deliver **secure and personalized authentication mechanisms** that adapt to each user's preference, in order to ensure **patients' trust** and achieve a viable equilibrium between **security and usability**

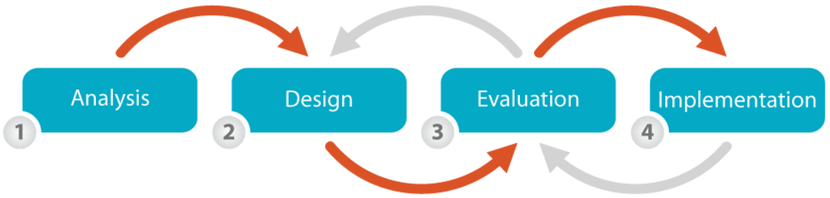


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# User-centered Design Method

- The UCD method will embrace three iterative cycles leading to three different system prototype releases
  - low-fidelity, high-fidelity, final release
- Each iteration entails an analysis, design, implementation and integration, ending with an evaluation of derived prototypes providing thus valuable feedback for designing the next release
- Evaluation is a cornerstone concept throughout



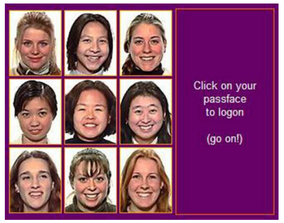


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# State-of-the-Art

- Textual passwords are widely applied in the healthcare domain
- Knowledge-based authentication will prevail in the next decade [Herley & van Oorschot]
  - in combination with other approaches (e.g., token, biometric)
- Several attempts to find alternative solutions
  - Graphical passwords
  - MFA with tokens





This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# State-of-the-Art

- Ineffective practice of usability in such tasks does not naturally embed the users' characteristics and context of use in the design process [Biddle et al.; Belk et al.]
- Users prefer and perform differently in knowledge-based authentication [Mare et al.]
  - any specific solution might not please everyone



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Flexible & Personalized Authentication

Move from current generic “one-size-fits-all” authentication systems
to **flexible, user-adaptable authentication systems**

- Provide a viable and flexible authentication solution
  - State-of-the-art practices in the healthcare domain
  - Applicable within the consortium’s end-user organizations

Belk, M., Fidas, C., Pitsillides, A. (2019). **FlexPass: Symbiosis of seamless user authentication schemes in IoT**. *ACM SIGCHI Human Factors in Computing Systems (CHI EA 2019)*, ACM Press, doi: 10.1145/3290607.3312951



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Flexible & Personalized Authentication

- Challenges
  - Easily transfer from the state-of-the-art towards the new approach
  - Our solution should include textual passwords as an option
  - Avoid changing the current practice
    - Users are familiar with textual passwords
  - Personalization – provide the option to users to switch the authentication type

