MISC

- Improving application fuzzing via QR codes
  - *What happens if we provide applications with malicious QR codes?*
  - *We have a tool to automatically test it! But, some improvements are needed:*
  - *> better malicious code generation, possibly using feedbacks (fuzzing)*
  - *> improving the stability of the virtualization testbed (coding)*
  - *> investigate novel strategies (function call hooks)*
  - *Contact person: Denis Donadel (donadel@math.unipd.it)*

- Can we attack channel hopping mitigation against DoS?
  - *Channel hopping is usually employed to prevent DoS in wireless communications*
  - *It is a simple but effective solutions… or isn't it?*
  - *Investigate state-of-the-art channel hopping strategies and attack them*
  - *Contact person: Denis Donadel (donadel@math.unipd.it) and Alessandro Brighente (alessandro.brighente@unipd.it)*

Acoustic communication

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Acoustic communications to evade network security policies
  - The use of acoustic communications as a hidden channel of communication can offer a useful tool to evade security policies implemented in ICT or industrial environments.
  - Evaluate if the cyber security standards consider this kind of attack and if not, which countermeasures can be suggested.
  - Create a testbed that considers how acoustic communications may violate at least one of the following scenarios:
    - offices of a company (IT scenario);
    - computers in a company's production line (OT scenario).
  - *Contact person:*
    Simone Soderi (simone.soderi@unifi.it)
    Gabriele Orazi (gabriele.orazi@phd.unipd.it)

Applied ML

- PoC of an Intrusion Response System (IRS)
  - *Intrusion Detection Systems (IDS) can detect anomalies in a network*
  - *Intrusion Prevention Systems can stop certain packets to mitigate attacks*
  - *What if an attack is still successful?*
  - *Development of a simple IRS which collect data from IDS/honeypots/syslogs and can react to alerts to block or slow down the attacker*
  - *Contact person: Denis Donadel (donadel@math.unipd.it)*

- An LLM-based assistant for sysadmins
  - *Can we employ LLMs to assist the job of technical figures like sysadmins?*
  - *Development of an assistant fine-tuned to answer specific technical requests and able to put the problem in the context of a specific network*
  - *Contact person: Denis Donadel (donadel@math.unipd.it)*

Vehicles Security

- ECU fingerprinting in a Black Box Reverse Engineer manner
  - *Understand the CAN Bus packet format and how the content could be differentiated*
  - *Classify the different ECUs and understand content format to extrapolate data*
  - *Contact person: Tommaso Bianchi (tommaso.bianchi@phd.unipd.it) and Francesco Marchiori (francesco.marchiori@math.unipd.it)*

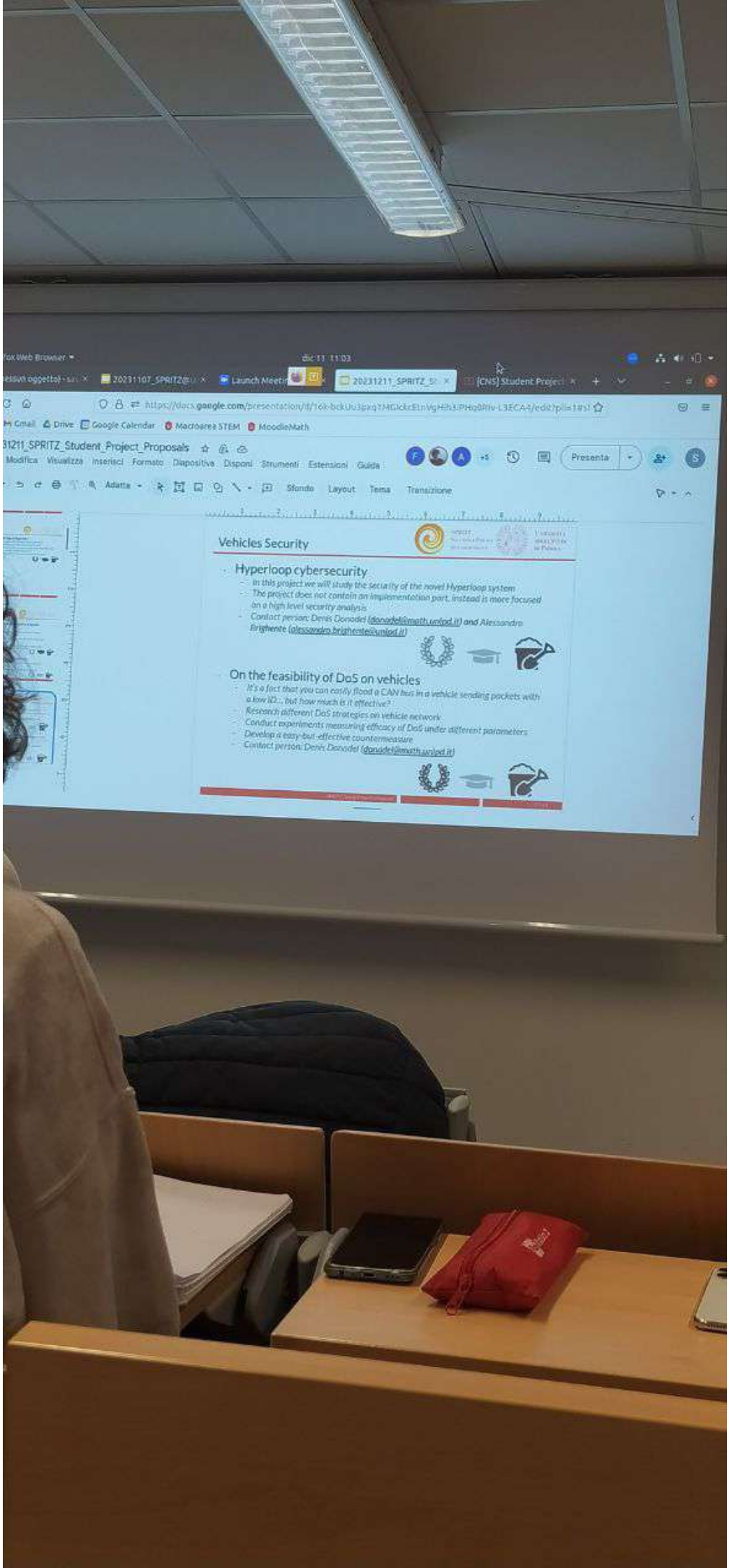
- Remote Keyless Entry Attack and Defenses
  - *Enumerate and analyze attacks and defenses present in literature for the remote keyless entry in cars*
  - *Contact person: Tommaso Bianchi (tommaso.bianchi@phd.unipd.it)*


Cryptography
Break Quantum KD Signal Algorithm
Signal proposes its own hybrid QKD algorithm (now at version 2)
In the project we want to analyze it and verify it using Tamarin
Can be extended for a possible thesis project (e.g. reproduce their results with ProVerif/CryptoVerif or provide a better version of it)
Contact person: Tommaso Bianchi (tommaso.bianchi@phd.unipd.it)


Cyber-Physical System Security
SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
Find exposed Uninterruptible Power Supplies on the wild
...and then try (not) to hack them!
Research which protocols and ports are employed by UPS and what other characteristics are peculiar to these devices
Employ Shodan (or similar tool) to detect UPS in the wild
Look for known vulnerabilities in these systems
Contact person: Tommaso Bianchi (tbianchi@math.unipd.it) and Denis Donadel (donadel@math.unipd.it)
SPRITZ Group Projects Proposal
14/64

EPZ privacy

- StravaGANte
  - *Strava is a social network where athletes (mostly runners and cyclists) post their activities*
  - *Start and ending points are sensitive geolocation (it can be private house, office...)*
  - *Current methods of Endpoint Privacy Zones (EPZ) anonymization are not safe enough*
  - *The project is about developing an innovative and robust method for EPZ generation using GANs*
  - *Contact person: Gabriele Orazi (*)


Vehicles Security
Hyperloop cybersecurity
In this project we will study the security of the novel Hyperloop system
The project does not contain an implementation part, instead is more focused on a high level security analysis
Contact person: Denis Donadel (donadel@math.unipd.it) and Alessandro Brighente (alessandro.brighente@unipd.it)
On the feasibility of DoS on vehicles
It's a fact that you can easily flood a CAN bus in a vehicle sending packets with a low ID... but how much is it effective?
Research different DoS strategies on vehicle network
Conduct experiments measuring efficacy of DoS under different parameters
Develop a easy-but-effective countermeasure
Contact person: Denis Donadel (donadel@math.unipd.it)

