ERC Consolidator Grant 2016
Research proposal [Part B1]

DIGITAL SHADOW:
PRIVATE DIGITAL AUTHENTICATION FOR THE PHYSICAL WORLD

— DIGIDOW —

- **Principal investigator (PI)**: René Mayrhofer
- **Host institution**: Johannes Kepler University Linz (JKU), Faculty of Engineering and Natural Sciences, Institute of Networks and Security (INS)

- **Proposal full title**: Digital shadow: Private digital authentication for the physical world
- **Proposal short name**: Digidow
- **Proposal duration**: 60 months (5 years)

How can we use digital identity for authentication in the physical world without compromising user privacy? This central question is an underlying concern for further groundbreaking developments in ubiquitous computing scenarios: enabling individuals to – for example – use public transport and other payment/ticketing applications, access computing resources on public terminals, or even cross country borders without carrying any form of physical identity document or trusted mobile device. Moving towards such a device-free infrastructure-based authentication could be easily facilitated by centralized databases with full biometric records of all individuals, authenticating and therefore tracking people in all their interactions in the digital and physical worlds. However, such centralized tracking is not compatible with fundamental human rights to data privacy. We therefore propose a fully decentralized approach to digital user authentication in the physical world, giving each individual better control over their digital and physical world interactions and data traces they leave.

In project *Digidow*, we will associate each individual in the physical world with a personal agent in the digital world, facilitating their interactions with purely digital or digitally mediated services in both worlds. This proposal has two major issues to overcome. The first is a problem of massive scale, moving from current users of digital identity to the whole global population as the potential target group. The second is even more fundamental: by moving from trusted physical devices and centralized databases to a fully decentralized and infrastructure-based approach, we remove the currently essential elements of trust. We will solve these issues based on a fundamental model for private tracking of user location and behavior, implement it in personal agents with a complete chain of trust over multiple parties, and build yearly prototypes for benchmark use cases like border control.

Section a: Extended Synopsis of the Scientific Proposal

We must plan for freedom, and not only for security,
if for no other reason than that only freedom can make security secure.
Sir Karl Raimund Popper, The Open Society and Its Enemies (1945)
For today's digital world, replace freedom with privacy.

1 Introduction

Digital identity will be a cornerstone of future applications, both in the digital and in the physical domains. Many services and activities of daily life are already purely digital or digitally mediated. Authenticating to these services currently requires manifold accounts with different usernames and passwords, causing problems both for usability and security. There are some technical approaches to assist users in managing these many accounts, including locally installed password manager software, dedicated web services, or trusted personal hardware devices such as smartcards or USB tokens to store the private keys and passwords. In the last few years, personal mobile devices – in particular the ubiquitous smart phones – have seen increased use for managing digital identities as proxies for their users. Consequently, many approaches to improve the seamless use of (digital) services with such digital identities (sometimes called electronic ID or e-ID) have been suggested, especially on the EU level.

Moving beyond the digital into the physical world, user authentication becomes directly entwined with activities and interactions of each individual, often spanning the boundaries between these domains. One motivating example is crossing country borders: currently, we have to handle physical objects (passports) that serve two purposes: to carry digital information (the various aspects of the individual's identity), and to make forging harder by relying on physical tokens that are supposedly more difficult to clone than the information they carry[1]. Such an interaction in the physical world then has direct consequences in the digital: validating information provided by the physical token in centralized databases, storing data traces of those interactions, debiting an account, etc. Many actions in the "real" physical world are therefore already shadowed in the digital one.

In addition to being inconvenient, the current reliance on physical objects poses a security risk of these objects being lost, stolen, or becoming unusable. Biometric authentication of individuals together with cryptographically signed digital identity documents stored in centralized databases has long been envisioned as a way to more seamlessly bridge this gap, supporting users to use even more different services with less direct attention[2]. The obvious disadvantage is that these centralized databases, tracking each interaction of individuals across both worlds, are in direct conflict with the fundamental human right to privacy [1, 2]. Current trends in the combination of social networks, big data analysis, and governmental surveillance pose immediate risk to free speech, social development of future generations, and democratic processes [3, 4]. Commercial players (such as search engine and social network companies) are already offering to act as digital identity providers, and transparent face recognition using central databases under their control is only a small – albeit dangerous – step ahead. We believe this direction not to be in the best interests of the European Union.

The goal of this proposal is therefore to enable for the first time ever **trustworthy infrastructure based biometric authentication without centralized databases**. Specifically, we aim for two big leaps with major consequences to authenticating individuals for real-life services:

(a) With biometric sensors distributed in the infrastructure, **individuals should no longer be required to carry any physical objects for proving their identity**, improving both *convenience* and *security*.

(b) Building a fully decentralized architecture, **individuals remain in control over the use of their digital identity**, providing *privacy* guarantees in accordance with European data privacy laws.

Our approach focuses on a decentralized architecture as summarized in Figure 1, specifically and intentionally spanning multiple parties under different administrative control and aiming at security levels that are sufficient to replace current international travel documents (passports).

[1] The same purposes are served by physical cash, other license documents, or physical keys.

[2] Science fiction has extensively experimented with this vision, for example with ubiquitous optical face and iris scanning in the popular movie "Minority Report".

