europass

Adriana Maria Berdich

WORK EXPERIENCE

07/07/2015 – 29/09/2019 Timisoara, Romania

FUNCTION AND SOFTWARE DEVELOPER CONTINENTAL AUTOMOTIVE ROMANIA

Main focus on function development in vehicle motion functions through all phases of the V-model:

1. requirement engineering,
2. concept,
3. function (mainly model-based development),
4. software (automatic code generation),
5. verification and validation.

28/02/2019 – 29/06/2020 Timisoara, Romania

ENGINEER RESEARCHER POLITEHNICA UNIVERSITY OF TIMISOARA

Research focusing on environment based device association:

1. overview of existing research topics in order to understand the state-of-the-art.
2. experiments, preparation and publication of conference and journal papers.

30/09/2019 – 31/03/2023 Timisoara, Romania

FUNCTION DEVELOPER VITESCO TECHNOLOGIES

Function Pilot for Renault and Alliance Renault-Nissan projects with main focus on:

1. organize and trigger the activities on software and function side after a pre-analysis.
2. requirement engineering.
3. tests on car for distinct calibration maturity level on injection realization component.

Function Developer with main focus on torque structure and vehicle motion functions.
World wide responsible for:

1. vehicle speed calculation,
2. vehicle acceleration calculation,
3. distance calculation,
4. engine speed limitation,
5. engine speed control,
6. torque determination.

06/10/2021 – 15/12/2021 Timisoara, Romania

ENGINEER RESEARCHER POLITEHNICA UNIVERSITY OF TIMISOARA

Researcher in the "New concepts for Secure Connectivity inside Cars" project financed by Ben-Gurion University of the Negev with main focus on:

1. sensor and ECU fingerprinting.
2. automotive cybersecurity, i.e., CAN bus security.

03/04/2023 – CURRENT Timisoara, Romania

SYSTEM TECHNICAL PROJECT MANAGER VITESCO TECHNOLOGIES

1. participates in creating offers in regards to technical concept and offers support for customer presentation.
2. ensures the reuse of available technical content.
3. monitors the status of all disciplines in the project.
4. prepares and performs project reviews (i.e. Engineering release, milestones)
5. performs risk identification, analysis, control and steers the implementation of risk response measures within research and development teams.
6. monitors the status of the engineering test activities.
7. coordinates and leads of technical project development team.
8. define the detailed project planning of technical development.
9. planning the tasks and assigning to discipline responsibles.

EDUCATION AND TRAINING

08/2013 – 06/2017 Romania

ENGINEER'S DEGREE IN AUTOMATION AND APPLIED INFORMATICS Politehnica University of Timisoara

Address Romania | **Website** https://ac.upt.ro/

08/2017 – 06/2019

MASTER'S DEGREE IN COMPUTER AND INFORMATICS SCIENCES AND SUPPORT SERVICES Politehnica University of Timisoara

08/2019 – CURRENT Romania

PHD IN MOBILE AND AUTOMOTIVE CYBERSECURITY Politehnica University of Timisoara

Address Romania | **Thesis** Fingerprinting Smartphones From Embedded Transducers

LANGUAGE SKILLS

Mother tongue(s): **ROMANIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C1	C1	C1	C1	C1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Good listener and communicator | Decision-making | Team-work oriented | Organizational and planning skills | Motivated | People oriented

Standards

ISO21434 | SAE J3061 | ISO26262

Tehnical

Matlab,Matlab Simulink | Latex: advanced user | Automotive Security | Deep Learning | Embeded C | ETAS INCA | Requirement Engineering | Machine Learning | Validation and Verification

ADDITIONAL INFORMATION

PUBLICATIONS

Sweep-to-Unlock: Fingerprinting Smartphones based on Loudspeaker Roll-off Characteristics – 2021

Fingerprinting smartphones based on acoustic characteristics of their loudspeaker may have a number of applications in device-to-device authentication as well as in forensic investigations. In this work we propose an efficient fingerprinting methodology by using the roll-off characteristics of the device speaker, i.e., the transition between the low and high stopbands to the passband segment of the speaker. We extract roll-off characteristics from sweep signals, also know as chirps, that are commonly used in practice to test speaker response. This procedure appears to be more stable against variations of the volume level and allows the use of simple linear approximations, which are intuitive and easy to compute, in order to extract the fingerprint. To increase detection accuracy, on the basis of the proven performance of deep learning techniques, a convolutional and a bi-directional long short term memory neural network are further proposed and their performance demonstrated for authentication purposes. While numerous applications may be envisioned, we specifically focus on the use of speaker characteristics in relation to in-vehicle infotainment units, checking if recordings from these units can be used to fingerprint a specific phone.