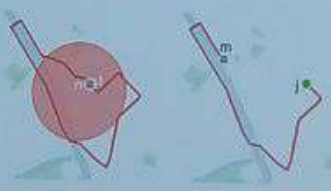
EPZ privacy

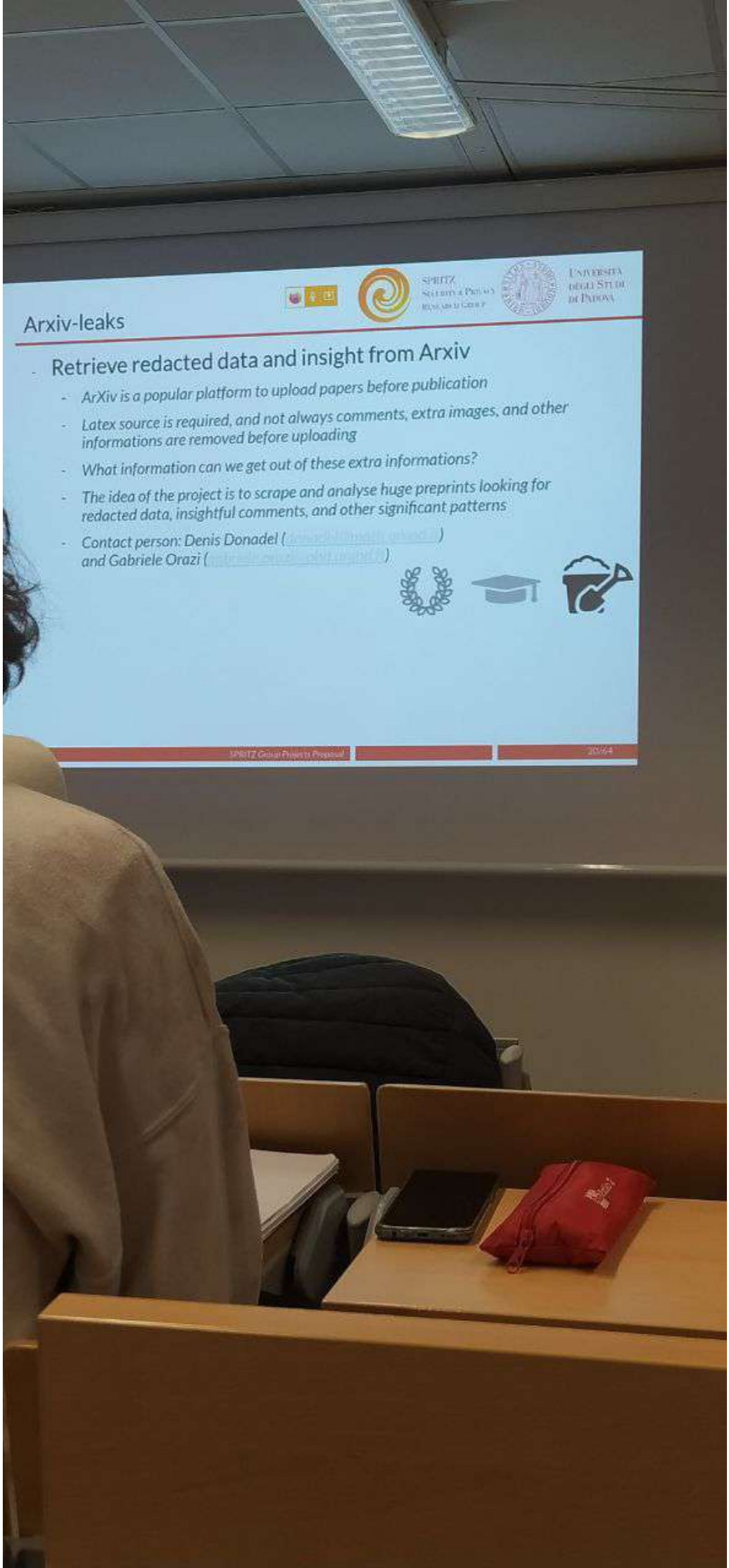
SPRITZ Security and Privacy Research Group

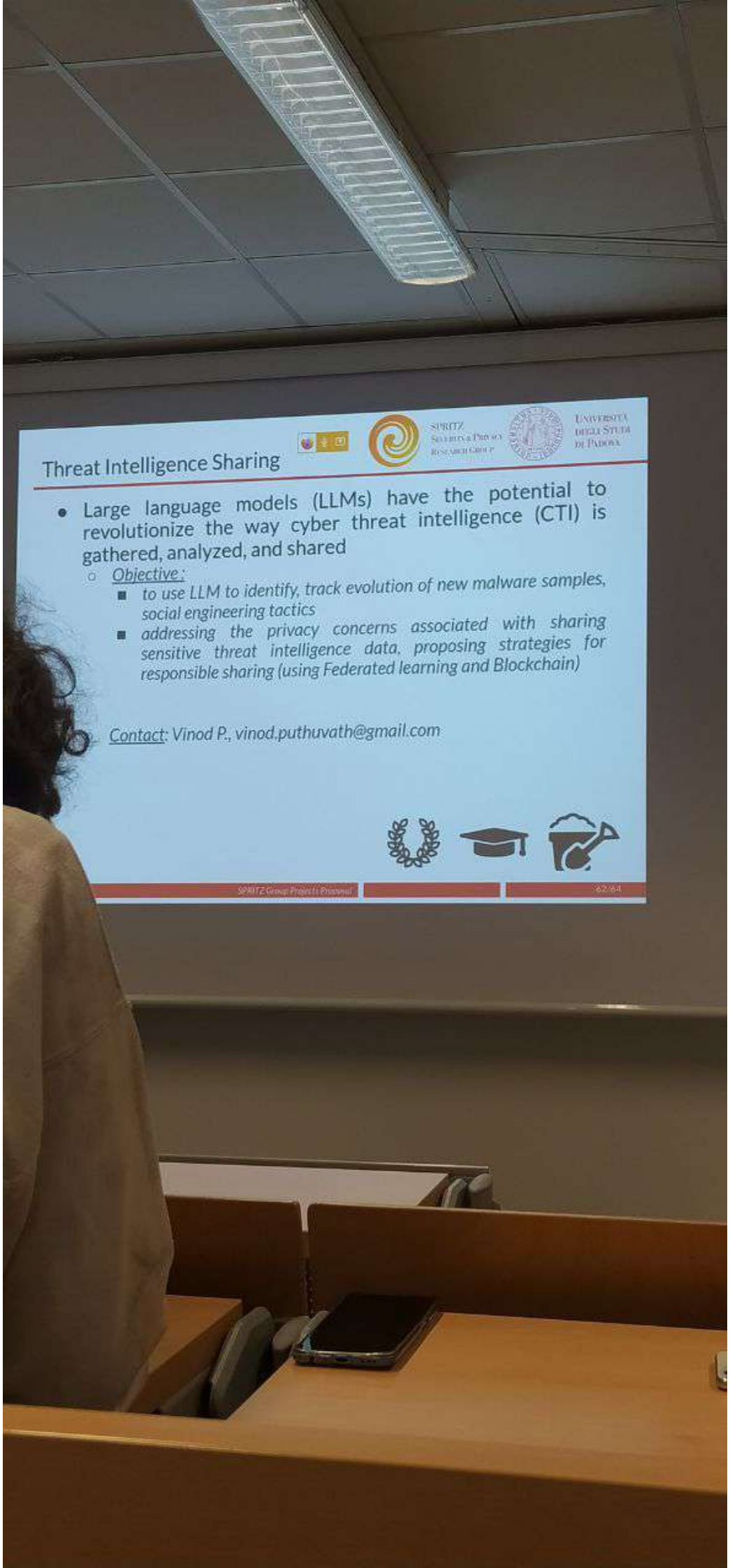
Università degli Studi di Padova

- StravaGANte
  - *Strava is a social network where athletes (mostly runners and cyclists) post their activities*
  - *Start and ending points are sensitive geolocation (it can be private house, office…)*
  - *Current methods of Endpoint Privacy Zones (EPZ) anonymization are not safe enough*
  - *The project is about developing an innovative and robust method for EPZ generation using GANs*
  - *Contact person: Gabriele Orazi (gabriele.orazi@phd.unipd.it)*

STRAVA




SPRITZ
Security & Privacy
Research Group
Università degli Studi di Padova
Arxiv-leaks
Retrieve redacted data and insight from Arxiv
ArXiv is a popular platform to upload papers before publication
Latex source is required, and not always comments, extra images, and other informations are removed before uploading
What information can we get out of these extra informations?
The idea of the project is to scrape and analyse huge preprints looking for redacted data, insightful comments, and other significant patterns
Contact person: Denis Donadel (
and Gabriele Orazi (
SPRITZ Group Projects Proposal
20/44


Threat Intelligence Sharing
SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
Large language models (LLMs) have the potential to revolutionize the way cyber threat intelligence (CTI) is gathered, analyzed, and shared
Objective :
to use LLM to identify, track evolution of new malware samples, social engineering tactics
addressing the privacy concerns associated with sharing sensitive threat intelligence data, proposing strategies for responsible sharing (using Federated learning and Blockchain)
Contact: Vinod P., vinod.puthuvath@gmail.com
SPRITZ Group Projects Proposal
62/64