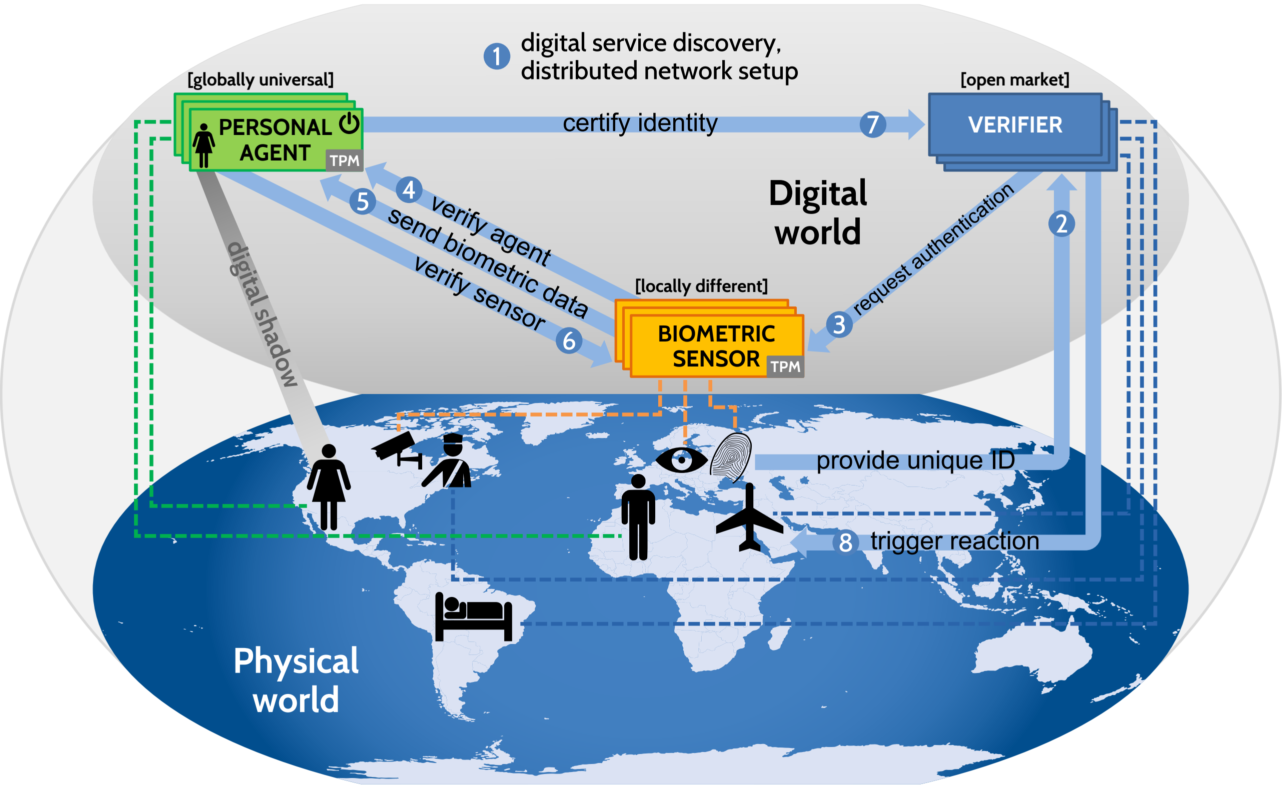

Figure 1: Conceptual overview of decentralized use of digital identity for services in the physical world

Sticking to this example of border control (with an assumed step (0) of creating the digital identity by the individual's home country), step (1) requires discovery of identity services spanning multiple countries in preparation of step (2), in which the person intending to cross a border may provide some form of unique identifier (e.g. full name, date and place of birth). Each individual is associated with a *personal agent* that acts as their **digital shadow**, tracking their actions in the physical world and mediating interactions with the digital one. This personal agent remains under administrative control of its associated user, who can freely choose where to run it (e.g. on a smart home controller in their own residence, at a cloud provider of their choice such as their bank, or even on their mobile phone) and when to turn it off. The (globally universal) agent manages various forms of identification, payment mechanisms, or other access tokens the user holds. In step (3), border control will then request verification of the claimed identity. Individuals are authenticated by (locally different) *biometric sensors* (such as cameras, fingerprint sensors, etc.) distributed throughout the infrastructure, which communicate their measurements to personal agents for verification. Because agents and sensors are controlled by different parties, they have to mutually verify their authenticity in steps (4) and (6) during the process of exchanging the (live) sensor data in step (5). The authenticated digital identity can then be used with an open-ended set of *verifiers* (such as border control, public transport, hotels, etc.) for physical or digital services. In practice, we distinguish this use of digital identity into certifying the claimed identity with a digital document in step (7), e.g. sending a digital passport certificate to the border gateway, and the action triggered in the physical world in step (8), e.g. opening the gate. Although personal agents will be under direct control of individuals, the whole system needs to support sufficient trust to replace physical identity documents and centralized databases.

On a technical level, we will formally design protocols and system components, simulate their behavior for interoperability and scalability analysis, and build prototype implementations of central components and exemplary sensors. Yearly demonstration prototypes will integrate current results from different project areas and support high-level architecture reviews and dissemination to a wider audience. On a social level, we will run user studies for evaluating usability and trust issues. On a legal level, we will take into account current laws and regulations on identity documents and privacy. All these levels build upon previous, extensive experience in the domain of mobile device security and bringing identity documents onto smart phones. This proposal brings together different lines of research among our group, and intends to produce a completely new basis for implementing many of the scenarios described in ubiquitous and mobile computing research.

