Co-funded by the
Erasmus+ Programme
of the European Union

Learning Teaching Training Activity (LTTA)
Intellectual Output 1 - Needs Analysis and Design of the Theoretical Framework for Continuous Student Identity Management

Argyris Constantinides, University of Cyprus

Intellectual Output 1 (IO1)

Co-funded by the
Erasmus+ Programme
of the European Union

- Needs Analysis and Design of the Theoretical Framework for Continuous Student Identity Management

- *Lead:* University of Patras
- *Participating Partners:*
  - University of Cyprus
  - Cognitive UX GmbH
  - University of Coimbra ISR

- *Output type:* Methodologies / guidelines – Methodological framework for implementation
- *Media:* Publications, Other, Dataset

IO1 - Key Activities and Tasks

- Started in early stages of the project working aiming to lay the foundations for implementing the continuous student identification framework

- Conduct a thorough literature review analysis in relevant key areas of the project
  - Identify and analyze state-of-the-art works of identity management within the HEI domain
  - Identify security metrics, policies and procedures that are currently applied in HEIs
  - Investigate state-of-the-art approaches in AI and ML with regards to continuously and unobtrusively identifying end-users based on voice, face and user interaction features
- Triangulate results of the literature review analysis
  - Conduct a series of semi-structured interviews with key stakeholders of the participating universities (*e.g.*, policy makers, administrators, security officers, etc.)
  - Identify the currently applied procedures and policies of identity management and authentication, the technologies and online learning platforms that are currently used in each university

IO1 – Target Groups

Co-funded by the
Erasmus+ Programme
of the European Union

- Stakeholders of HEIs
  - Institutional policy makers
  - Strategic planners
  - Administration
  - Teaching staff
  - Government

- Outcomes will be valuable
  - Researchers and practitioners working in the area of intelligent and continuous user identification
  - Class instructors (*e.g.*, Professors, Lecturers, etc.)
  - System administrators of HEIs

IO1 – Key Objectives

Co-funded by the
Erasmus+ Programme
of the European Union

- Conduct needs analysis of students, teachers and academic policy makers related to continuous student identity management
- Define security metrics and policies for continuous student identity management
- Set the specifications of the framework by considering privacy aspects within diverse online learning/academic scenarios
- Design a multi-dimensional user model for continuously identifying end-users based on a variety of inputs (voice, image, user interaction)
- Triangulate and combine findings from literature and real-world case studies in three different HEIs

IO1 - Tasks and Task Leaders

Co-funded by the
Erasmus+ Programme
of the European Union

- Task 1.1: Needs Analysis on Identity Management in HEIs
  - *Lead:* University of Coimbra
  - *Participating:* University of Patras, University of Cyprus, Cognitive UX GmbH
- Task 1.2: Needs Verification at HEIs
  - *Lead:* University of Patras
  - *Participating:* University of Cyprus, Cognitive UX GmbH, University of Coimbra
- Task 1.3: Specification of the Framework
  - *Lead:* Cognitive UX GmbH
  - *Participating:* University of Patras, University of Cyprus, University of Coimbra

Task 1.1: Needs Analysis on Identity Management in HEIs

Co-funded by the Erasmus+ Programme of the European Union

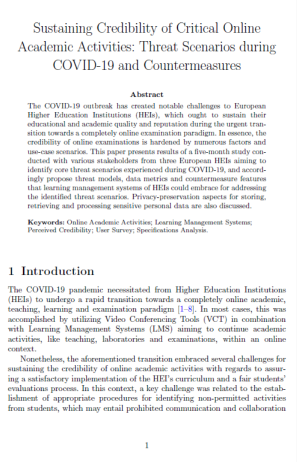
- *Aims*
  - Identify important security metrics and policies of the domain
  - Identify current best practices and guidelines in the area of intelligent biometric authentication and identification within the online/distance learning domain

- Conduct a thorough literature review analysis of the state-of-the-art area of usable privacy and security, intelligent user interfaces, distance learning, etc.
- Investigate existing voice, image and interaction behavior approaches for continuously identifying end-users

Task 1.2: Needs Verification at HEIs

- *Aims*
  - Verify the needs analysis with the active involvement of the participating HEIs
  - Identify the current authentication and identity management practices and their drawbacks within the online/distance learning domain

- Conduct a series of semi-structured interviews with stakeholders with the university partners
  - *Sample:* 31 stakeholders participated from all partner HEIs



Sustaining Credibility of Critical Online Academic Activities: Threat Scenarios during COVID-19 and Countermeasures

Abstract

The COVID-19 outbreak has created notable challenges to European Higher Education Institutions (HEIs), which ought to sustain their educational and academic quality and reputation during the urgent transition towards a completely online examination paradigm. In essence, the credibility of online examinations is hardened by numerous factors and use-case scenarios. This paper presents results of a five-month study conducted with various stakeholders from three European HEIs aiming to identify core threat scenarios experienced during COVID-19, and accordingly propose threat models, data metrics and countermeasure features that learning management systems of HEIs could embrace for addressing the identified threat scenarios. Privacy-preservation aspects for storing, retrieving and processing sensitive personal data are also discussed.

Keywords: Online Academic Activities; Learning Management Systems; Perceived Credibility; User Survey; Specifications Analysis.

1 Introduction

The COVID-19 pandemic necessitated from Higher Education Institutions (HEIs) to undergo a rapid transition towards a completely online academic, teaching, learning and examination paradigm [1–8]. In most cases, this was accomplished by utilizing Video Conferencing Tools (VCT) in combination with Learning Management Systems (LMS) aiming to continue academic activities, like teaching, laboratories and examinations, within an online context.