Adversarial ML

- Generate adversarial examples for an adversarially trained model
  - *You will be provided with an adversarially trained model and try to create adversarial examples for it.*
  - *Prerequisites: Python, Python for AI (not in depth, willingness to learn is enough)*
  - *Contact person: Stefanos Koffas (s.koffas@tudelft.nl)*

- Test different backdoor attacks in deep learning (source specific vs source agnostic, clean-label vs dirty-label, multiple triggers same label, multiple triggers multiple labels) against SOTA backdoor countermeasures
  - *Prerequisites: Python, Python for AI (willingness to learn is enough)*
  - *Contact person: Stefanos Koffas (s.koffas@tudelft.nl)*

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Drones/UAVs

Rescue UAVs under attack

- The project involves the identification and exploit of onboard sensors to rescue a compromised UAV (e.g., images, path ecc...)
  - Attack definition
- Onboard sensors identification and Testbed creation
- Possible Machine Learning application
- Contact person: Giulio Rigoni (giulio.rigoni@uniroma1.it)

Safe UAV's backward journey (windy scenario)

- Extensive Real flights/Testbed creation with UAVs in windy situations
- Development of Machine Learning models
- Contact: Giulio Rigoni (giulio.rigoni@uniroma1.it)

UAV Remote Attestation Survey

- Searching literature for recent scientific articles
- Writing of a survey


Biometrics
SPRITZ Security & Privacy Research Group
Università degli Studi di Padova
IDAP (Identity Dialer Acquisition Protocol)
- Dialers can fool (relevant) people on phone calls to carry masquerades
- Additional vulnerability given by audio deep-fakes
- Develop a (scalable) biometric system to verify identities
Tattoo identification
- Europol enforced challenge
- Investigators shared query tattoos as significant intel
- Detection and identification of suspects
Contact Person: Saverio Cavasin
saverio.cavasin@phd.unipd.it
SPRITZ Group Projects Proposal

Android Security

Solving the Android Semantic Gap

- *Existing dynamic analysis techniques that intercept invocations of the Android API Framework can be easily bypassed*
- *An alternative approach would be to trace the system calls, but there is a semantic gap between a sequence of system calls and the original invoked Android API*
- *We would to study how to build this knowledge and fix this gap*
- *Contact Person: Eleonora Losiouk*
- *eleonora.losiouk@unipd.it*

Measurements of Interactions among Android Apps

- *Android apps are sandboxed, but they can interact among each other with Android framework*
- *We want to measure how and which apps interact among each other*
- *Contact Person: Eleonora Losiouk*
- *eleonora.losiouk@unipd.it*

Machine-learning for Audio

- Creating profiles from audio clips
  - *Area of interest: Machine Learning (ML)*
  - *Topic: Training an ML model on audio clips to create user profile*
  - *Prerequisite: Some knowledge on ML and programming*
  - *Contact person: Ankit Gangwal (CiaoAnkit@gmail.com)*

- NFT Playground
  - *Area of interest: Data mining*
  - *Topic: Data collection, analysis, and numerical statistics*
  - *Prerequisite: Simple python programming for data scraping and analysis*
  - *Contact person: Ankit Gangwal (CiaoAnkit@gmail.com)*

Anomaly Detection on IoT Networks

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Creation of a network traffic dataset based on real IoT hardware

- Area of interest: computer networks, IoT, data analysis
- Topic: creation of an IoT network traffic dataset comprehensive of various types of attacks
- Prerequisite: programming skills, networking, packet sniffing
- Contact person: Giacomo Quadrio (giacomo.quadrio@unipd.it)

Survey on most frequent IoT attacks

- Searching scientific literature about the topic
- Writing of a survey
- Contact person: Giacomo Quadrio (giacomo.quadrio@unipd.it)

Homomorphic encryption in IIoT privacy

SPRITZ Security and Privacy Research Group

Università degli Studi di Padova

-*Objective:* To enhance IIoT privacy

- Analysis of lightweight homomorphic encryptions for IIoT
- Privacy-classification of IIoT transactions using smart contract
- Using zero-knowledge proofs for data sharing in IIoTs

-*Impact of project:* 1) Enhanced security/privacy application development
2) New knowledge-base
3) Blockchain applications

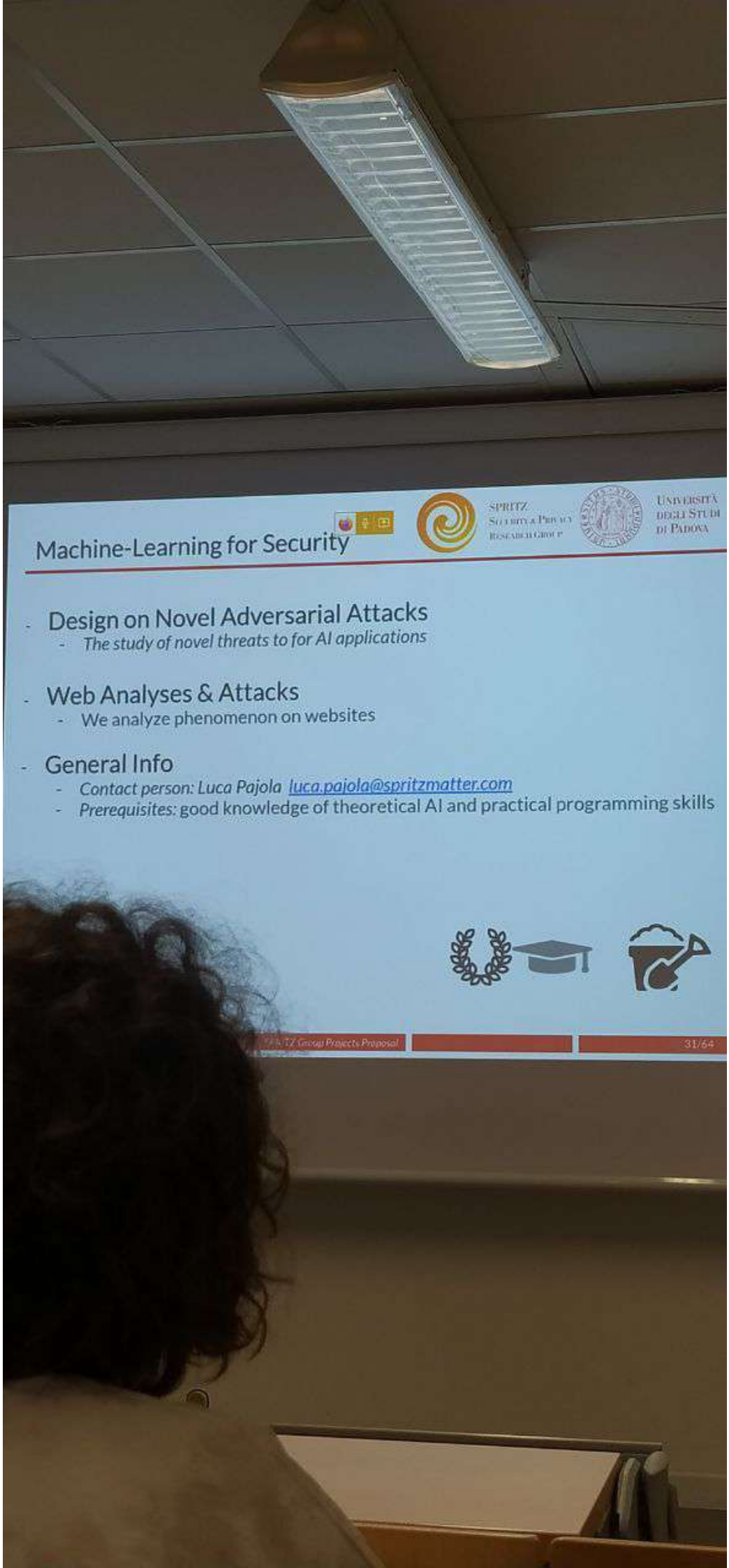
Pre-requisite: Good if you know C++, Python, Knowledge of mathematical functions, basic knowledge of IIoT, cryptography

Contact person:

Gulshan Kumar

gulshan.kumar@unipd.it

gulshan3971@gmail.com


Machine-Learning for Security
SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
- Design on Novel Adversarial Attacks
- The study of novel threats to for AI applications
- Web Analyses & Attacks
- We analyze phenomenon on websites
- General Info
- Contact person: Luca Pajola luca.pajola@spritzmatter.com
- Prerequisites: good knowledge of theoretical AI and practical programming skills
SPRITZ Group Projects Proposal
31/64

Malware Detection

- Malware visualization
  - Malware visualization is a technique used to transform malware files into visually interpretable representations, such as images or graphs
  - Key limitations: Loss of information in the conversion process, lack of context and interpretation, limited ability to capture dynamic behavior, etc.
  - Objective :
    - to design specific XAI techniques that can effectively explain the decision-making processes of malware detection and classification models,
    - adversarial attacks aim to manipulate data or model inputs to mislead the model into making incorrect predictions. Understanding how XAI can be used to defend against such attacks

Contact: Vinod P., vinod.puthuvath@gmail.com

Jamming Tool Development

SPRITZ Security & Privacy Research Group

Title: Jamming tools on wireless network simulator

Target: To implement a more convenient library that could be used on existing wireless network simulators (e.g., NS-3 and Contiki-NG).