2 State of the art and project focus: What is missing

For currently deployed systems, authentication in the physical world depends on physical identity documents backed by validation through centralized databases with all the disadvantages discussed above. To alleviate the first issue of carrying many physical documents, there is an active field of current research projects that aim at integrating digital identity documents into smart phones. One of these projects is currently performed within the scope of our own Josef Ressel Center for User-friendly Secure Mobile Environments (*JRC u'smile*, `https://usmile.at`, which forms a joint research group with the Institute of Networks and Security at JKU, both lead by the PI). We aim for a working prototype of an Austrian mobile driving license (AmDL) running on Android devices within the next 6–12 months. To achieve security levels in accordance with current legislation, private keys and dynamic cryptographic signing will be implemented on UICCs (SIM cards) as the currently ubiquitous programmable smart cards. Recent cryptographic work for privacy-conscious digital ID [5, 6, 7, 8] leaves an unsolved issue of revoking IDs without compromising pseudonymity or anonymity, and assumes physically trusted tokens instead of a decentralized infrastructure based authentication. For the remainder of this proposal, we define digital ID on smart phones as current state-of-the-art (even if it has not been widely deployed yet) and base further discussions on this assumption.

Similar in terms of underlying technology, authentication options for and use of digital identity for purely digital services are currently being investigated, including EU projects such as STORK [9] and FutureID [10] or the eIDAS regulation [11]. These are orthogonal to Digidow and could benefit directly and immediately from an implementation of decentralized, transparent e-ID.

The missing big step is secure authentication without physical objects carried by individuals, relying on biometric infrastructure sensors for seamless interaction in the physical world. It is not surprising that this step has not yet been taken, as the conflicting requirements of convenience, security, and privacy make it challenging on many levels. We argue that the inherently diversified and decentralized political and social culture within the European Union will more likely support a decentralized, privacy-aware architecture than other, more centralized or company-oriented structures – Digidow is therefore intentionally proposed at the EU level for the research and prototype development phase, but with a future global outlook for deployment.

3 Main challenges: What needs to be solved

There are two major issues to overcome. The first is a **problem of scale**: moving from current (potential) users of digital ID (i.e. smart phone users) to the whole global population as the (potential) target group (which is already starting to become difficult for digital-only eID on just Austrian scale [12]). The second is even more fundamental: by moving away from trusted personal objects (physical identity documents like passports or smart phones with embedded smart cards), we remove one currently central **element of trust**. Future infrastructure components will be installed and run by potentially untrustworthy third parties, and any authentication use of such an infrastructure will have to tackle the issue of trust from both points of view: a) individuals and their digital shadows (we call them the proving party or provers, implemented by the personal agents) will have to – at least partially – trust the sensors scattered throughout the physical world not to abuse their raw measurements so as to give rise to identity theft; and b) third parties authenticating users (we call them the verifying party or verifiers) will have to – at least partially – trust the same sensors to provide live, authentic, and sufficiently complete data of the users to be authenticated, and additionally trust the personal agents to provide correct identities. Finally, agents and verifiers will additionally have to trust each other's protocol runs for the transaction at hand. This includes a set of specific open research issues:

- Globally scalable, distributed network service discovery (Figure 1, step 1) is required to establish the set of cooperating parties for each individual interaction. The main challenges are **scale** and **latency**.
- Biometric authentication of users needs to be made secure, usable, and privacy-conscious. Current systems typically support two out of three of these requirements, and the main challenge is therefore to develop **multi-party protocols** (Figure 1, steps 4–7) together with sensor data analysis approaches to enable private (under the control of the user, not the sensor or verifier) use of modern biometric methods.
- To be perceived as secure and trustworthy by a global, highly diverse population with different cultural backgrounds, personal agents and biometric sensors themselves need to be secure, with the obvious challenge of current software engineering practices being seemingly unable to create **secure code**. Personal agents

become a central component of individuals' digital lives, and are therefore an obvious target for attacks. Furthermore, this security and privacy compliance needs to be communicable to non-experts to enable a wide range of the global population to trust such a complex system.

It is important to note that all of these research issues carry high risk, and it is possible that some deviations to the proposed architecture will be necessary. We firmly believe that the overall concept is workable even when some issues cannot be directly addressed but need to be worked around (we already have some alternatives).

4 Scientific approach: How we will solve it

In addition to many engineering challenges that will be solved in building the Digidow architecture and which in turn are expected to raise more scientific issues, there are three particular novel approaches in our design:

- With respect to the physical world, the game-changing concept is **private user tracking**. Currently, individuals are being tracked by different institutions, including e.g. advertiser networks in the digital domain or mobile phone operators and government agencies in the physical one. This is problematic from a privacy point of view, because it can be easily abused without knowledge of the concerned individuals. If, however, personal agents with a direct, one-to-one relationship to "their" users perform this tracking, then we can utilize the advantages without sacrificing user privacy. Note that private tracking of individuals among physical locations and through their interactions in the physical and digital worlds enables to solve currently difficult challenges: a) Biometric authentication is never error-free, and we will therefore combine multiple biometric events from infrastructure devices and correlate their readings in a single probabilistic model for each individual. By including tracking in time and location, we support more accurate estimates of user interactions. b) Service discovery between the three parties for every single interaction within a few seconds each (assuming users will not be prepared to wait longer before e.g. entering public transport) does not seem realistic without prior knowledge. By taking into account the physical location of users, we will significantly limit the search space and therefore allow service discovery to be globally scalable with short latencies.
- In the digital world, we will utilize identity-based cryptography (IBC, most probably in an elliptic curve variant) in combination with overlay networks to provide pseudonymous and, for some use cases anonymous, communication. This is akin to the cryptographic protocol architecture of Bitcoin [13], but with significant scientific challenges in scale (one personal agent per individual), latency (transaction times of few seconds instead of 10 minutes), and the addition of global service discovery on top of this network. One specific novel approach is a multi-phase service discovery/use process on top of DNS/DHT-indexed overlay networks, but with the added challenge of making DHTs anonymous (which they are not in current designs [14]).
- To better guarantee the security of biometric sensors and personal agents, we will combine hardware/firmware security approaches (including TPMs in complex sensor systems such as networked cameras [15]) with short-term certificates (e.g. renewed daily) for reputation management of infrastructure components participating in the global service discovery. The highly critical code of personal agents will be (semi-) formally specified, designed for reproducible builds, verified statically during compile time, validated in a multi-party chain of trust starting from power-on, and verified dynamically for conformance to protocol specifications. All these methods require novel approaches in detail (cf. part B2), and a fundamentally new way of combining them.