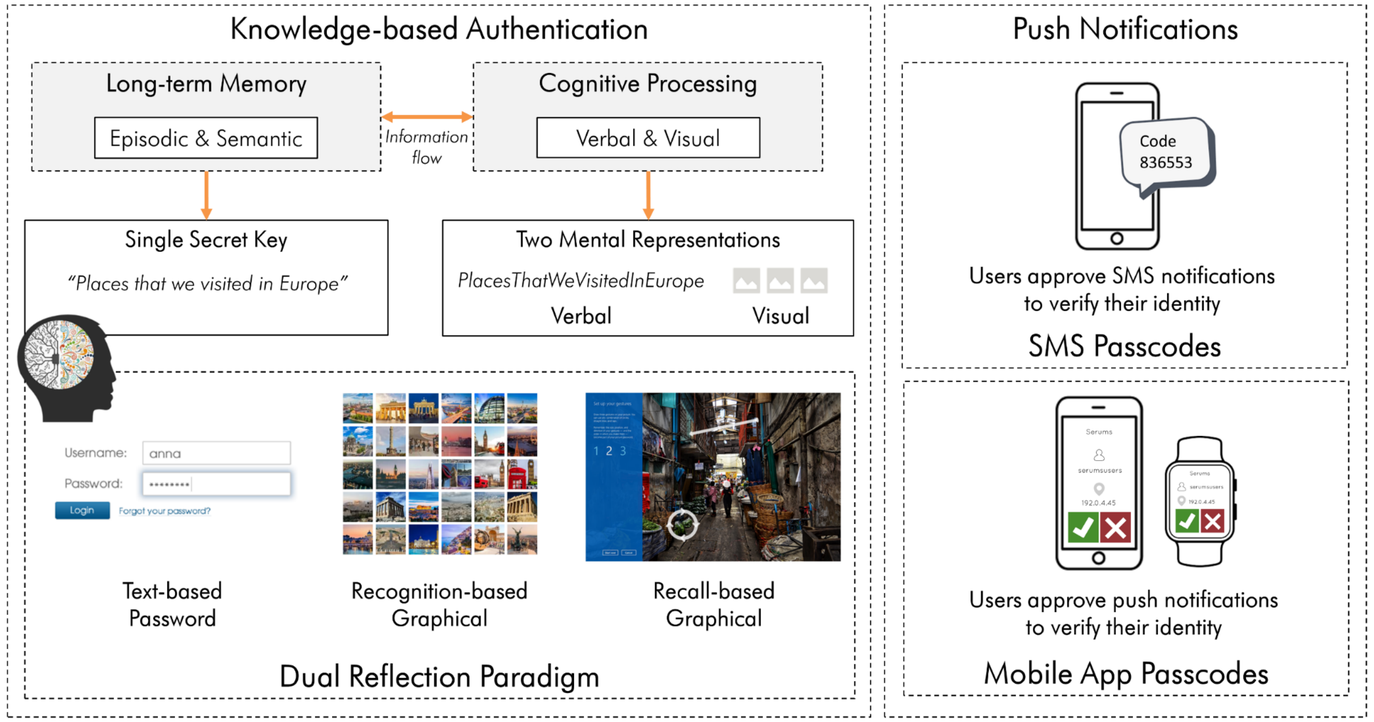
Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Flexible & Personalized Authentication






This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Flexible & Personalized Authentication

- Aim
  - Design and develop an authentication system that combines textual and graphical passwords under a flexible authentication paradigm
- Concept
  - Use a single, user-selected secret that can be reflected in both textual and graphical passwords
- Additional security layer – two-factor authentication
  - Mobile application
    - Push notifications
    - Time-based One Time Passwords (TOTP)
  - Allows users to approve the notifications to verify their identity

Co-financed by the European Union
Connecting Europe Facility

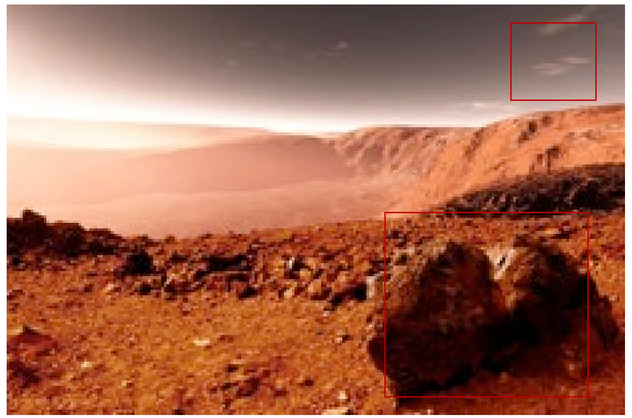


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Retrospective Graphical Passwords

- Image semantics affect security strength of user-chosen passwords
- Type of images
  - Generic: not directly relevant nor familiar to the users, e.g., abstract, nature, landscapes, etc.
    - susceptible to hotspots
    - creating predictable passwords
    - [Thorpe & van Oorschot; Bulling et al.; Alt et al.; Belk et al.]