Requisites: C/C++, wireless network protocols

Contact person: Shuo Wang

Email: shuo.wang@phd.unipd.it

More IP and E2EE

- IP retransmissions and accounting
  - *Blackbox analysis of IP retransmissions on traffic accounting (metered connections, such as mobile ISPs)*
  - *Literature review and on-field tests*
  - *Contact: Enrico Bassetti, bassetti@di.uniroma1.it*

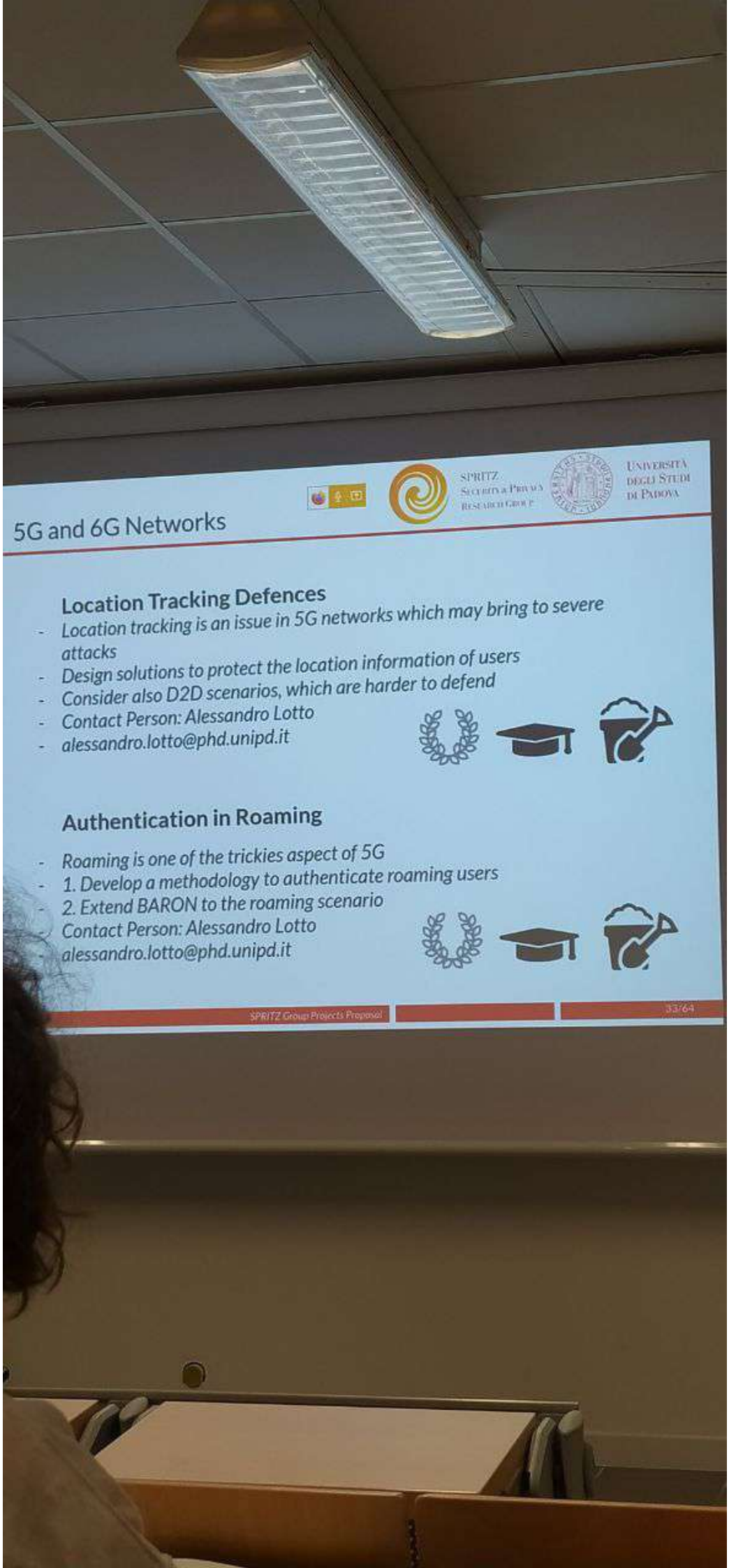
- E2EE contact verification ceremonies
  - *Current ceremonies to verify contacts in end-to-end encrypted chats are complex, and vulnerable to MitM/impersonation*
  - *Have you ever verified one of your conversations?*
  - *Design a human-friendly e2ee contact verification ceremony*
  - *Contact: Enrico Bassetti, bassetti@di.uniroma1.it*

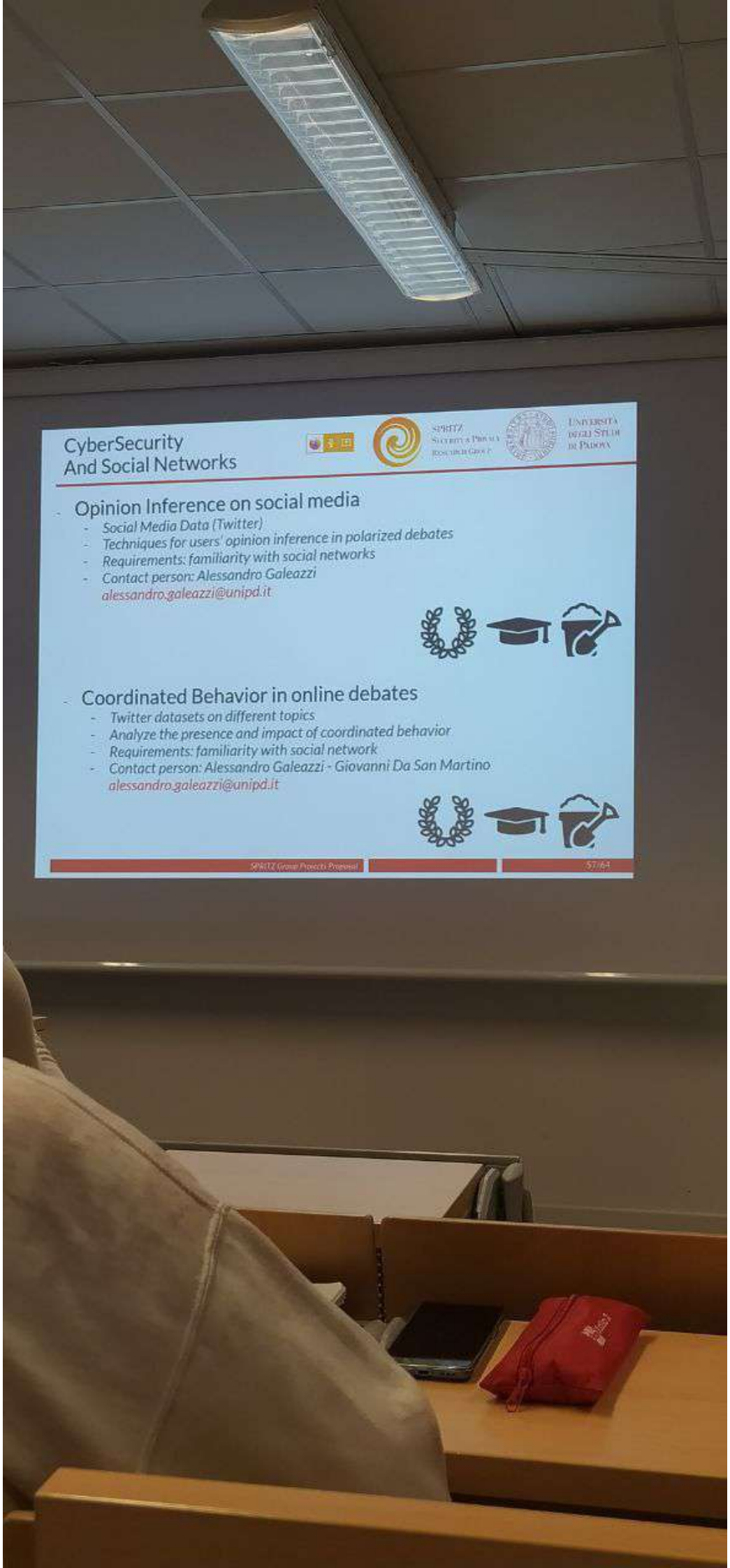
Communication Analysis

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Detection of Location Spoofing Attacks in Air-Traffic Communication: Leveraging Physical Layer and Space Tessellation
  - *Develop a robust one-class classifier-based system of detecting ADS-B location spoofing attacks by employing anomaly detection through Deep learning models.*
  - *Contact person:*
    - *Alessandro Brighente (alessandro.brighente@unipd.it),*
    - *Sitora Salaeva (sitora.salaeva@phd.unipd.it)*


SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
5G and 6G Networks
Location Tracking Defences
- Location tracking is an issue in 5G networks which may bring to severe attacks
- Design solutions to protect the location information of users
- Consider also D2D scenarios, which are harder to defend
- Contact Person: Alessandro Lotto
- alessandro.lotto@phd.unipd.it
Authentication in Roaming
- Roaming is one of the trickies aspect of 5G
- 1. Develop a methodology to authenticate roaming users
- 2. Extend BARON to the roaming scenario
- Contact Person: Alessandro Lotto
- alessandro.lotto@phd.unipd.it
SPRITZ Group Projects Proposal
33/64


CyberSecurity
And Social Networks
SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
Opinion Inference on social media
Social Media Data (Twitter)
Techniques for users' opinion inference in polarized debates
Requirements: familiarity with social networks
Contact person: Alessandro Galeazzi
alessandro.galeazzi@unipd.it
Coordinated Behavior in online debates
Twitter datasets on different topics
Analyze the presence and impact of coordinated behavior
Requirements: familiarity with social network
Contact person: Alessandro Galeazzi - Giovanni Da San Martino
alessandro.galeazzi@unipd.it
SPRITZ Group Projects Proposal
57/64

Adversarial ML

- Explore the behavior of ChatGPT when it behaves like a terminal.
  - *Investigate whether we can affect its output with malicious commands.*
  - *Prerequisites: LLM Jailbreaks (only willingness to learn is enough)*
  - *Contact person: Stefanos Koffas (*[redacted]*)*

- Implement dynamic backdoor attacks in computer vision.
  - *Investigate if using a trigger with a neutral background creates a dynamic backdoor.*
  - *Prerequisites: Python, Python for AI (or willingness to learn)*
  - *Contact person: Stefanos Koffas (*[redacted]*)*

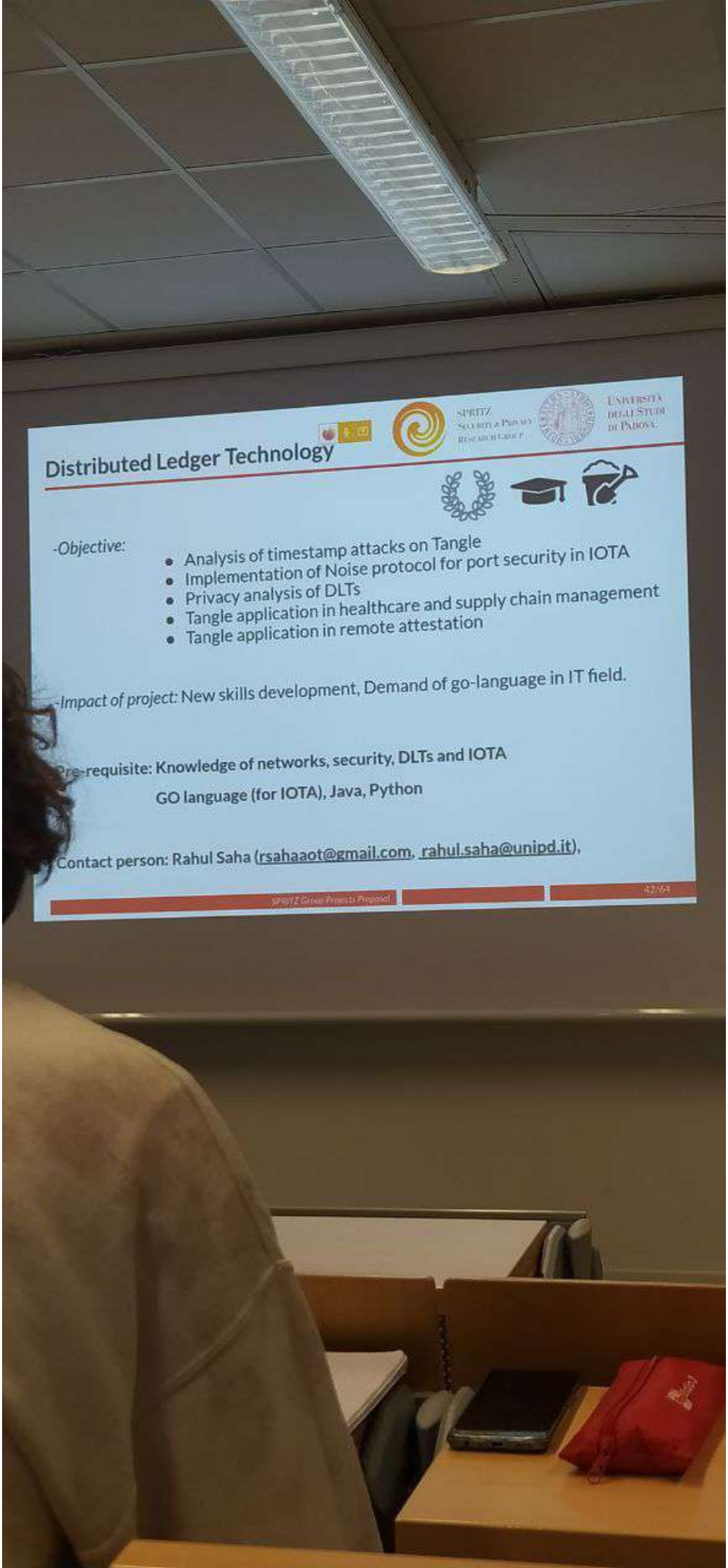
Vehicular Networks Security

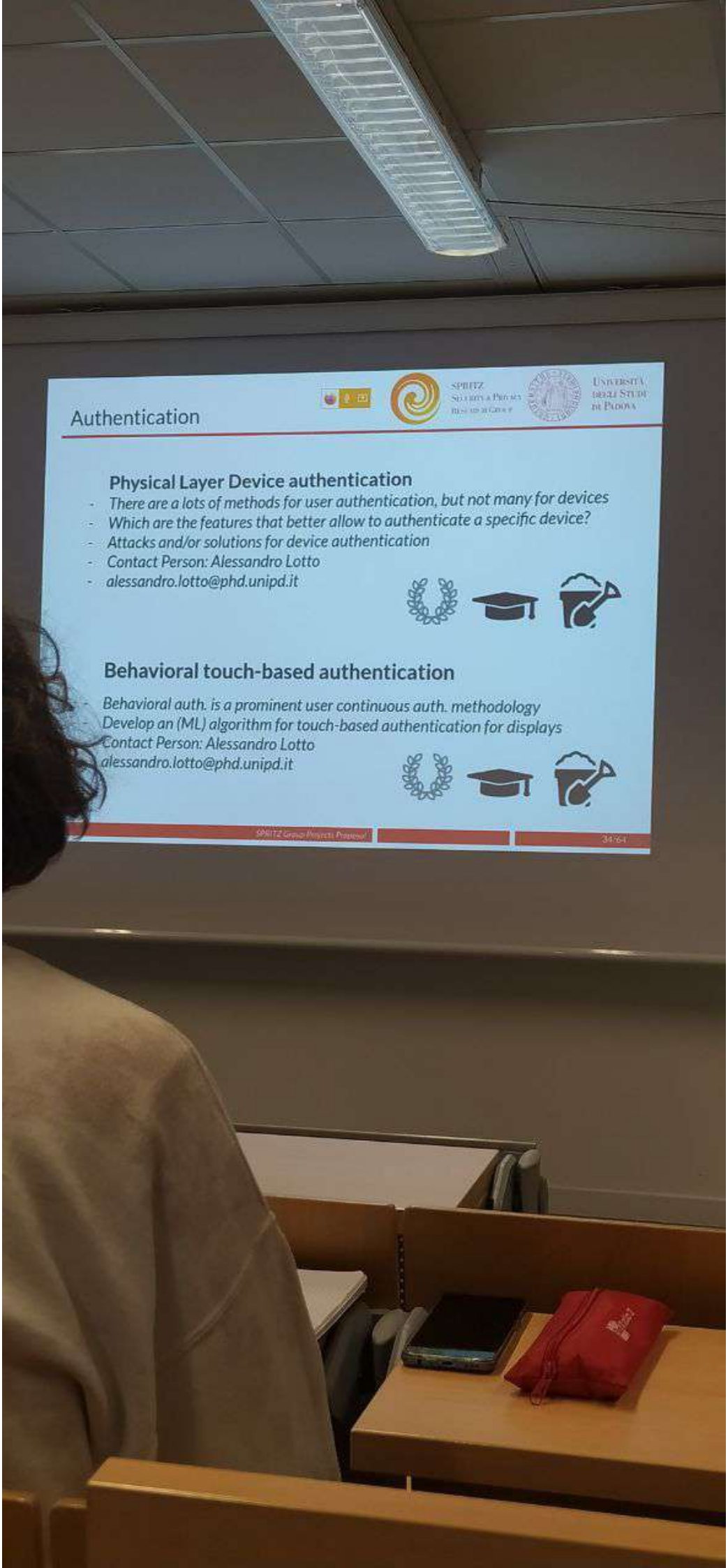
SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