Together, these design aspects allow personal agents to track their associated users as they move throughout the physical world, while denying this complete tracking to third parties by regularly changing the cryptographic identity (pseudonyms) used for specific transactions. One very unconventional approach to integrate both aspects that we will investigate is to combine the physical location of an individual with the pseudonym derived from IBC, and therefore to bind a specific transaction to both the physical and digital domains[3].

Summary of the scientific approach: Through our fundamentally novel model for private user tracking, we at the same time improve security (with a more comprehensive statistical model of physical and digital interactions of each individual), convenience (by relieving users from carrying physical objects and decreasing the latency for service discovery and other scalability issues), and user privacy (because these models are computed by secure and trusted personal agents and therefore remain under the control of each individual themselves, and

[3] Note that a cryptographic binding of physical location with the pseudonym used for an interaction across the physical/digital interface makes attacks much harder when verifiers also take this into account in their protocol run. Attackers would be limited to the same geographic area, and could no longer act globally, making identity theft less scalable than it is now with standard user accounts.

through the automatic use of pseudonymous transactions). If successful, implications will be far-reaching, enabling countries and service providers within and outside the EU to deploy completely new ways of securely authenticating and interacting with individuals in a privacy-conscious manner.

5 Project structure and existing resources: How and why the project will work

The project will be structured in four distinct research areas, overlapping in terms of research challenges and high-level project goals they address, but defined by the different scientific methods required to address them:

- Area A ("Authentication") will focus on multi-party biometric authentication (with third parties in the sense of multiple domains of control). Specific topics include the design, formal modelling, and simulation of cryptographic protocols; selection and characterization of biometric sensing with pre-processing, feature extraction, and classification; and identity federation (e.g. making our results usable by STORK [9], FutureID [10], and FastPass [16]). We will specifically build upon our recent results on biometric authentication [17, 18] and cryptographic protocols [19, 20, 21] and unify these approaches into a single, multi-party protocol.
- Area B ("Tracking") will focus on tracking individuals and continuous authentication, specifically modeling of physical movement, statistical tracking of discrete events to estimate confidence in current authentication states, and sensor fusion over multiple biometric sensing modalities. We have existing experience in campus-scale WiFi based tracking [22, 23] and will cooperate with colleagues on tracking in video networks [24].
- Area C ("Trust") will focus on establishing trust in sensors and agents. Next to novel work on secure coding and systems security, we will integrate TPMs for cryptographic chains of trust from hardware to application software (cf. [15]) and DAA for proving this cryptographically to third parties [6, 8]. A specific focus is on cross-platform compatibility, to enable execution of personal agents on embedded hardware as well as cloud infrastructure. This area will build upon our previous experience with embedded Linux-based network devices (Gibraltar firewall) and Android system security (in the JRC u'smile).
- Area D ("Network") will focus on globally scalable service discovery, in particular on the level of network protocols and distributed systems. The designed protocols will be prototyped and simulated concerning their scalability towards potential global use of a single standard. Research in this area will span a wide range of networking protocols, from hierarchically structured index servers (e.g. DNS) and decentralized indices (e.g. DHT) to higher-level communication protocols (e.g. PubSub patterns).

There are cross-cutting interdisciplinary aspects in all areas, including legal/legislative (privacy and security requirements), social (usability, trust of users in the whole system), and ethical (control of identity and interactions), and we will put our work in context of these aspects through regular exchange with experts outside our research group. JKU is particularly well suited to interdisciplinary exchange due to its integration of all major scientific disciplines in a single organization.

Specifically for the aspects of secure code in area C, the PI is in a globally unique position to make significant advances. In addition to INS, there are four other institutes in the same computer science building with complementary research areas, and based on an initiative by the PI, JKU has recently started a strategic focus area on "Secure Code". This is an excellent environment of scientific expertise for work on trustworthy code.

Concerning many aspects of creating and using digital ID, Austria has long experience with e-government in the form of the national citizen card (Bürgerkarte). Under the lead of the PI, the JRC u'smile is co-funded and supported by main stakeholders (Austrian state printing house, A1 Telekom Austria, Drei-Banken-EDV, NXP Semiconductors) and is the only consortium in Austria working on a digital driving license as legally acceptable, digital photo ID. The PI is therefore already in close cooperation with the required technology (smart cards, person registers) and use case partners (mobile network operator, banks) for evaluating and deploying prototypes of digital identity systems. We build upon this experience for the proposed paradigm change.

From a practical management perspective, the project will be run similarly to the currently successful JRC u'smile with 1–4 PhD or post-doc researchers working on each area, but relying on shared code repositories and regular exchange to discuss overall architectures and project goals. We will build one complete prototype each year, including the respective latest results from each of the areas. This will improve integration on the level of protocols and code, and will provide opportunity to communicate research outcome to a broader audience.