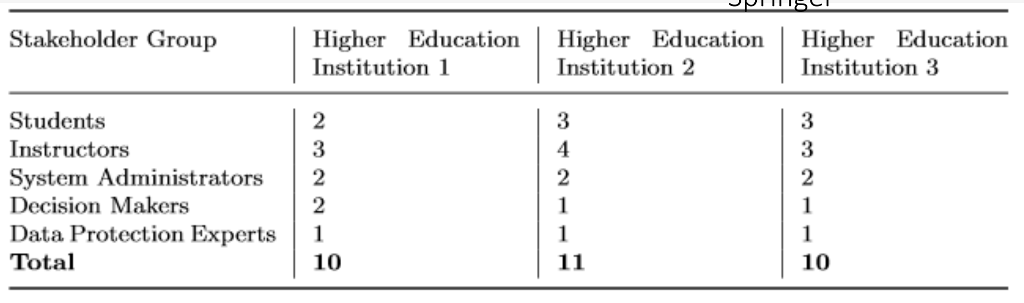
Nonetheless, the aforementioned transition embraced several challenges for sustaining the credibility of online academic activities with regards to assuring a satisfactory implementation of the HEI's curriculum and a fair students' evaluations process. In this context, a key challenge was related to the establishment of appropriate procedures for identifying non-permitted activities from students, which may entail prohibited communication and collaboration

1

Journal submission: ”Sustaining Credibility of Critical Online Academic Activities: Threat Scenarios during COVID-19 and Countermeasures”, Universal Access in the Information Society Journal, Springer

Three-phase methodology

- **Phase A:** Needs Analysis
- **Phase B:** Needs Verification Analysis
- **Phase C:** Countermeasures and Features



Stakeholder Group	Higher Education Institution 1	Higher Education Institution 2	Higher Education Institution 3
Students	2	3	3
Instructors	3	4	3
System Administrators	2	2	2
Decision Makers	2	1	1
Data Protection Experts	1	1	1
Total	**10**	**11**	**10**

Phase A – Needs Analysis (2 months)

Co-funded by the
Erasmus+ Programme
of the European Union

- Needs analysis on how HEI stakeholders perceive the credibility of critical academic activities during the COVID-19 period and identify threat scenarios and malicious activities of students during critical academic activities

- Sampling and Procedure
  - *Participants:* Thirty-one (31) participants from three European universities
  - *Stakeholder profiles:* Students; Instructors; System Administrators; Decision Makers; Data Protection Experts *Semi-structured interviews:* We conducted a series of semi-structured interviews with each participant that lasted approximately 60 minutes each, discussing around different topics based on the research questions

Phase B – Needs Verification Analysis (2 months)

Co-funded by the Erasmus+ Programme of the European Union

- Verify the outcome of the needs analysis and prioritize the identified threat scenarios in terms of importance and severity with HEI stakeholders

- **Sampling and Procedure**
  - *Participants:* Seven (7) participants from the same three European universities
  - *Stakeholder profiles:* Students; Instructors; System Administrators; Decision Makers; Data Protection Experts
  - *Semi-structured interviews:* We conducted a series of semi-structured interviews with each participant that lasted approximately 60 minutes each in which each participant verified the outcome of the needs analysis and prioritized the identified threat scenarios in terms of importance and severity.
    - Through the analysis we also identified challenges for adoption and relevant privacy issues with regards to such technologies

Phase C – Countermeasures and Features (2 months)

Co-funded by the
Erasmus+ Programme
of the European Union

- Identify requirements and propose countermeasure features of the framework to be implemented for addressing the identified threat scenarios during critical academic activities

- **Countermeasures** related to student identification and verification, continuous student identification, monitoring the student’s digital context, monitoring the student’s behavior within the physical context, intelligent insights through data analytics

- **Features** for addressing the identified threats and fulfilling the countermeasure requirements

Research Questions

- *RQ_1.* How did the stakeholders perceive the credibility of online examinations and other critical academic activities during the COVID-19 period (March 2020-August 2021)?

- *RQ_2.* Which threat scenarios that include impersonation activities of students should be urgently addressed during online examinations?

- *RQ_3.* Which threat scenarios that include forbidden communication, collaboration and/or resource access activities of students should be urgently addressed during online examinations?

Deployed tools of HEIs during critical academic activities

- In-house developed LMS systems
- Nation-wide developed LMS systems
- Off-the-shelf (e.g., Moodle) LMS systems
- LMS have been used during the COVID-19 period, adapted to the current situation

- All universities have a common pattern for student identification purposes
  - Tools for conducting meetings are used for student identification purposes, *e.g.*, Zoom, Microsoft Teams, etc.

- Identified three main type of examinations
  - Oral
  - Written online
  - Written hardcopy

Phases in an Online Examination

Student Identity Verification

Examination Session

Perceived Credibility of Online Examinations during COVID-19 (*RQ_1*)

Co-funded by the
Erasmus+ Programme
of the European Union

- Consensus among all participants/stakeholder groups that the current workflows and deployed Information and Communication Technologies (ICT) tools embrace vulnerabilities and therefore threaten the credibility of critical online academic activities, such as, online examinations

- Absence of validated procedures in COVID-19 realms compared to pre-COVID-19 validated procedures in which critical academic activities were conducted within controlled physical realms

Perceived Credibility of Online Examinations during COVID-19 (*RQ$_1$*)

- From a decision maker's perspective, responses revealed that all are **very well aware of the limitations of the current examination methods** and are **working towards improving the LMS features** to address malicious activities, like plagiarism comparisons
  - One policy maker stressed that the current online examination procedures entail a high number of threat scenarios, which makes this attempt very difficult to reach the standards of physical examinations

- From an instructor's perspective, responses revealed that the online examination procedures had an **effect on emotional and ethical aspects of instructors** since they could not assure the fairness among students who were well-prepared for examinations and students who misused the limitations of the currently applied online examination procedures

- From a student's perspective, all students **agreed about questioning the current procedures** within critical online academic activities, nonetheless, some students mentioned that the online-based procedure was **easier and more convenient than the conventional physical examination**

Threat Scenarios in Online Academic Activities within Existing Learning Management Systems