**Generic Image**

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Retrospective Graphical Passwords

- Personal: directly relevant and highly familiar to the users, e.g., depicting people, objects, or scenes highly personal to users
  - creation of passwords easily guessable by someone who knows the user
  - users often use personal photos that violate the privacy of others depicted in the photo, as well as theirs, since private information is revealed during login
  - [Tullis & Tedesco; Wiedenbeck et al.; Schaub et al.; Ahern et al]

**Personal Image**



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Retrospective Graphical Passwords

**Need for a more sophisticated approach within graphical password schemes to achieve a better tradeoff between security and memorability** *[Biddle et al.]*

- State-of-the-art approaches embrace deficiencies
  - Random image delivery: users tend to choose easy-to-remember and predictable hotspots [Tullis & Tedesco; Renaud]
  - Users upload their image: users tend to create easily guessable passwords [Tullis & Tedesco] and often violate the privacy of people depicted in the uploaded images [Ahern et al.]

Constantinides, A., Fidas, A., Belk, M., Pietron, A.M., Han, T., Pitsillides, A. (2020). **From hot-spots towards experience-spots: Leveraging on users' sociocultural experiences to enhance security in cued-recall graphical authentication**. *International Journal of Human-Computer Studies*, Elsevier

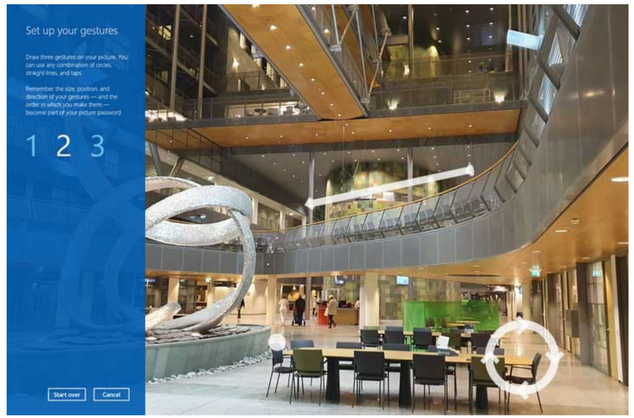


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Retrospective Graphical Passwords

- A retrospective-based approach for graphical password schemes
  - Deliver images to end-users, which depict sceneries that reflect users' prior experiences, thus moving from hot-spot selections towards experience-spots
  - Expand the state-of-the-art spectrum; not too generic nor too personal