As PI, this ERC grant will enable me to consolidate current lines of research and significantly extend the practical impact of fundamental research in my group, giving us public visibility within and outside the EU.

References

[1] European Union, "Charter of the fundamental rights," *Official Journal of the European Communities*, no. 364/01, 2000. [Online]. Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[2] Italian Parliament, "Declaration of internet rights," July 2015. [Online]. Available: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf

[3] G. Greenwald, *No place to hide: Edward Snowden, the NSA & the surveillance state*. Penguin Books, 2014.

[4] M. Langheinrich, R. Finn, V. Coroama, and D. Wright, "Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight," in *Reloading Data Protection*. Springer, Jan. 2014, pp. 151–182.

[5] E. Brickell and J. Li, "Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities," in *Proc. 2007 ACM Workshop on Privacy in Electronic Society*, ser. WPES '07. ACM, 2007, pp. 21–30.

[6] T. Nyman, J.-E. Ekberg, and N. Asokan, "Citizen Electronic Identities using TPM 2.0," *arXiv:1409.1023 [cs]*, Sep. 2014, arXiv: 1409.1023. [Online]. Available: http://arxiv.org/abs/1409.1023

[7] K. Potzmader, J. Winter, D. Hein, C. Hanser, P. Teufl, and L. Chen, "Group Signatures on Mobile Devices: Practical Experiences," in *Trust and Trustworthy Computing*, ser. LNCS. Springer, Jun. 2013, no. 7904, pp. 47–64.

[8] L. Chen, D. Page, and N. P. Smart, "On the Design and Implementation of an Efficient DAA Scheme," in *Proc. 9th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Application*, ser. CARDIS'10. Springer, 2010, pp. 223–237.

[9] STORK Consortium, "Stork project." [Online]. Available: https://www.eid-stork.eu/

[10] FutureID Consortium, "FutureID project." [Online]. Available: http://futureid.eu/

[11] European Commission, "Electronic identification and trust services (eIDAS): regulatory environment and beyond." [Online]. Available: http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond

[12] B. Zwattendorfer and D. Slamanig, "The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality," *Journal of Information Security and Applications*, 2015.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[14] A. Tran, N. Hopper, and Y. Kim, "Hashing It out in Public: Common Failure Modes of DHT-based Anonymity Schemes," in *Proc. 8th ACM Workshop on Privacy in the Electronic Society*, ser. WPES '09. ACM, 2009, pp. 71–80.

[15] T. Winkler, A. Erdelyi, and B. Rinner, "TrustEYE.M4: Protecting the sensor – Not the camera," in *Proc. 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, Aug. 2014, pp. 159–164.

[16] FastPass Consortium, "FastPass - a harmonized, modular reference system for all European automated border crossing points." [Online]. Available: https://www.fastpass-project.eu/

[17] R. D. Findling and R. Mayrhofer, "Towards Pan Shot Face Unlock: Using Biometric Face Information from Different Perspectives to Unlock Mobile Devices," *International Journal of Pervasive Computing and Communications (IJPCC)*, vol. 9, p. 190–208, Aug. 2013.

[18] R. Mayrhofer and T. Kaiser, "Towards usable authentication on mobile phones: An evaluation of speaker and face recognition on off-the-shelf handsets," in *Proc. IWSSI/SPMU 2012: 4th International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, colocated with Pervasive 2012*, Jun. 2012.

[19] M. Hölzl, E. Asnake, R. Mayrhofer, and M. Roland, "A Password-authenticated Secure Channel for App to Java Card Applet Communication," *International Journal of Pervasive Computing and Communications (IJPCC)*, vol. 11, pp. 374–397, Oct. 2015.

[20] J. González, M. Hölzl, P. Riedl, P. Bonnet, and R. Mayrhofer, "A Practical Hardware-Assisted Approach to Customize Trusted Boot for Mobile Devices," in *Proc. 17th Information Security Conference (ISC 2014)*. Springer, Oct. 2014, pp. 542–554.

[21] R. Mayrhofer, J. Fuss, and I. Ion, "UACAP: A Unified Auxiliary Channel Authentication Protocol," *IEEE Transactions on Mobile Computing*, vol. 12, p. 710–721, Apr. 2013.

[22] H. Schmitzberger and W. Narzt, "Campus-Wide Indoor Tracking Infrastructure," *International Journal On Advances in Networks and Services*, vol. 4, no. 1 and 2, pp. 138–148, 2011.

[23] P. Riedl and R. Mayrhofer, "Towards a Practical, Scalable Self-Localization System for Android Phones Based on WLAN Fingerprinting," in *Proc. 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2012, pp. 98–101.

[24] T. Winkler and B. Rinner, "Security and Privacy Protection in Visual Sensor Networks: A Survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, pp. 1–42, 2014.

Section b: Curriculum Vitae

Personal information

René Mayrhofer, born 30.4.1979 in Graz, Austria, ORCID orcid.org/0000-0003-1566-4646
Web: https://ins.jku.at/staff/rene-mayrhofer, https://www.mayrhofer.eu.org (personal)

Current positions

- **Head of the Institute of Networks and Security (INS)** 2014 – now
  at Johannes Kepler University Linz (JKU), Austria
- **Head of the Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile)** 2012 – now
  at Campus Hagenberg, University of Applied Sciences Upper Austria, Austria