Co-funded by the
Erasmus+ Programme
of the European Union

Phases in an Online Examination

Student Identity Verification

Examination Session

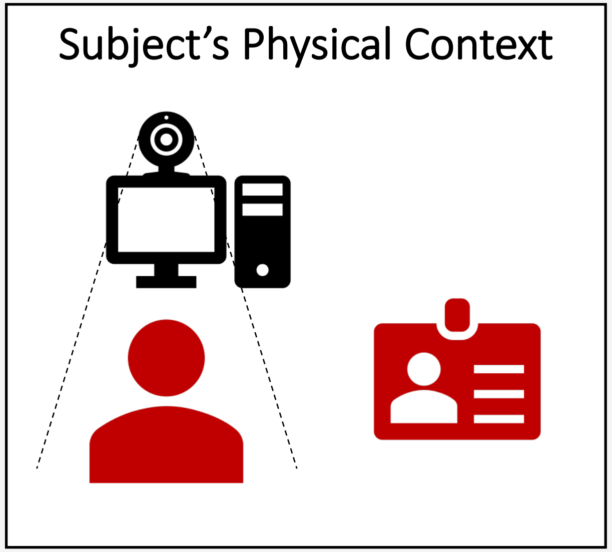
Threat Scenarios

- **Impersonation activities**, refer to actions of a person imitating or replicating the behavior or actions of another person.
- These scenarios can happen **during the student identification phase** or even **throughout the examination session**, *e.g.*, subject fakes his/her identity proofs during enrolment

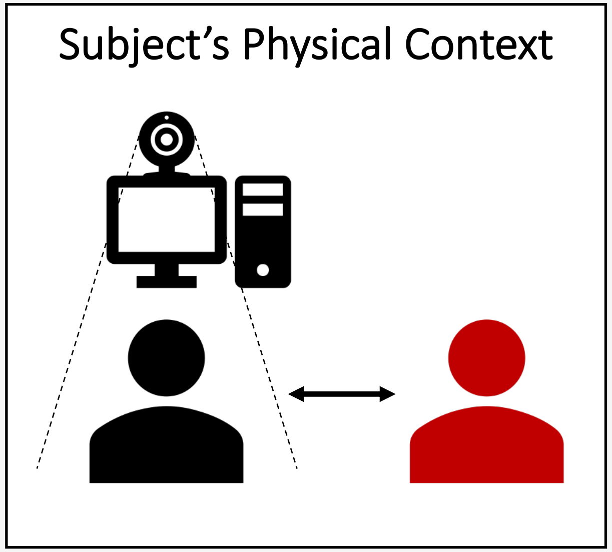
- **Forbidden collaboration and/or communication scenarios with other persons**, either within the physical or remote context
  - **In-situ** collaboration activities: related to suspicious activities that take place in the subject's physical context
  - **Computer mediated** collaboration activities: related to suspicious activities that involve remote collaboration and/or communication with other persons
- **Forbidden access to material**, either within the physical or remote context

Identification of Impersonation Threat Scenarios *(RQ_2)*

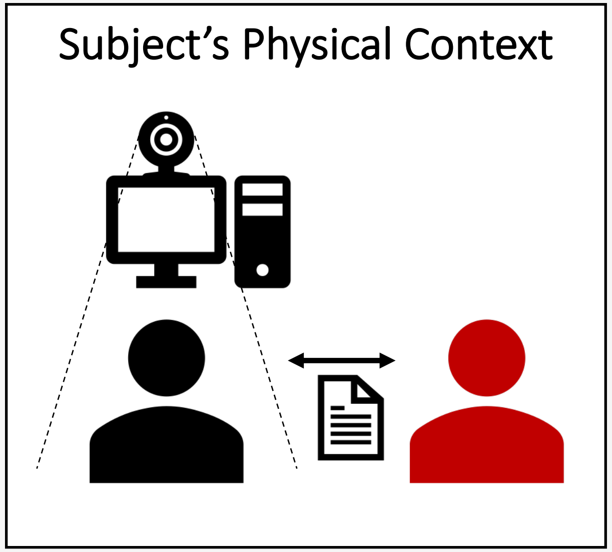
Co-funded by the
Erasmus+ Programme
of the European Union



Subject fakes his/her identity proofs during enrolment



Subject switches seats with another person after enrolment

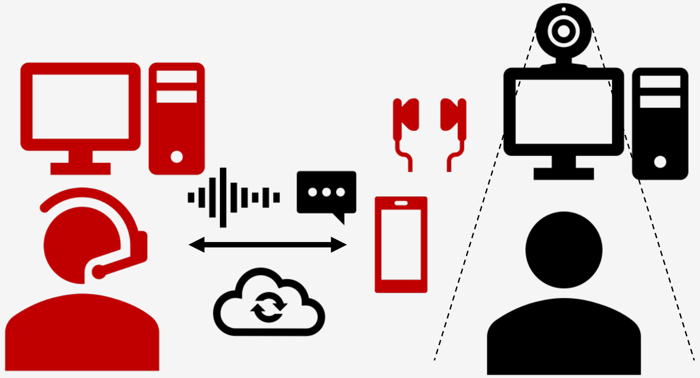


Exchange of hardcopy written messages

Identification of Communication, Collaboration and Resource Access Threat Scenarios *(RQ_3)*

Co-funded by the
Erasmus+ Programme
of the European Union

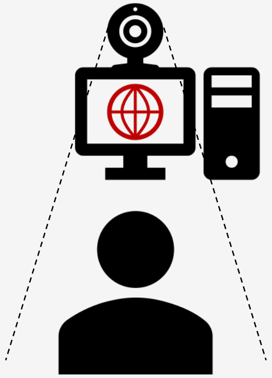
- Computer Mediated Scenarios



Remote communication/collaboration between a smartphone or another computer of the subject and another remote computer