Fingerprinting Smartphones Based on Microphone Characteristics From Environment Affected Recordings

– 2022

Fingerprinting devices based on unique characteristics of their sensors is an important research direction nowadays due to its immediate impact on non-interactive authentications and no less due to privacy implications. In this work, we investigate smartphone fingerprints obtained from microphone data based on recordings containing human speech, environmental sounds and several live recordings performed outdoors. We record a total of 19,200 samples using distinct devices as well as identical microphones placed on the same device in order to check the limits of the approach. To comply with real-world circumstances, we also consider the presence of several types of noise that is specific to the scenarios which we address, e.g., traffic and market noise at distinct volumes, and may reduce the reliability of the data. We analyze several classification techniques based on traditional machine learning algorithms and more advanced deep learning architectures that are put to test in recognizing devices from the recordings they made. The results indicate that the classical Linear Discriminant classifier and a deep-learning Convolutional Neural Network have comparable success rates while outperforming all the rest of the classifiers.

Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport – 2020

We address the secure pairing of mobile devices based on accelerometer data under various transportation environments, e.g., train, tram, car, bike, walking, etc. As users commonly commute by several transportation modes, extracting session keys from various scenarios to secure the private network of user's devices or even the public network formed by devices belonging to distinct users that share the same location is crucial. The main goal of our work is to establish the amount of entropy that can be collected from these environments in order to determine concrete security bounds for each environment. We test several signal processing techniques on the extracted data, e.g., low-pass and high-pass filters, then apply sigma-delta modulation in order to expand the size of the feature vectors and increase both the pairing success rate and security level. Further, we bootstrap secure session keys by the use of existing cryptographic building blocks EKE (Encrypted Key Exchange) and SPEKE (Simple Password Exponential Key Exchange). We implement our proof-of-concept application on Android smart-phones and take benefit from numerical processing environments for the off-line analysis of the collected datasets.

ANTARES-ANonymous Transfer of vehicle Access Rights from External cloud Services – 2020

As car sharing becomes an increasingly common task, mediating user access rights from external servers comes with threats regarding user’s privacy. Clearly, users can be tracked by service mediators, e.g., cloud providers, that manage vehicle fleets, etc. In this work we design and test a simple solution based on oblivious transfer, a well-known and secure cryptographic block, that allows to preserve user’s privacy when gaining access to the vehicle. We test the feasibility of deploying such a solution on Android capable smartphones but also account for potential in-vehicle components, e.g., car head units, that may be soon put to such tasks. We use Microsoft Azure as cloud service provider and deploy a Java implementation, based on the Bouncy Castle cryptographic library, on the server side. Our experimental results show that Android based units are capable of handling the required cryptographic operations and the implementation of the employed protocol can be done by existing open-source support.

Secure Audio-Visual Data Exchange for Android In-Vehicle Ecosystems – 2021

Mobile device pairing inside vehicles is a ubiquitous task which requires easy to use and secure solutions. In this work we exploit the audio-video domain for pairing devices inside vehicles. In principle, we rely on the widely used elliptical curve version of the Diffie-Hellman key-exchange protocol and extract the session keys from the acoustic domain as well as from the visual domain by using the head unit display. The need for merging the audio-visual domains first stems from the fact that in-vehicle head units generally do not have a camera so they cannot use visual data from smartphones, however, they are equipped with microphones and can use them to collect audio data. Acoustic channels are less reliable as they are more prone to errors due to environmental noise. However, this noise can be also exploited in a positive way to extract secure seeds from the environment and audio channels are harder to intercept from the outside. On the other hand, visual channels are more reliable but can be more easily spotted by outsiders, so they are more vulnerable for security applications. Fortunately, mixing these two types of channels results in a solution that is both more reliable and secure for performing a key exchange.