Previous positions

- **Professor for Mobile Computing**, University of Applied Sciences Upper Austria 2010 – 2014
- **Head of Research and Development**, eSYS GmbH, Attnang-Puchheim, Austria 2009 – 2010
  Main topics: server virtualization, server and network security
- **Guest Professor for Mobile Computing**, University of Vienna, Austria 2008 – 2009
- **Marie-Curie Intra-European Fellow**, Lancaster University, UK 2005 – 2008
  Advisor: *Prof. Dr. Hans Gellersen*
- **University Assistant**, Johannes Kepler University Linz, Austria 2002 – 2005
  Advisor: *Univ.-Prof. Dr. Alois Ferscha*

Education

- Habilitation (venia docendi) for Applied Computer Science, Vienna University, Austria Mar. 2009
  Thesis: *Ubiquitous Computing Security: Authenticating Spontaneous Interactions*
- Ph.D. (Dr.techn.) in Computer Science, **Promotio sub auspiciis Praesidentis rei publicae** Nov. 2005
  Johannes Kepler University Linz, Austria
  Thesis: *An Architecture for Context Prediction*, Advisor: *Univ.-Prof. Dr. Alois Ferscha*

Supervision of students

I am currently supervising 6 PhD students. Two of my former PhD students achieved important results:

- H. Schmitzberger (thesis: "Harnessing Wireless LAN Communication for Scalable Indoor Localization and Tracking", 2007–2012) — developed and quantitatively analyzed a WLAN tracking system that was installed throughout the campus of JKU Linz.
- M. Roland (thesis: "Security Issues in Mobile NFC Devices", 2009–2013) — his PhD thesis also appeared as a book in the Springer "T-Labs Series in Telecommunication Services" and the main result of the PhD thesis led to inclusion in the Google Security Hall of Fame.

Within the last 13 years I have been supervising 19 Master students. R. D. Findling (thesis: "Pan Shot Face Unlock: Towards Unlocking Personal Mobile Devices using Stereo Vision and Biometric Face Information from multiple Perspectives", 2011–2013) received the OCG Incentive Award 2015 and Fred Margulies Award 2015 for his Master's thesis and is currently one of my active PhD students.

Organization of scientific meetings

- 14th Int. conf. on Mobile and Ubiquitous Multimedia (MUM 2015), Linz Dec. 2015
  Role: General chair, 90 participants
- 1st Android Security Symposium, Vienna, Austria Sept. 2015
  Role: General chair, 160 participants
- 11th Int. conf. on Advances in Mobile Computing & Multimedia (MoMM 2013), Vienna Dec. 2013
  Role: Program committee chair, 100+ participants
- Series of workshops on mobile computing technologies (MCPT), Gran Canaria 2011 – 2015
- Series of workshops on authentication and privacy in mobile phones (IWSSI/SMPU) 2007 – 2012

Other academic services

- Editorial board member of MDPI *Computers* journal (ISSN 2073-431X)
- Guest editor for Springer *Personal and Ubiquitous Computing* (Theme Issue on Security and Trust in Personal and Ubiquitous Computing, 2012) and *Security and Networks* (IJSN) journals
- Reviewer for journals: Elsevier *Pervasive and Mobile Computing* (PMC), Elsevier *Information and Software Technology* (IST), Springer *Theory of Computing Systems* (TOCS), Springer *Information Security* (IJIS), IEEE *Transactions on Mobile Computing*, IEEE *Transactions on Vehicular Technology*, IEEE *Transactions on Automation Science and Engineering* (T-ASE), IEEE *Transactions on Parallel and Distributed Systems*, IEEE *Pervasive Computing*, IEEE *Internet of Things*, ACM *Transactions on information and System Security*, ACM *Computing Surveys* (CSUR), Wiley *Security and Communication Networks* (SCN), *Software - Practice & Experience*, *Mobile Computing and Multimedia Communications* (IJMcMc)
- Program committee member of *Ubicomp* 2016/2010/2008, *Pervasive* 2012–2010, *WiSec* 2016–2010, MuM 2013–2012, CCNC 2014–2009, BICT 2015, EUC 2013, *PerCom* 2012, ACSA 2012, iiWAS 2014–2007, MoMM 2015–2012, SecureComm 2012, SETOP 2012, UCAmI & IWAAL 2012, FTRA ACSA 2012, TAMoCo 2012, IoT 2014–2010, WCC-WTA 2011, ISWC 2010, CIOT 2010, MobileHCI 2009, Tamoco/Moteus 2009, MobiQuitous 2010–2009, LoCA 2009, IMUx2008, TwUC 2010/2009/2008, WoT 2010, TEI 2010–2007, AmI 2007, ICT 2007, EuroSSC 2007, ICPCA 2009–2007, IWSAWC 2007, PerTec 2007, PerSec 2007, UCI'07, SMP-07, UCS2006, IWSH06, Smart Home Session at ICHIT2006, SPCA'06, PervasiveHealth 2006

Teaching

Multiple courses at PhD, Master, and Bachelor level at Johannes Kepler University Linz (7), University of Applied Sciences Upper Austria (9), Vienna University (4), and Lancaster University, UK (2) with a focus on computer security and networking in addition to fundamental computer science courses.

Research interests and scientific profile

In my academic career, there are three distinct periods that need to be distinguished because of extending and complementing my research interests in between. During my PhD studies (completed in the minimal possible time of two years and with the highest possible distinction in Austria) I focused on machine learning and embedded systems. Insights from sensor data analysis and predictability that I have developed led to an idea to combine machine learning methods with cryptographic protocols. Thus I decided to apply for a Marie Curie Fellowship and joined the group of Prof. Hans Gellersen (Lancaster University, UK). There I initiated the "spontaneous security" research area. As guest professor at University of Vienna, I again extended my research focus to mobile security in general, which I continued during my appointment at University of Applied Sciences Upper Austria (Campus Hagenberg). I started a new research group on security in mobile computing with various funded project grants, resulting in 5 full-time researchers and 1 part-time administrative staff in 2014. The largest funded project is JRC u'smile, which I am still leading until the end of funding in September 2017. Appointment as head of the Institute of Networks and Security (INS) at Johannes Kepler University Linz (JKU) with 7 full-time and 2 part-time permanent staff members allowed me to (once more) extend my strategic research areas to digital identity and secure code.