B_1: *Communication through voice or chat*

B_2: *Collaboration through mobile application (e.g., remote desktop connection)*

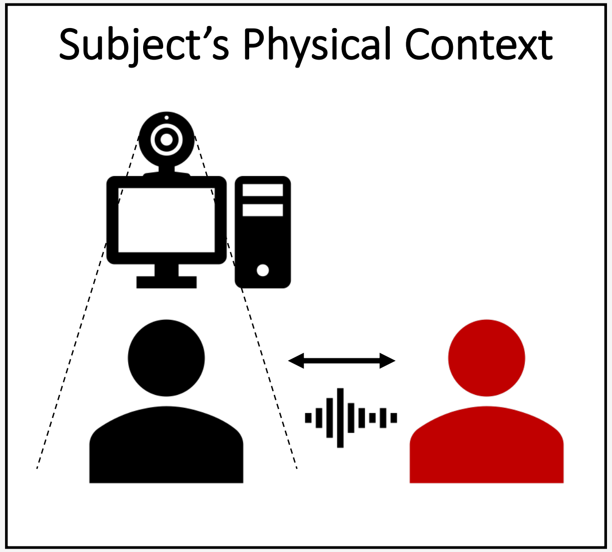


Subject seeks for help from online resources, search engines, which are not allowed based on the examination policy

Identification of Communication, Collaboration and Resource Access Threat Scenarios *(RQ_3)*

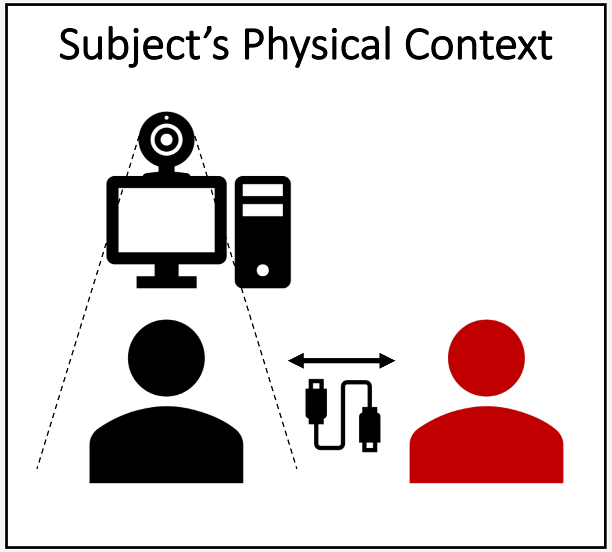
Co-funded by the
Erasmus+ Programme
of the European Union

- In-situ Scenarios



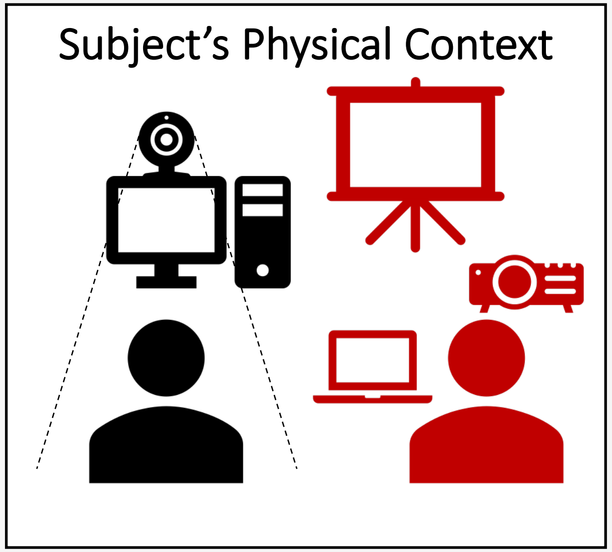
Subject’s Physical Context

Interaction with another person in the same room through voice



Subject’s Physical Context

Another person that is in the same room as the subject is interacting with the examination using other devices of the subject’s computer