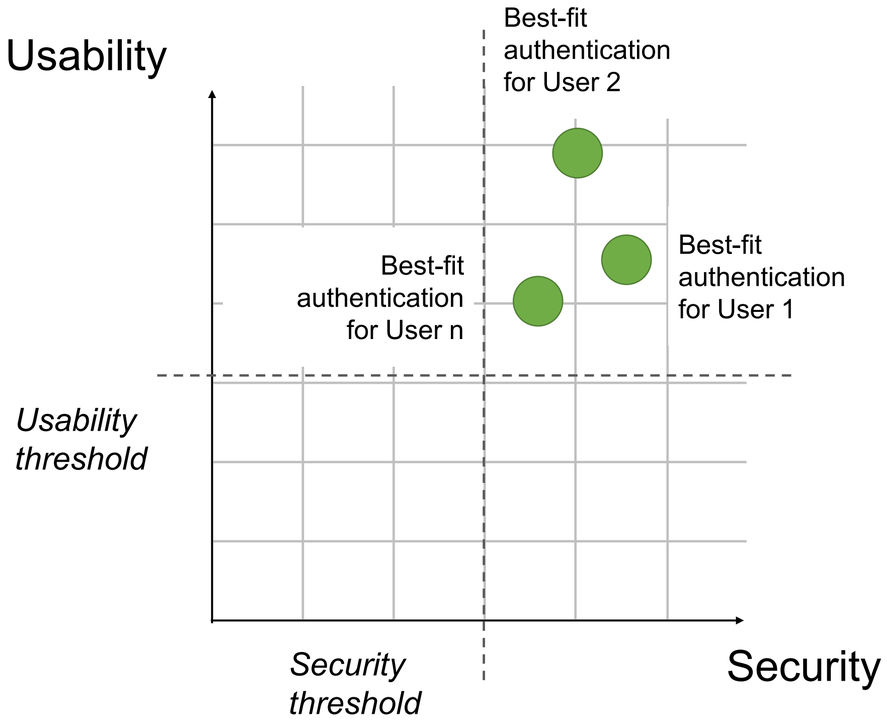



**Retrospective approach**


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# On Adaptable Authentication Policies




- **Security Metrics**
  - Key space
  - Entropy
  - Guessability
  - Password complexity
  - Shoulder surfing
- **Usability Metrics**
  - Task completion efficiency & effectiveness
  - Memorability – memory time
  - Perceived usability, memorability
  - Perceived security, trust

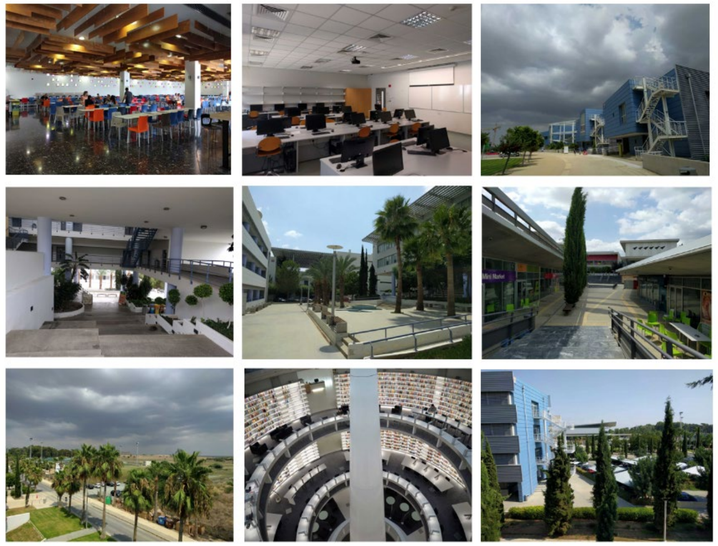


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# User Evaluation Study

- Two between-subjects user studies with students
  - Study 1 – Security: Eye tracking study (n=42)
  - Study 2 – Memorability: Two-week study (n=36)
- Procedure
  - Participants created a picture password on images
    - Content related to their prior experiences (University campus)
    - Content unfamiliar to the users



**University Campus**

Is there a significant **improvement in the security strength and memorability** of the created graphical passwords between the experimental group ***(retrospective images – suggested approach)*** and control group ***(generic images – state-of-the-art approach)***?



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# User Evaluation Study

- Metrics
  - Security strength: number of guesses required to crack a password
    - Points of Interests-assisted attack model [Sadovnik & Chen; Zhao et al.]
  - Memory time: greatest length of time between password creation and a successful password login using the same graphical password