1. Secure Protocol for IoVs Communication Components (V2V, V2S, V2I, V2R, V2P)
   - Design cryptographic protocol for secure authentication and communication among Internet of Vehicles components.
   - *Requirements: Basic Cryptography.*
   - *Contact person: Harsha Vasudev*
   - ***(drharshavasudev@gmail.com, harsha.vasudevanpillai@unipd.it).***

2. PQC -based Protocols for IoVs/VANETs.
   - *Design protocol using Post-Quantum Cryptography.*
   - *Requirements: Basics of PQC techniques.*
   - *Contact person: Harsha Vasudev*
   - ***(drharshavasudev@gmail.com, harsha.vasudevanpillai@unipd.it).***


Distributed Ledger Technology
SPRITZ
Security and Privacy
Research Group
Università
degli Studi
di Padova
-Objective:
Analysis of timestamp attacks on Tangle
Implementation of Noise protocol for port security in IOTA
Privacy analysis of DLTs
Tangle application in healthcare and supply chain management
Tangle application in remote attestation
-Impact of project: New skills development, Demand of go-language in IT field.
Pre-requisite: Knowledge of networks, security, DLTs and IOTA
GO language (for IOTA), Java, Python
Contact person: Rahul Saha (rsahaaot@gmail.com, rahul.saha@unipd.it),
SPRITZ Group Projects Proposal
42/64


Authentication
SPRITZ
Security & Privacy
Research Group
Università degli Studi di Padova
Physical Layer Device authentication
- There are a lots of methods for user authentication, but not many for devices
- Which are the features that better allow to authenticate a specific device?
- Attacks and/or solutions for device authentication
- Contact Person: Alessandro Lotto
- alessandro.lotto@phd.unipd.it
Behavioral touch-based authentication
- Behavioral auth. is a prominent user continuous auth. methodology
- Develop an (ML) algorithm for touch-based authentication for displays
- Contact Person: Alessandro Lotto
- alessandro.lotto@phd.unipd.it
SPRITZ Group Projects Proposal
34/64

Drones/UAVs

FPV data persistency/authenticity

- *Analyze the state of the art for data persistency/authenticity and find a solution suitable for drones images transmissions, necessary in contexts like humanitarian and rescue missions*
- *Contact person: Giulio Rigoni (giulio.rigoni@uniroma1.it)*

Multilateration vs GPS spoofing

- *Study the application of the multilateration technique regards a fleet of UAVs for safety purposes*
- *Contact person: Giulio Rigoni (giulio.rigoni@uniroma1.it)*

Adversarial Attacks

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Attacks on License Plate Recognition Systems

- *Optical Character Recognition (OCR) is just a part of the pipeline*
- *Real world scenario LCR has many challenges (e.g., noise, orientation, angle of view, lightning, ...)*
- *Also, black box scenario(?)*
- *See what are the most effective attack vectors and how it is possible to affect the pipeline*
- *Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it), Saverio Cavasin (saverio.cavasin@phd.unipd.it)*


Cyber Threat Intelligence and NLP
SPRITZ Security & Privacy Research Group
Università degli Studi di Padova
Advanced Persistent Threat classification
Advanced Persistent Threats (APT) represent malicious groups that establish a persistent presence in a networks with the aim of stealing information
CTI researchers maps their tactics and techniques to prevent further intrusions and share them in natural language reports
From data of known intrusions, classify the most probable APT
Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it), Vinod P (vinod.puthuvath@gmail.com)
SPRITZ Group Projects Proposal
29/64

SPRITZ Security & Privacy Research Group

UNIVERSITÀ DEGLI STUDI DI PADOVA

IP security

- Security of custom IP stacks
  - *Suitable for embedding in Internet-of-Things, such as lwIP*
  - *Userland libraries, such as Google gVisor (the "Container Security Platform"), software defined networks (SDN)*
  - *Course/extra project: test/adapt/port IPv6 attacks in literature*
  - *Contact: Enrico Bassetti, bassetti@di.uniroma1.it*

- Multi-path TCP and MP-QUIC
  - *Learn the state-of-the-art papers about MP-TCP and MP-QUIC*
  - *Multiple directions: analyze existing MP-TCP attacks against MP-QUIC, develop a blackbox fuzzer, differential fuzzing, etc.*
  - *Contact: Enrico Bassetti, bassetti@di.uniroma1.it*

Automotive Security

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Quantum-Safe Cryptography in Connected Vehicles
  - *Assess the vulnerability of current cryptographic protocols in connected vehicles to quantum attacks, propose Quantum-safe alternatives*
  - *Investigate the impact of quantum computing on existing encryption algorithms*
  - *Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it)*

bluewind

- Authenticating ECUs through CAN bus physical signals
  - *CAN lacks any kind of message authentication*
  - *Extracting features from the physical CAN signals (fingerprinting)*
  - *Possible internship with company to gather dataset*
  - *Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it)*

Membership Inference Attack (MIA)

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Modeling the distribution of distinguishable metric for non-member data

  - *Target:* find a suitable metric to make the **member data (training data)** as the extreme values (outliers) of the **non-member data (test data or data from similar or different distributions)** distribution

  - *Proposal (key steps):*
    1. *Acquire the knowledge of MIAs and Extreme Value Theory*
    2. *Design functions to display the metric distribution of the data*
    3. *Try previous metrics in MIAs*
    4. *Find a new metric*

  - *Requirements:* Basic Python, Basic Machine Learning, Skilled Statistics (especially, Extreme Value Theory)

  - *Contact person:*
    Anderson Rocha ( )
    Jiaxin Li ( )

Automotive Security

- Resilience Testing for Connected Vehicles
  - *Develop methodologies for resilience testing to assess how well connected vehicles can withstand and recover from cyber-attacks*
  - *Implement scenarios that simulate cyber-attacks on various components of connected vehicles, including communication networks, ECUs, and sensors*
  - *Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it)*

bluewind

- Cyber Threat Intelligence on Automotive
  - *Evaluate the effectiveness of threat intelligence sharing platforms specific to the automotive industry*
  - *History of vulnerabilities, countermeasures and intelligence related to the automotive industrial process*
  - *Contact person: Francesco Marchiori (francesco.marchiori@math.unipd.it)*

Covert channels

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Solution for Covert Channel in Federated Learning systems
  - FL systems can be turned into covert channels to implement a stealth communication infrastructure;
  - Based on the POC of the attack, we want to develop the countermeasure to solve the issue;
  - The solution might involve Differential Privacy or Anomaly Detection techniques.

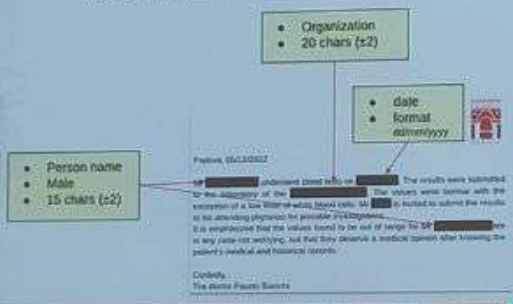
- *Contact person:*
  Simone Soderi (simone.soderi@unipd.it)
  Gabriele Orazi (gabriele.orazi@phd.unipd.it)
  Jiaxin Li (jiaxin.li@studenti.unipd.it)

Document UnRedaction

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Context Driven Un-redaction of documents
  - Redaction is used to hide and obfuscate sensitive and personal information in documents (PII).
  - Are we really protecting PII? How much information is still leaking? How much we can infer from the context?
  - The aim is prove the ineffectiveness of current redaction techniques.
  - Main subject: NLP (specifically, Named Entity Recognition)
  - *Contact person: Gabriele Orazi ([redacted]) and Francesco Marchiori ([redacted])*