Subject’s Physical Context

Projection of answers on a whiteboard

Co-funded by the
Erasmus+ Programme
of the European Union

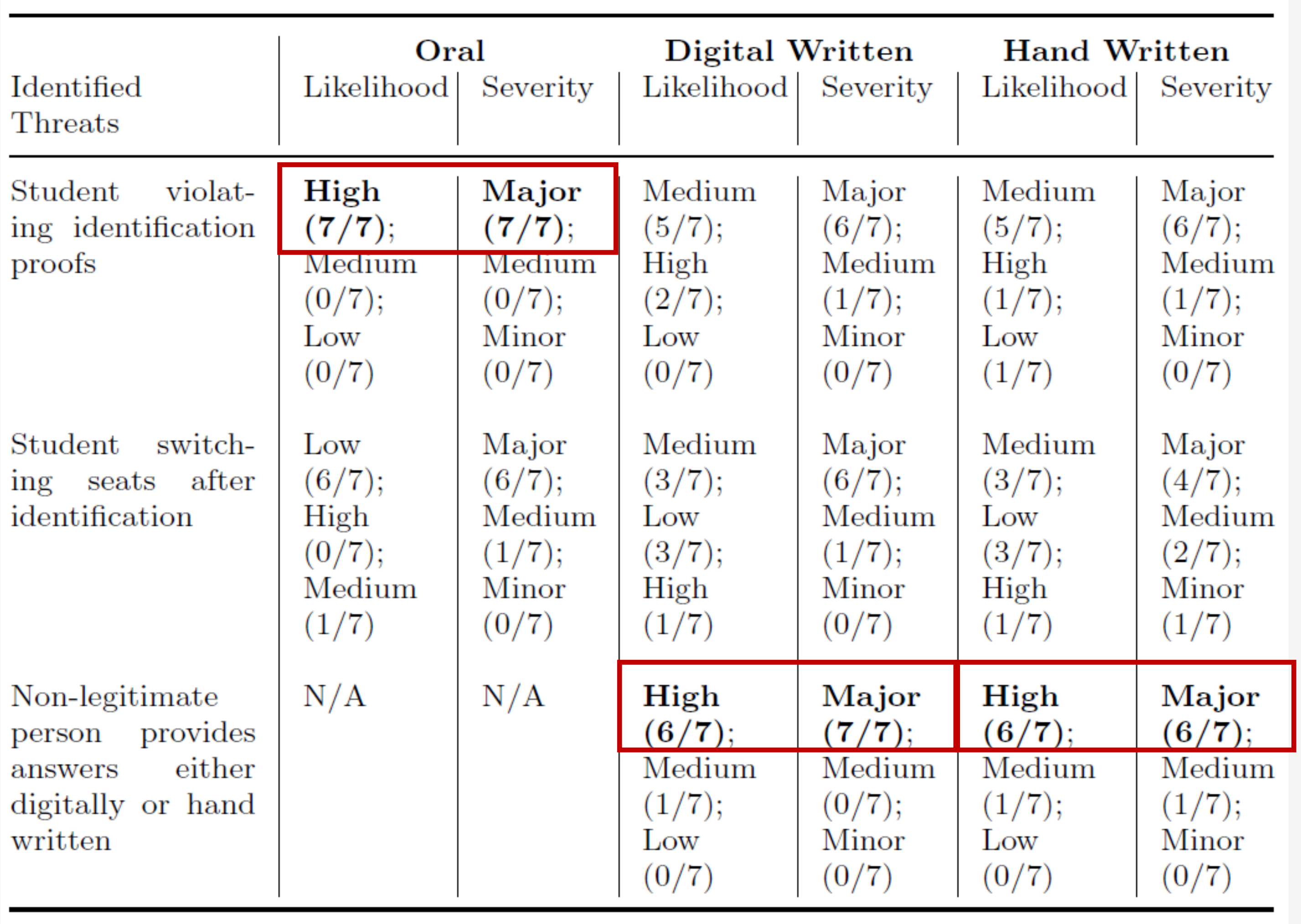
Rating of Threat Scenarios

- A total of seven (7) participants were recruited from three European universities.

- The sample included participants with a variety of roles, i.e., four (4) instructors, one (1) decision maker, 1 (one) system administrator and one (1) data protection expert.

- We conducted a series of semi-structured interviews with each participant that lasted approximately 60-90 minutes each, discussing around topics related to rating the threat scenarios identified in terms of likelihood/probability to happen and their severity

Rating of Impersonation Threats



Identified Threats	Oral		Digital Written		Hand Written	
	Likelihood	Severity	Likelihood	Severity	Likelihood	Severity

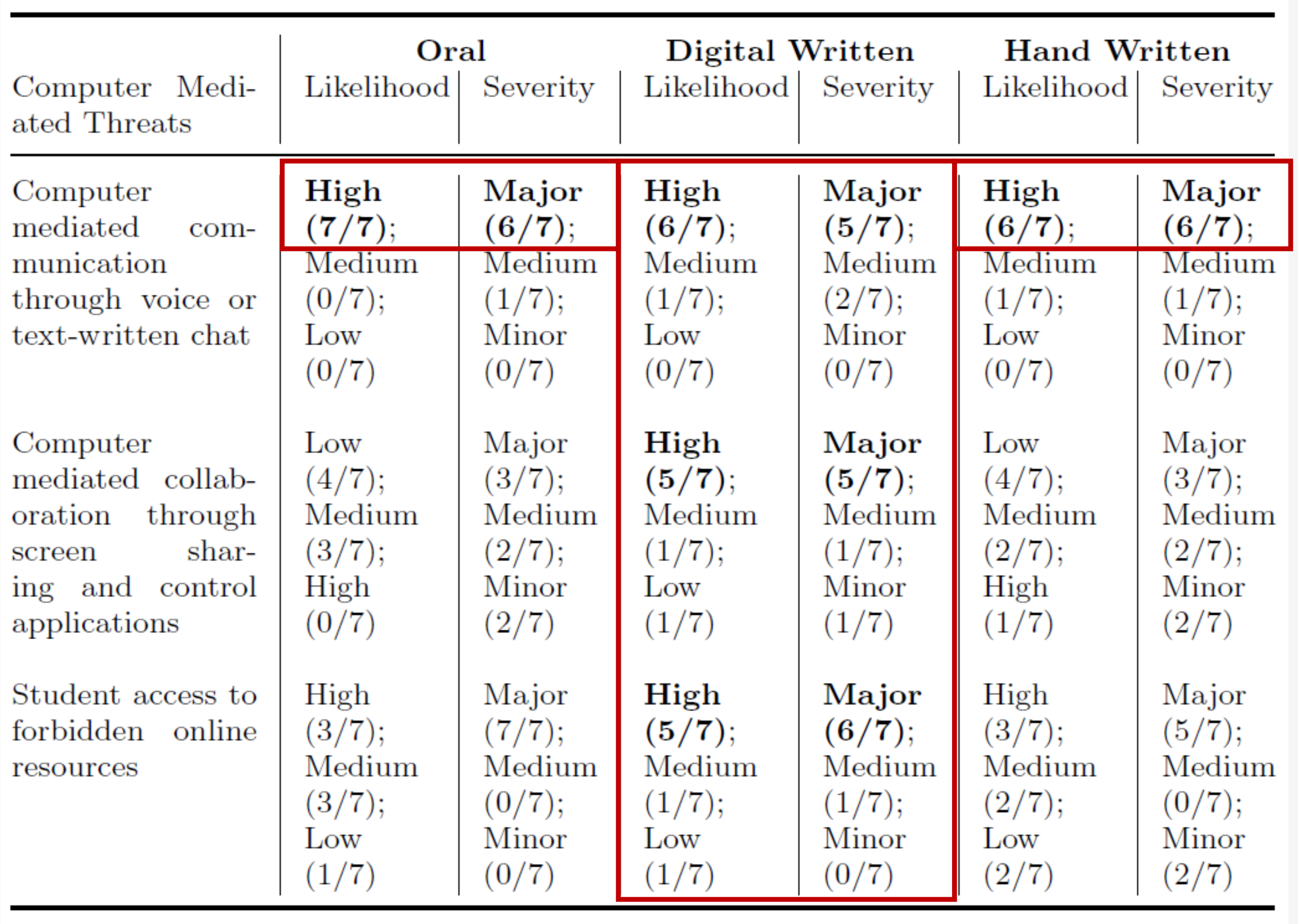
Student violating identification proofs	**High (7/7)**;
	Medium (0/7);
	Low (0/7)
		Major (7/7);
		Medium (0/7);
		Minor (0/7)
			Medium (5/7);
			High (2/7);
			Low (0/7)
				Major (6/7);
				Medium (1/7);
				Minor (0/7)
					Medium (5/7);
					High (1/7);
					Low (1/7)
						Major (6/7);
						Medium (1/7);
						Minor (0/7)