Collaborations relevant to the project

Dr. Jan-Erik Ekberg
Trustonic, FI and UK
topics: ARM TrustZone access, digital ID

Dr. Edgar Weippl
SBA Research, AT
topics: app and service security

Dr. Mario Ivkovic
NXP Semiconductors, AT and BE
topics: smartcards, crypto hardware

Prof. Marc Langheinrich
University of Lugano (USI), CH
topics: privacy, mobile security

Prof. Hans Gellersen
Lancaster University, UK
topics: human computer interaction

Prof. Bernhard Rinner
University Klagenfurt, AT
topcs: video networks

Prof. Michael Mayrhofer
JKU Linz, Dept. of Technical Law
topics: Internet and identity law

Prof. Helmut Renöckl
JKU Linz
topics: ethics

Prof. Hanspeter Mössenböck
JKU Linz, Inst. of Systems Software
topics: secure code

Appendix:
All ongoing and submitted grants and funding of the PI (Funding ID)

Since the beginning of my academic career, I have been responsible for managing research project funds of over 2.1 Mio. EUR. I was primarily responsible for the acquisition (writing grant proposals and negotiating with project partners) of 1.7 Mio. EUR out of these total funds.

On-going Grants

Project Title	Funding source	Amount (Euros)	Period	Role of the PI	Relation to current ERC proposal
Josef Ressel Center *u'smile*	Christian Doppler Research Association (CDG)	1.430.000 €	2012–2017	Head of Center	JRC u'smile targets secure mobile devices for authentication and service use (incrementally improving current use cases technology), Digidow aims at a completely new leap by eliminating mobile devices for current and future use cases – significantly different technology will be required.
Connected Vehicles	European Regional Development Fund	794.000 €	2016–2019	Lead of one of four research areas	Connected vehicles studies car-to-car communication networks, and our research group is involved with securing these links. We may prove if some cryptographic protocols and tracking models might be useful for and have similar structure in Digidow.
JKU/UAS *Joint International PhD Program in Computer Science*	State of Upper Austria	306.000 €	2016–2018	Head of funded PhD program at JKU Linz, responsible for grant application and management	One out of three PhD students funded by this program will work on cryptographic protocols in a related area (secure backup of digital identities).
JKU/UAS *Joint International PhD Program in Computer Science*	University of Applied Sciences Upper Austria	250.000 €	2011–2016	Head of funded PhD program at University of Applied Sciences, responsible for management of funds	One out of two PhD students funded by this program is working on biometric authentication in a related but different scenario (mobile device authentication).

Section c: Early Achievements Track-Record

For project Digidow, broad knowledge of multiple computer science disciplines is required, and my experience in different areas and most relevant publications are therefore explicitly highlighted below. The citation counts mentioned for the following highlighted papers (in bold) were taken from Google Scholar on 2015-01-05, with a total (accumulated over the periods) of more than 1200 citations (h-index 16, i10-index 26). Publications (updates at https://www.mayrhofer.eu.org/publications) without my PhD supervisor are marked (★).

PhD period

During my PhD studies I have developed an architecture that was the first to combine context awareness with time series prediction to estimate future (device and user) contexts and was optimized to execute on mobile devices of that time. Rooted in ubiquitous computing, my main research focus was on **machine learning** (specifically feature extraction, unsupervised classification, and time series prediction) and **embedded systems**.

- ★ R. Mayrhofer, "An Architecture for Context Prediction", vol. C 45 of *Schriften der Johannes-Kepler-Universität Linz*, Trauner Verlag, April 2005 — revised version of PhD thesis (>**160** in total)
- R. Mayrhofer, H. Radi, and A. Ferscha, "Recognizing and predicting context by learning from user behavior", *Radiomatics: Journal of Communication Engineering*, vol. 1, pp. 30–42, May 2004 — extended version of conference paper at MoMM 2013, (ca. **100** in total)
- ★ R. Mayrhofer, "Context prediction based on context histories: Expected benefits, issues and current state-of-the-art", in Proc. *ECHISE 2005*: 1st International Workshop on Exploiting Context Histories in Smart Environments, May 2005, part *Pervasive 2005* (**57**)
- **Patents issued**: "System for the rapid adjustment of industrial processes" (co-authors M. Franz, M. dos Santos Rocha, E. Chtcherbina, A. Ferscha, M. Hechinger, R. Mayrhofer; WO/2006/079569, PCT/EP2006/050012) and "RFID tag-based file system and associated access methods" (co-authors M. dos Santos Rocha, A. Ferscha, M. Franz, M. Hechinger, R. Mayrhofer, A. Zeidler; WO/2007/065747, PCT/EP2006/067197)

Postdoc period

During an awarded Marie Curie Fellowship at Lancaster University (UK), I initiated the "spontaneous security" research, combining machine learning methods and **cryptographic protocols**, and started a corresponding workshop series (IWSSI/SPMU). Specific contributions from this period include my most-cited work on accelerometer based secure device pairing, ultrasound, and visible laser based authentication protocols.