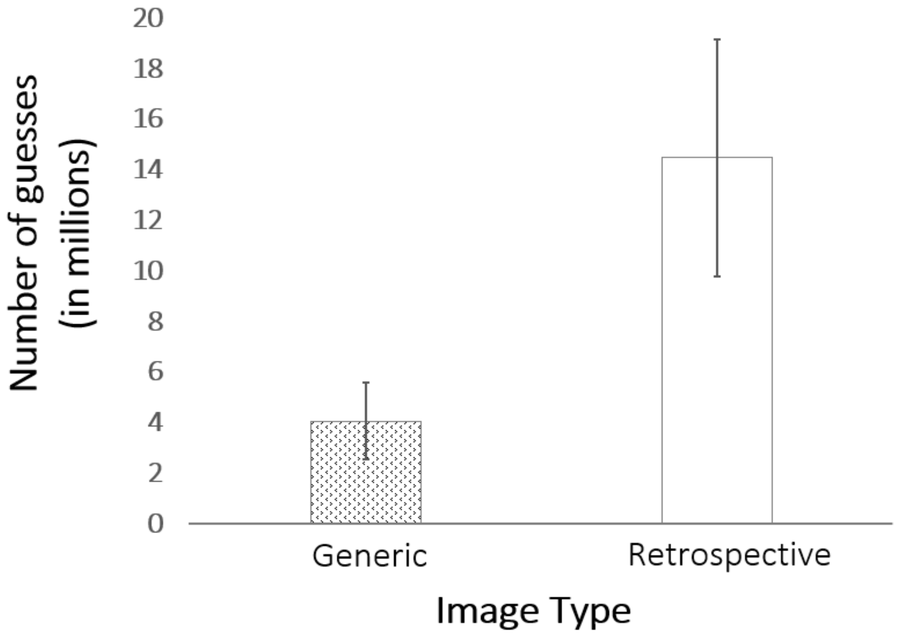


This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

- Security Strength – PoI-assisted Brute-force Attack
  - Retrospective group required more guesses to crack (14.49 ± 4.69M) than users of the generic group (4.09 ± 1.5M)
    - statistically significant difference of 9.8 ± 4.3M (95% CI, .746 to 1.88), t(21.513)=2.248, p=.035





This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

- Memorability – memory time
  - Retrospective group: 267 hours
  - Generic group: 258 hours
    - No statistically significant differences p>.05