Student switching seats after identification	Low (6/7);
	High (0/7);
	Medium (1/7)
		Major (6/7);
		Medium (1/7);
		Minor (0/7)
			Medium (3/7);
			Low (3/7);
			High (1/7)
				Major (6/7);
				Medium (1/7);
				Minor (0/7)
					Medium (3/7);
					Low (3/7);
					High (1/7)
						Major (4/7);
						Medium (2/7);
						Minor (1/7)

Non-legitimate person provides answers either digitally or hand written	N/A	N/A	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (7/7)**; Medium (0/7); Minor (0/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)

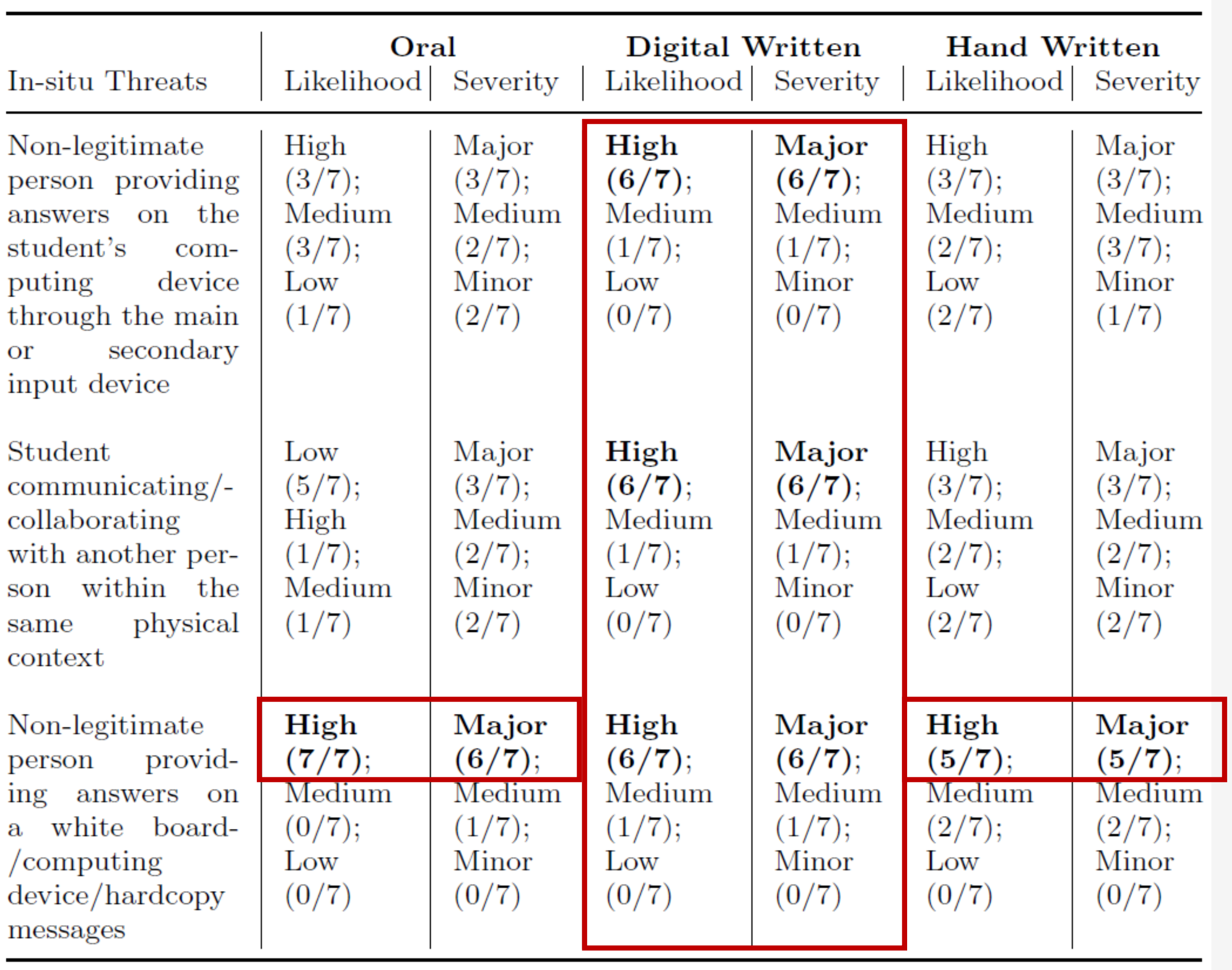
Communication, Collaboration and Resource Access Threats