Car-to-Smartphone Interactions: Experimental Setup, Risk Analysis and Security Technologies – 2019

Vehicle access control and in particular access to in-vehicle functionalities from smart mobile devices, e.g., phones or watches, has become an increasingly relevant topic. Security plays a critical part, due to both a long history of car keys that succumbed to attacks and recently reported intrusions that use various vehicle communication interfaces to further gain access to in-vehicle safety-critical components. In this work we discuss existing technologies and functionalities that should be embedded in an experimental setup that addresses such a scenario. We make emphasis on existing cryptographic technologies, from symmetric to asymmetric primitives, identity-based cryptography and group signatures. We also discuss risks associated with in-vehicle functionalities and mitigation, e.g., intrusion detection systems.

PRESTvO: Privacy enabled smartphone based access to vehicle on-board units – 2020

Smartphones are quickly moving toward complementing or even replacing traditional car keys. We advocate a role-based access control policy mixed with attributes that facilitates access to various functionalities of vehicular on-board units from smartphones. We use a rights-based access control policy for in-vehicle functionalities similar to the case of a file allocation table of a contemporary OS, in which read, write or execute operations can be performed over various vehicle functions. Further, to assure the appropriate security, we develop a protocol suite using identity-based cryptography and we rely on group signatures which preserve the anonymity of group members thus assuring privacy and traceability. To prove the feasibility of our approach, we develop a proof-of-concept implementation with modern smartphones, aftermarket Android head-units and test computational feasibility on a real-world in-vehicle controller. Our implementation relies on state-of-the-art cryptography, including traditional building blocks and more modern pairing-friendly curves, which facilitate the adoption of group signatures and identity-based cryptography in automotive-based scenarios.

Smartphone Camera Identification from Low-Mid Frequency DCT Coefficients of Dark Images

Camera sensor identification can have numerous forensics and authentication applications. In this work, we follow an identification methodology for smartphone camera sensors using properties of the Dark Signal Nonuniformity (DSNU) in the collected images. This requires taking dark pictures, which the users can easily do by keeping the phone against their palm, and has already been proposed by various works. From such pictures, we extract low and mid frequency AC coefficients from the DCT (Discrete Cosine Transform) and classify the data with the help of machine learning techniques. Traditional algorithms such as KNN (K-Nearest Neighbor) give reasonable results in the classification, but we obtain the best results with a wide neural network, which, despite its simplicity, surpassed even a more complex network architecture that we tried. Our analysis showed that the blue channel provided the best separation, which is in contrast to previous works that have recommended the green channel for its higher encoding power.

CarTwin—Development of a Digital Twin for a Real-World In-Vehicle CAN Network – 2023

Digital twins are used to replicate the behavior of physical systems, and in-vehicle networks can greatly benefit from this technology. This is mainly because in-vehicle networks circulate large amounts of data coming from various sources such as wired, or in some cases even wireless, sensors that are fused by actuators responsible for safety-critical tasks that require careful testing. In this work, we build a laboratory in-vehicle network that mimics a real vehicle network in regards to wire length, number of stubs and devices that are connected to it. The Controller Area Network (CAN), which is still the most popular communication bus inside cars, is used as a network layer. Using models defined in MATLAB for various subsystems, e.g., Anti-lock Braking System (ABS), Powertrain and Electric Power-Steering, deployed on automotive-grade microcontrollers, we evaluate the in-vehicle bus digital twin by providing realistic inputs and recording and reproducing in-vehicle network traffic. The experimental results showed good correlation between the output of the implemented digital twin and the data collected from an actual car.

Master-Slave Tracking System for Mobile Robots – 2018

In mobile robot applications, to track and follow moving targets is a challenging task. In this paper there is developed a robot tracking system with two mobile robots: the master robot tele-operated from an Android application via Bluetooth, and the autonomous slave robot with three ultrasonic sensors which will track the master. The tracking algorithm of the slave robot employs: i) a position control to maintain a constant distance between slave and master, and ii) a tracking direction control in one of the six control states detected by a finite-state machine based on fuzzy logic, with smooth transitions between states. The master-slave mobile robot system and the tracking algorithm are designed and implemented by using low-cost microcontroller boards. The experimental results validate the proposed master-slave solution with tracking algorithm.