Co-financed by the European Union
Connecting Europe Facility

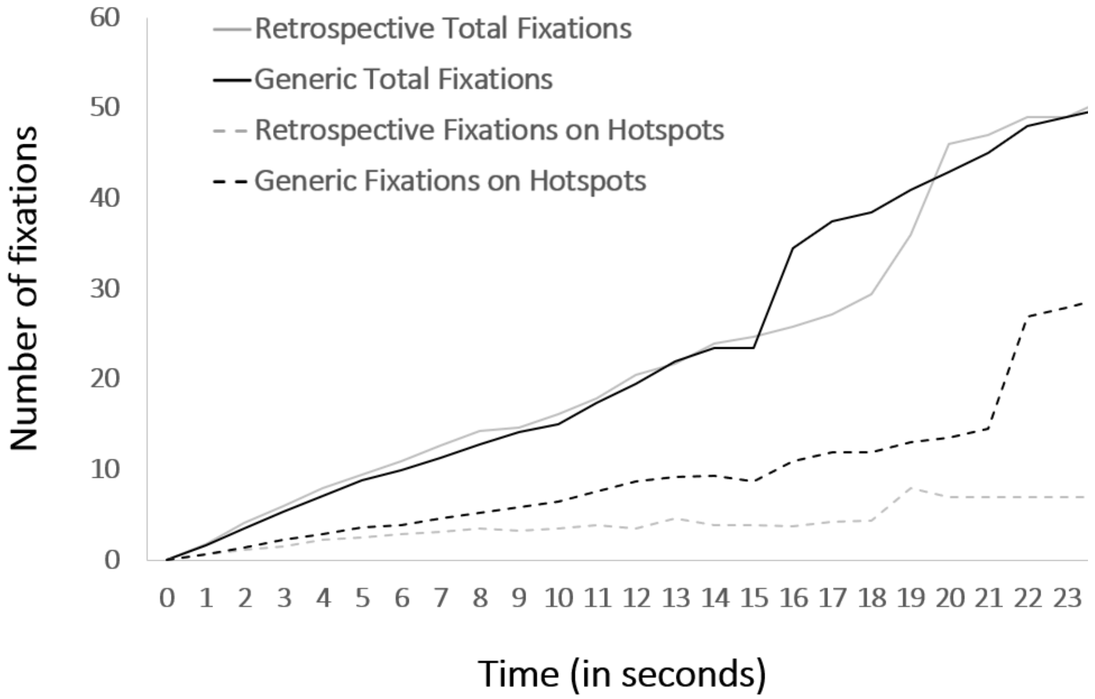


This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

- Visual Behavior – proportion of fixation count on hotspots
  - Generic group exhibited higher proportion of fixation count on hotspots (0.417 ± 0.148) than the retrospective group (0.224 ± 0.171)
    - statistically significant difference F(2, 27)=6.217, p=.006; Wilks' Λ=.685; partial η2=.315




Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# User Evaluation Study with Patients

- Aim
  - Evaluate patients' likeability, perceived usability, security and trust towards the initial FlexPass user authentication system
- Two User Studies
  - 55 participants
- Procedure
  - Step 1 – Create Picture Password
  - Step 2 – Create Textual Password (optional)
  - Step 3 – Login and Approval
  - Step 4 – Answer Questionnaire

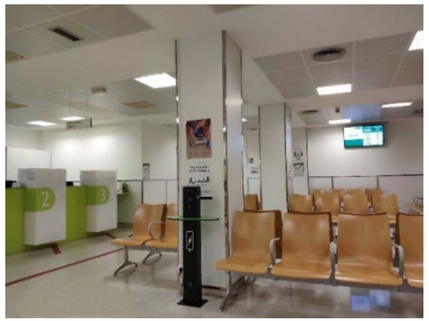
Co-financed by the European Union
Connecting Europe Facility



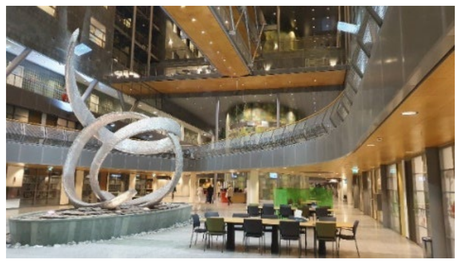
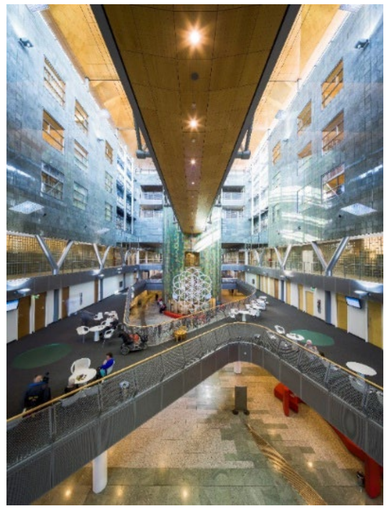
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

## CONTENT 8

### Public images from partner hospitals

### Public images from partner hospitals



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

| Likeability | Extremely | Very | Moderately | Slightly | Not at all |
|---|---|---|---|---|---|
| Study A | 18 | 9 | 2 | 2 | 1 |
| Study B | 2 | 11 | 7 | 3 | 1 |
| **Total** | **20** | **20** | **9** | **5** | **2** |

**72%**



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

- Perceive the system as secure (76%)

- Password creation is easy to use (64%), moderately easy to use (25%)
  - 6/55 (11%) reported difficulties in creating the password
    - Users are not familiar with the new paradigm
    - Further design improvements are required in the password creation phase



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 8

# Results

- Login is easy to use (74%) with low mental demand (72%) in recalling the password
  - 9/55 (16%) reported high mental demand
    - Could be explained by the fact that some users were older adults, not experienced in using technologies
- Users could effectively recall their password (80%)
- Users trust the technology (75%) and its ability to keep their data private and secure (73%)
- The majority of users (78%) would like to use FlexPass as an alternative password system

Co-financed by the European Union
Connecting Europe Facility



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

# Thank you.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423