Co-funded by the Erasmus+ Programme of the European Union



Computer Mediated Threats	Oral		Digital Written		Hand Written	
	Likelihood	Severity	Likelihood	Severity	Likelihood	Severity
Computer mediated communication through voice or text-written chat	**High (7/7)**; Medium (0/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (5/7)**; Medium (2/7); Minor (0/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)
Computer mediated collaboration through screen sharing and control applications	Low (4/7); Medium (3/7); High (0/7)	Major (3/7); Medium (2/7); Minor (2/7)	**High (5/7)**; Medium (1/7); Low (1/7)	**Major (5/7)**; Medium (1/7); Minor (1/7)	Low (4/7); Medium (2/7); High (1/7)	Major (3/7); Medium (2/7); Minor (2/7)
Student access to forbidden online resources	High (3/7); Medium (3/7); Low (1/7)	Major (7/7); Medium (0/7); Minor (0/7)	**High (5/7)**; Medium (1/7); Low (1/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	High (3/7); Medium (2/7); Low (2/7)	Major (5/7); Medium (0/7); Minor (2/7)

Communication, Collaboration and Resource Access Threats



	Oral		Digital Written		Hand Written	
In-situ Threats	Likelihood	Severity	Likelihood	Severity	Likelihood	Severity
Non-legitimate person providing answers on the student's computing device through the main or secondary input device	High (3/7); Medium (3/7); Low (1/7)	Major (3/7); Medium (2/7); Minor (2/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	High (3/7); Medium (2/7); Low (2/7)	Major (3/7); Medium (3/7); Minor (1/7)
Student communicating/collaborating with another person within the same physical context	Low (5/7); High (1/7); Medium (1/7)	Major (3/7); Medium (2/7); Minor (2/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	High (3/7); Medium (2/7); Low (2/7)	Major (3/7); Medium (2/7); Minor (2/7)
Non-legitimate person providing answers on a white board/computing device/hardcopy messages	**High (7/7)**; Medium (0/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	**High (6/7)**; Medium (1/7); Low (0/7)	**Major (6/7)**; Medium (1/7); Minor (0/7)	**High (5/7)**; Medium (2/7); Low (0/7)	**Major (5/7)**; Medium (2/7); Minor (0/7)

Task 1.3: Specification of the Framework

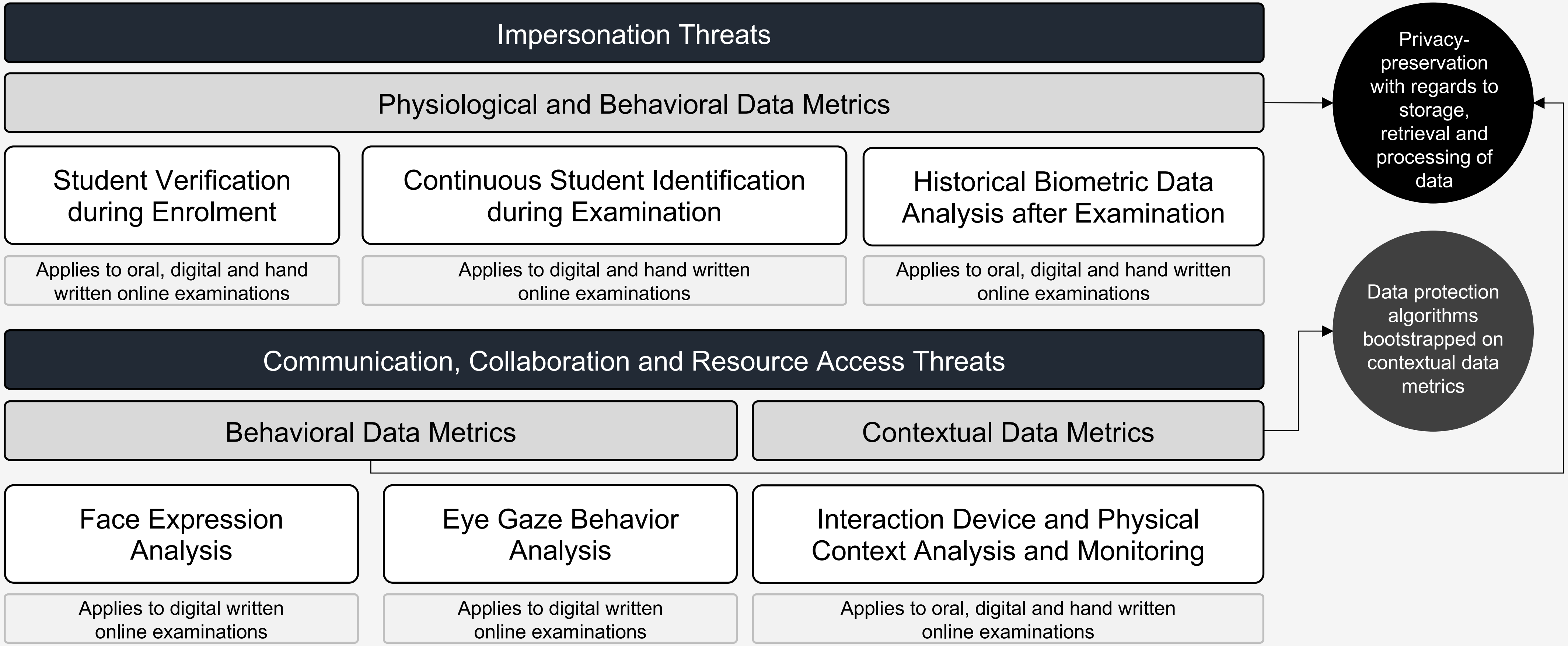
- *Aims*
  - Define the methodology and conduct an analysis, elicitation and validation of the security measurements, metrics and policies of the framework
  - Define, at a conceptual level, a multi-dimensional user model for continuous identification of end-users

- The framework and model will be based on input from T1.1 (literature analysis) and T1.2 (semi-structured interviews with stakeholders of HEIs)
- Algorithms will be identified and designed for continuous identification based on a combination of voice, image and interaction behavior data
- This will guide the development of the corresponding intelligent user identification mechanisms in IO2