Drones and Autonomous Driving

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Drones Startup Safety Check

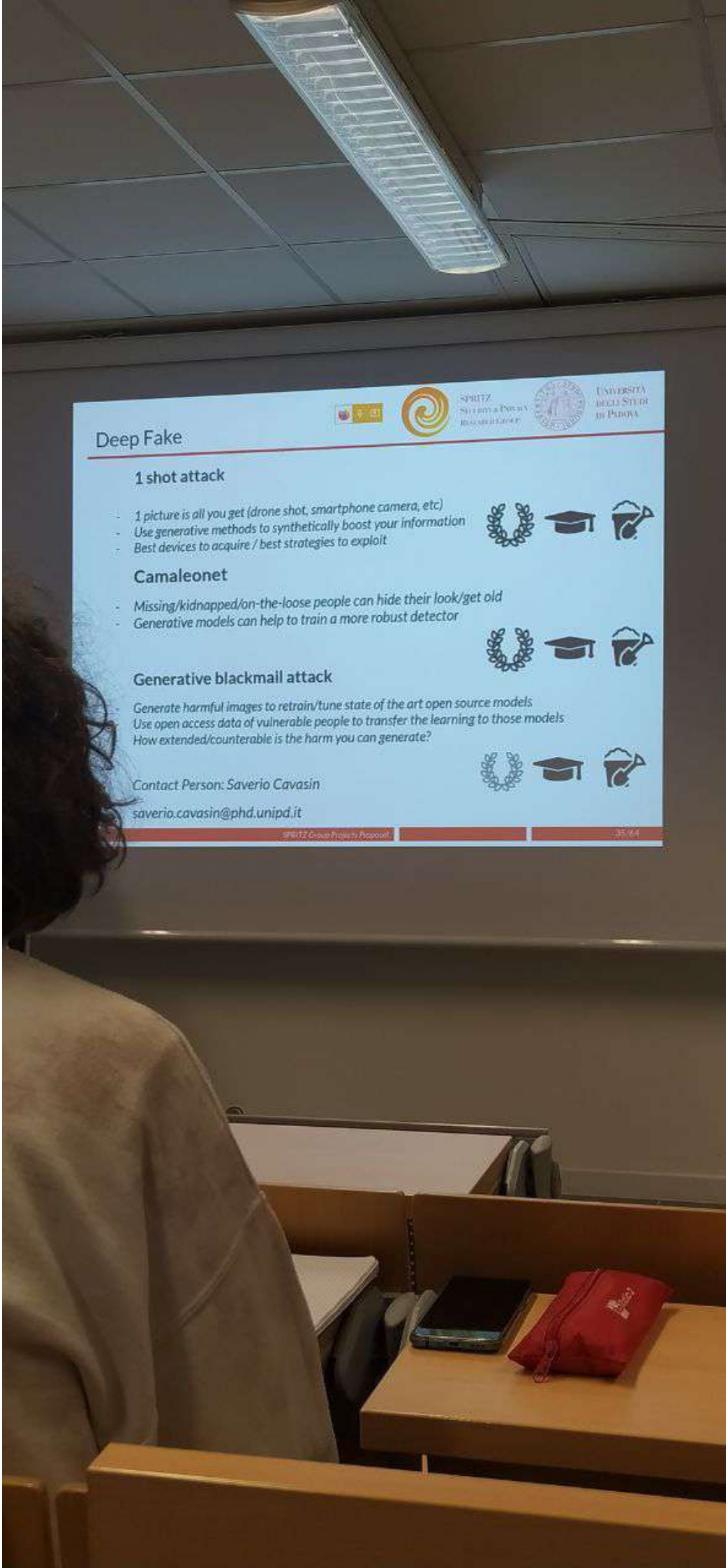
Upon starting up, drones execute a protocol to check all components and that everything is ok

How does it work? Can we spoof some of the messages?

- *Contact Person: Alessandro Brighente*
- [redacted]

Driving Behavior Authentication

- *There currently exists many datasets and solutions to identify drivers based on how they drive*
- *Write a survey on the best practices and compare them*
- *Contact Person: Alessandro Brighente*
- *alessandro.brighente@unipd.it*


Deep Fake
1 shot attack
- 1 picture is all you get (drone shot, smartphone camera, etc)
- Use generative methods to synthetically boost your information
- Best devices to acquire / best strategies to exploit
Camaleonet
- Missing/kidnapped/on-the-loose people can hide their look/get old
- Generative models can help to train a more robust detector
Generative blackmail attack
- Generate harmful images to retrain/tune state of the art open source models
Use open access data of vulnerable people to transfer the learning to those models
How extended/counterable is the harm you can generate?
Contact Person: Saverio Cavasin
saverio.cavasin@phd.unipd.it
SPRITZ Group Projects Proposal
35/64

Privacy and Anonymity

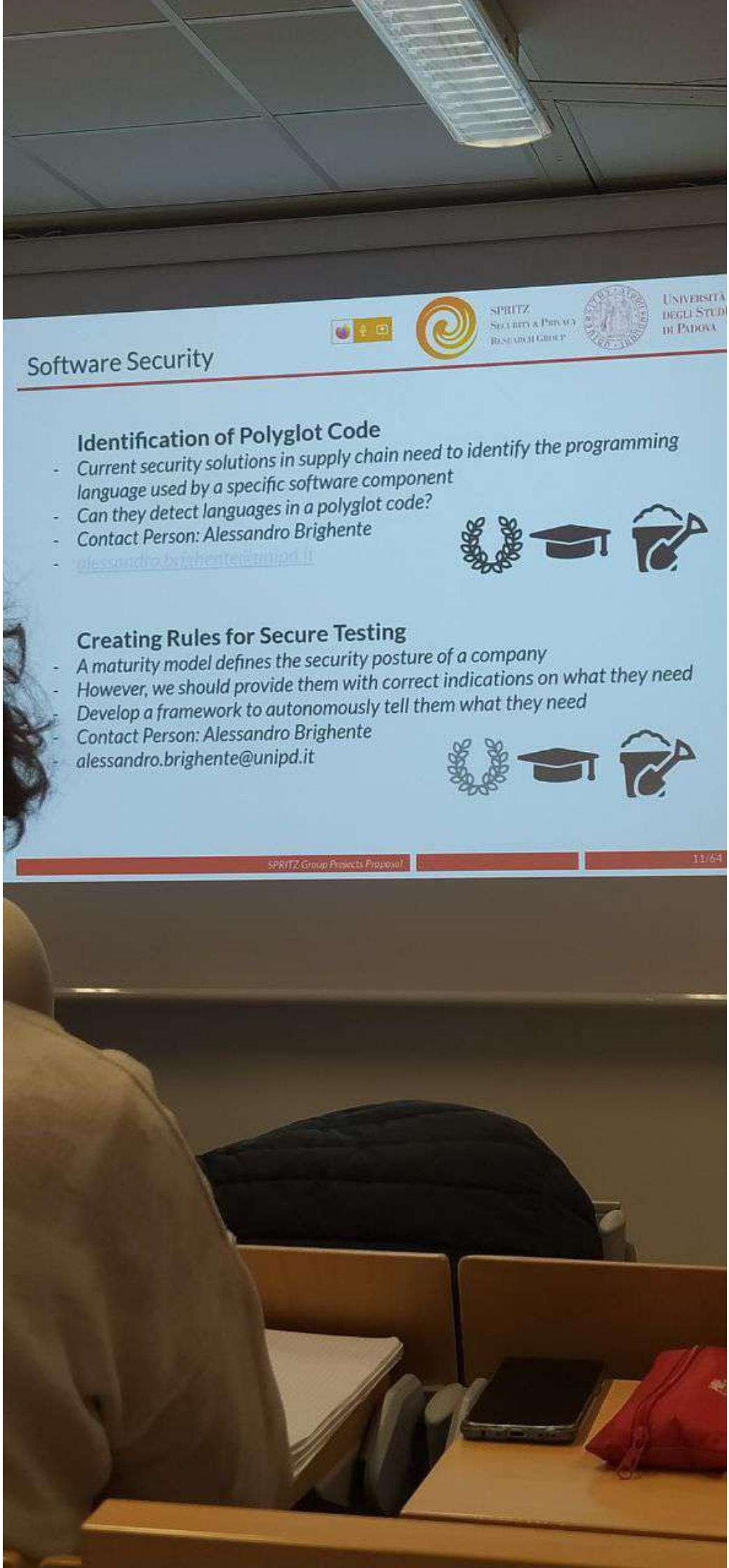
Tracking users in Wi-Fi

- *Probe requests are packets needed to connect to a wi-fi network*
- *MAC address randomization is not sufficient anymore, use reduced sets.*
- *How much should we reduce and is that actually effective?*
- *Contact Person: Alessandro Brighente*
- *alessandro.brighente@unipd.it*

Is Easy-Connect Really Secure?

Easy connect allows for zero touch device provisioning
How much information does it need and how secure is it?