- ★ R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices", IEEE *Transactions on Mobile Computing*, vol. 8, pp. 792–806, June 2009 — revised and extended version of conference paper "Shake well before use: Authentication based on accelerometer data" at *Pervasive 2007* (>**300** in total, **awarded best Pervasive 2007 paper**)
- ★ R. Mayrhofer, H. Gellersen, and M. Hazas, "Security by spatial reference: Using relative positioning to authenticate devices for spontaneous interaction", in Proc. *Ubicomp 2007*: 9th International Conference on Ubiquitous Computing, pp. 199–216, Springer-Verlag, September 2007 (**23**)
- ★ R. Mayrhofer, "The candidate key protocol for generating secret shared keys from similar sensor data streams", in Proc. *ESAS 2007*: 4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks, pp. 1–15, Springer-Verlag, July 2007 (**32**)
- ★ R. Mayrhofer and M. Welch, "A human-verifiable authentication protocol using visible laser light", in Proc. *ARES 2007*: 2nd International Conference on Availability, Reliability and Security, pp. 1143–1147, IEEE CS Press, April 2007 (**59**)

Professor period

During my time at University of Applied Sciences Upper Austria (Campus Hagenberg, 2010–2014), I started a new research group on **security in mobile computing**. The largest funded project is JRC u'smile, which has a strong focus on Android security and is on its way to develop the first mobile phone based digital driving license suitable as valid photo ID in Austria within 2016. In my current position as head of the Institute of Networks and Security (INS) at University Linz (JKU), strategic research areas are now **digital identity** and **secure code**. The selected journal articles present some of our latest achievements relevant to project Digidow.

- ★ P. Riedl, R. Mayrhofer, A. Möller, M. Kranz, F. Lettner, C. Holzmann, and M. Koelle, "Only play in your comfort zone: interaction methods for improving security awareness on mobile devices", Springer *Personal and Ubiquitous Computing*, pp. 1–14, March 2015
- ★ M. K. Chong, R. Mayrhofer, and H. Gellersen, "A survey of user interaction for spontaneous device association", ACM *Computing Surveys*, vol. 47, July 2014
- ★ R. Mayrhofer, "An architecture for secure mobile devices", Security and Communication Networks, 2014
- ★ R. Mayrhofer, J. Fuss, and I. Ion, "UACAP: A unified auxiliary channel authentication protocol", IEEE *Transactions on Mobile Computing*, vol. 12, pp. 710–721, April 2013
- ★ R. Findling and R. Mayrhofer, "Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices", *International Journal of Pervasive Computing and Communications*, vol. 9, pp. 190–208, 2013

Invited talks, lectures, and participations

I have given many technical talks at scientific conferences, academic institutions, congresses for policy stakeholders and interest organizations, as well as open source events. Some relevant invited talks are listed below:

- **Keynotes** at congresses "Banking Trends & Technologies" (Vienna, June 2012), "Security & Risk Management" (Waidhofen, May 2012), and KSÖ "Cyber-Security / Cyber-Crime" (Vienna, May 2011)
- **Lectures** at European Patent Office (on methods for spontaneous security, Munich, March 2009), BaCaTec Summer School (on pervasive computing security, Chiemsee, August 2007)
- Dagstuhl seminars 'Eyewear Computing – Augmenting the Human with Head-mounted Wearable Assistants" (January 2016) and "My Life, Shared - Trust and Privacy in the Age of Ubiquitous Experience Sharing" (July 2013)

Summary of academic awards

- **Best full papers**: *MoMM 2014* "ShakeUnlock: Securely unlock mobile devices by shaking them together" (D. Hintze, R. D. Findling, S. Scholz, R. Mayrhofer), *iiWAS 2014* "Optimal derotation of shared acceleration time series by determining relative spatial alignment" (R. Mayrhofer, H. Hlavacs, R. D. Findling), *Pervasive 2007* "Shake well before use: Authentication based on accelerometer data" (R. Mayrhofer, H. Gellersen)
- *iiWAS/MoMM 2007* **best workshops paper** "A context authentication proxy for IPSec using spatial reference" (R. Mayrhofer)
- *UbiComp/ISWC 2014* **programming competition winner** "Diversity in locked and unlocked mobile device usage" (D. Hintze, R. D. Findling, M. Muaaz, S. Scholz, R. Mayrhofer)
- **Researcher award** of the University of Applied Sciences Upper Austria 2012 (FH OÖ Forscherpreis)
- Marie-Curie Intra-European Fellowship (2006–2008 at Lancaster University)
- Promotion with highest possible distinction by the President of the Austrian republic (*Promotio sub auspiciis Praesidentis rei publicae*: grades average 1.0 for PhD, Master, and Bachelor studies and high school diploma, studies finished in minimum time)

Other Achievements

Started during my under-graduate studies and in parallel to my academic activities, from 2000 to 2012 I initiated, developed, and managed the project *Gibraltar Firewall* (archived at http://gibraltar.at) with the main advantage of the root file system being read-only and therefore significantly more difficult to subvert with simple malware/attacker toolkits. Starting in 2003, Gibraltar Firewall was successfully bundled with embedded hardware appliances and commercialized with the company eSYS GmbH with a stronger focus on UTM (unified threat management) functionality. In 2006, it was the first (and still the only commercial) firewall to include multiple anonymization proxies to support network privacy in addition to security. Until 2012, there were nearly 1000 hardware appliances in global use and a larger number of custom installations of the free version, including organizations like the University of Washington and larger customer networks managed by the German T-Systems. Managing Gibraltar Firewall equipped me with in-depth knowledge of **secure embedded systems design** (specifically on Linux), **networking protocols**, and developing and supporting code for stable in-production use.