Threat Model, Data Metrics and Countermeasures

Co-funded by the
Erasmus+ Programme
of the European Union

ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY



Impersonation Threats

Physiological and Behavioral Data Metrics

Student Verification during Enrolment

Applies to oral, digital and hand written online examinations

Continuous Student Identification during Examination

Applies to digital and hand written online examinations

Historical Biometric Data Analysis after Examination

Applies to oral, digital and hand written online examinations

Communication, Collaboration and Resource Access Threats

Behavioral Data Metrics

Contextual Data Metrics

Face Expression Analysis

Applies to digital written online examinations

Eye Gaze Behavior Analysis

Applies to digital written online examinations

Interaction Device and Physical Context Analysis and Monitoring

Applies to oral, digital and hand written online examinations

Privacy-preservation with regards to storage, retrieval and processing of data

Data protection algorithms bootstrapped on contextual data metrics

■ Threat model composed in terms of impersonation, communication, collaboration, resource access threats

▨ Data metrics for analyzing and monitoring physiological, behavioral and contextual data

□ Suggested countermeasures and features for addressing the identified threats

Addressing Impersonation Threats through Physiological Data Analysis

Co-funded by the Erasmus+ Programme of the European Union

- Impersonation threats can be addressed by analyzing the students' biometric data (physiological and behavioral), such as, face and voice data
  - Impersonation threats during *student examination enrolment* can be addressed through **automatic student verification based on ground truth biometric data**
  - Impersonation threats during the *examination session* can be addressed based on **continuous student identification based on biometric data**
  - Impersonation threats can be identified *after an online examination* has completed through **intelligent data analytics based on historical biometric data**

Leveraging on Ground Truth Physiological and Behavioral Data aiming to Verify Students

- *Relevant threat scenario:* student violating identification proofs
- *Relevant examination type:* all online examination types (oral, digital written, hand written)
- *Countermeasures:*
  - *Face-based identification:* comparison of the student's face characteristics and the provided identity card with ground truth data that are provided by the university;
  - *Voice-based identification:* comparison of the student's voice signals and ground truth voice data that are provided by the university;
  - *Knowledge-based identification:* asking the students a series of secret questions (e.g., what is your grandmother's name) and compare them with ground truth data

Continuous Student Identification based on Physiological and Behavioral Data

- *Relevant threat scenario:* student switching seats after identification, and a non-legitimate person providing answers through shared LMS credentials
- *Relevant examination type:* digital written, hand written
- *Countermeasures:*
  - Continuously identify the students by comparing the students' face and/or voice data with ground truth (historical) data from the university's LMS.
  - Detect authentic *vs.* pre-recorded input video streams by applying specific methods for detecting the authenticity of video streams;
  - Monitor the student's login sessions by checking whether concurrent login sessions exist from the same students;
  - Monitor the student's interaction device by checking whether the device characteristics of the student have changed during the examination session.

Intelligent Data Analytics for Identifying Impersonation Cases based on Historical Physiological and Behavioral Data

- *Relevant threat scenario:* analyzing historical data and identifying impersonation cases over time
- *Relevant examination type:* all online examination types (oral, digital written, hand written)
- *Countermeasures:*
  - Comparing facial embeddings of students across multiple examination instances in the system aiming to detect whether a user with the same facial characteristics has been identified within multiple user accounts.
  - Detecting common handwriting styles between different students' submissions, i.e., by comparing a student's submitted hand-written examination with their previously submitted examinations.

Addressing Communication, Collaboration and Resource Access Threats through Behavioral and Contextual Data Analysis

- Communication, collaboration and resource access threats can be addressed by analyzing the students’ behavioral data:
  - Analysis of face expressions and eye gaze behavior data
  - Monitoring the student's computing device and physical context

- Such threats are primarily applied during an examination session aiming to detect whether students are communicating and/or collaborating with another person, and whether they are attempting to access forbidden resources

Analysis of the Student's Behavioral Data and Patterns

- *Relevant threat scenario:* student communicating/collaborating with another person within the same physical context, and a non-legitimate person providing answers on a white board/computing device/hardcopy messages
- *Relevant examination type:* all online examination types (oral, digital written, hand written)
- *Countermeasures* - Monitoring the student's behavioral data as follows:
  - *Face behavior and expression tracking:* through state-of-the-art facial and expression recognition algorithms aiming to identify any suspicious activity (e.g., model the facial expressions of students that provide answers to the examination system vs. students that are idle and only look at the screen);
  - Eye gaze behavior tracking: through real-time eye-gaze analysis (e.g., in the case were students frequently look beyond the monitor during the examination session.

Monitoring the Student's Computing Device and Physical Context

Co-funded by the Erasmus+ Programme of the European Union

- *Relevant threat scenario:* all computer mediated communication, collaboration and resource access threat scenarios, and the threat scenario in which a non-legitimate person provides answers on the student's computing device through the student's main input device or a secondary input device
- *Relevant examination type:* all online examination types (oral, digital written, hand written)
- *Countermeasures* - **Monitoring the student's computing device and/or the physical context in which the online examination takes place as follows:**
  - *Voice signal processing*, through environmental audio signal processing algorithms to detect cases were students might be talking to other persons;
  - *Monitoring and control of communication/collaboration applications*, aiming to prevent students communicating and/or collaborating with other persons through certain applications;
  - *Monitoring and control of websites' access* aiming to allow or restrict access to specific websites depending on the examination protocol and policy;
  - Keyboard keystroke and computer mouse click analysis aiming to process and identify any keyboard-related and/or computer mouse-related activity;
  - Identification of secondary input/output devices, which may be used by other persons to type in questions to the examination system.

Co-funded by the
Erasmus+ Programme
of the European Union

ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY

TrustID

Thank you!

Argyris Constantinides, University of Cyprus

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ UNIVERSITY OF PATRAS

University of Cyprus

ISR INSTITUTO DE SISTEMAS E ROBÓTICA UNIVERSIDADE DE COIMBRA

cognitiveux