- *Contact Person: Alessandro Brighente*
- *alessandro.brighente@unipd.it*


SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova
Software Security
Identification of Polyglot Code
- Current security solutions in supply chain need to identify the programming language used by a specific software component
- Can they detect languages in a polyglot code?
- Contact Person: Alessandro Brighente
- alessandro.brighente@unipd.it
Creating Rules for Secure Testing
- A maturity model defines the security posture of a company
- However, we should provide them with correct indications on what they need
- Develop a framework to autonomously tell them what they need
- Contact Person: Alessandro Brighente
- alessandro.brighente@unipd.it
SPRITZ Group Projects Proposal
11/64

5G and IoT Security

SPRITZ Security and Privacy Research Group

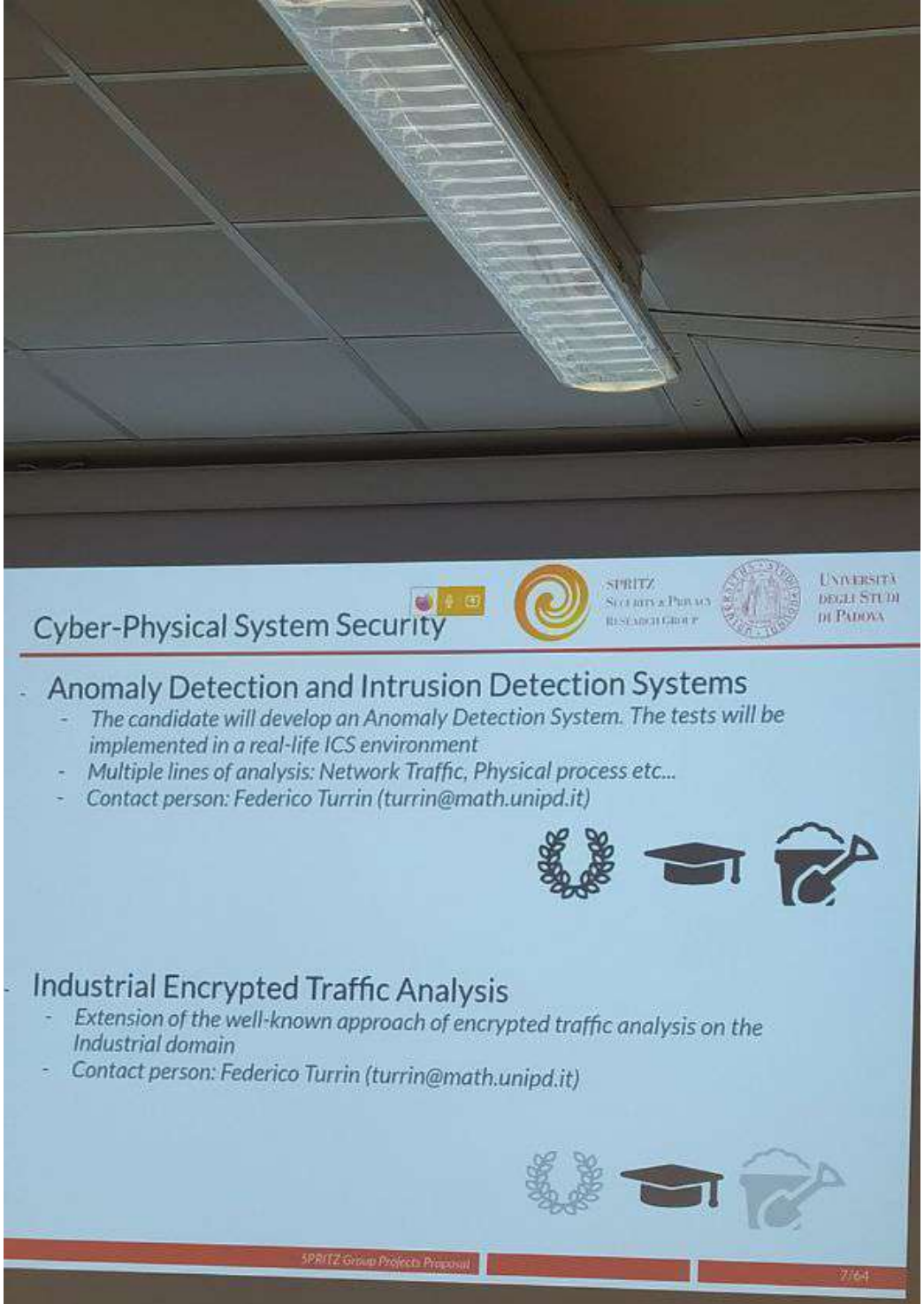
Università degli Studi di Padova

Jamming IoT Devices

- *IoT devices transmit on different channels to avoid interference*
- *In this project you will develop a module able to follow the channel sequence and interrupt the communication*
- *Contact Person: Alessandro Brighente*
- *alessandro.brighente@unipd.it*

End-to-end attack to 5G networks

- *The core network is responsible for device localization and tracking*
- *In this project, you will develop an end-to-end simulation of the 5G system using open source software, and testing attacks to its localization capabilities*
- *Contact Person: Alessandro Brighente*
- *alessandro.brighente@unipd.it*



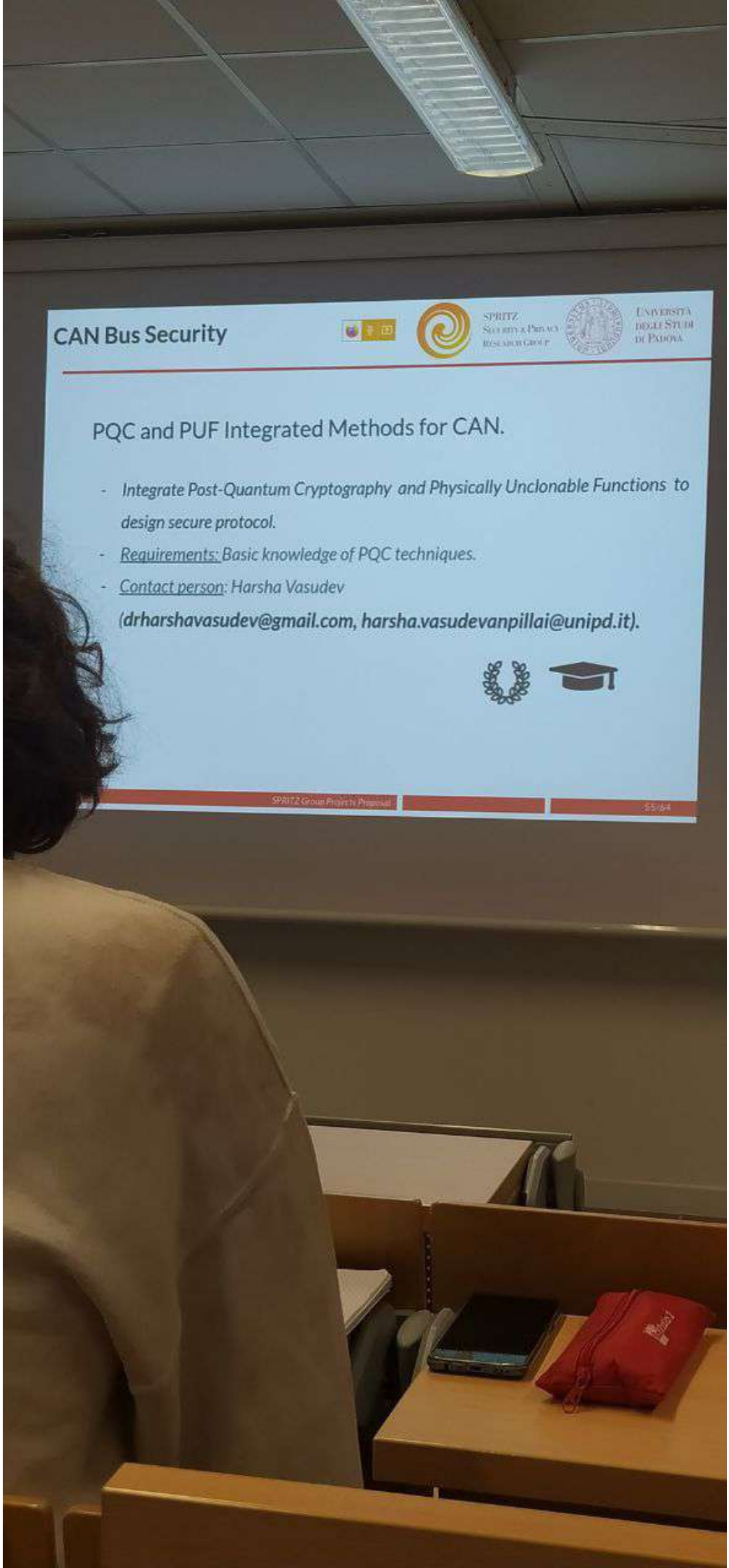
Cyber-Physical System Security

SPRITZ Security and Privacy Research Group

Università degli Studi di Padova

- **Anomaly Detection and Intrusion Detection Systems**
  - *The candidate will develop an Anomaly Detection System. The tests will be implemented in a real-life ICS environment*
  - *Multiple lines of analysis: Network Traffic, Physical process etc...*
  - *Contact person: Federico Turrin (turrin@math.unipd.it)*

- **Industrial Encrypted Traffic Analysis**
  - *Extension of the well-known approach of encrypted traffic analysis on the Industrial domain*
  - *Contact person: Federico Turrin (turrin@math.unipd.it)*


CAN Bus Security
SPRITZ Security & Privacy Research Group
Università degli Studi di Padova
PQC and PUF Integrated Methods for CAN.
- Integrate Post-Quantum Cryptography and Physically Unclonable Functions to design secure protocol.
- Requirements: Basic knowledge of PQC techniques.
- Contact person: Harsha Vasudev
(drharshavasudev@gmail.com, harsha.vasudevanpillai@unipd.it).
SPRITZ Group Projects Proposal
55/64