Networks and Security

10 YEARS INS@JKU

INSTITUTE
OF NETWORKS
AND SECURITY

JOHANNES KEPLER
UNIVERSITY LINZ

Das Institut für **Netzwerke und Sicherheit (INS)**

Unsere Mission ist die Absicherung von Computersystemen und Kommunikation – im Spektrum von akademischer Forschung und Lehre zu praktischer Umsetzung in Projekten und von lokalen Anwendungen bis zum globalen Internet und kritischer Infrastruktur.

The Institute of **Networks and Security (INS)**

Our mission is to secure computer systems and communication – with a scope ranging from academic research and teaching to practical project implementation, and from local applications to the global Internet and critical infrastructure.

CONTENT

ÜBER UNS

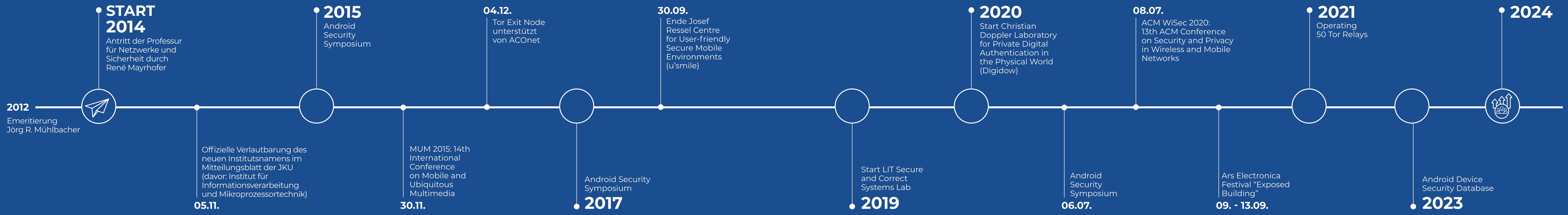
Wir streben danach, die Sicherheit und Netzwerkkonnektivität von Computersystemen sowohl in weltweiten als auch in lokalen Netzwerken durch Forschung, Bildung und spezifische Projektarbeit zu verbessern.

Neben der akademischen Forschung und Lehre sind wir der festen Überzeugung, dass es unsere gemeinsame Aufgabe ist, die praktische Sicherheit alltäglicher Computersysteme und -infrastrukturen zu verbessern, auf die unsere gegenwärtige Gesellschaft in zunehmendem Maße angewiesen ist.
Computernetze und Sicherheit sind schnell bewegende Ziele. Forschung und Lehre am Institut für Netzwerke und Sicherheit umfasst daher das gesamte Spektrum von theoretischen bis hin zu sehr praktischen Fragestellungen

ABOUT US

We strive to improve security and network connectivity of computer systems both in world-wide and in local networks through research, education, and specific project work.

In addition to academic research and teaching, we firmly believe that it is our shared responsibility to improve the practical security of everyday computer systems and infrastructure that our current society is increasingly dependent upon.
Computer networks and security are fast-moving targets. Research and teaching at the Institute of Networks and Security therefore includes the full range from theoretical to highly practical issues.



2012 Emeritierung Jörg R. Mühlbacher

START 2014 Antritt der Professur für Netzwerke und Sicherheit durch René Mayrhofer

05.11. Offizielle Verlautbarung des neuen Institutsnamens im Mitteilungsblatt der JKU (davor: Institut für Informationsverarbeitung und Mikroprozessortechnik)

2015 Android Security Symposium

30.11. MUM 2015: 14th International Conference on Mobile and Ubiquitous Multimedia

04.12. Tor Exit Node unterstützt von ACOnet

2017 Android Security Symposium

30.09. Ende Josef Ressel Centre for User-friendly Secure Mobile Environments (u'smile)

2019 Start LIT Secure and Correct Systems Lab

2020 Start Christian Doppler Laboratory for Private Digital Authentication in the Physical World (Digidow)

06.07. Android Security Symposium

08.07. ACM WiSec 2020: 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks

09. - 13.09. Ars Electronica Festival "Exposed Building"

2021 Operating 50 Tor Relays

2023 Android Device Security Database

2024

KEY FIGURES

19 Mitarbeiter:innen
(Voll- oder Teilzeit)

3+
Mio EUR
akquirierte
Mittel bisher

22 Kooperationspartner

8 Konferenzen
organisierte internationale

174 Publikationen

4
Keynote
presentations

1,2 PB
transportierter Tor Traffic

42 Masterarbeiten
abgeschlossene

9 Dissertationen
abgeschlossene

22	reguläre Lehrveranstaltungen
20	spezielle Lehrveranstaltungen

5
CVEs

9,5 KM Ethernet-Kabel (3,5km im Labor) und **~5,8 KM** Glasfaser-Kabel

TEAM

Das Institut lebt alleine durch sein großartiges Team und die Erfolge entstehen nur durch die Zusammenarbeit. Wir sind zutiefst dankbar für das Engagement und die Initiative aller Mitarbeiter:innen.

The institute really is the amazing people contributing to its success and all results are a team effort. We are deeply thankful for all their dedication and initiative.

At the beginning . . .

Mission Statement

We work in three areas of advancing the state-of-the-art:

- In research, we look at the full spectrum between **fundamental research** issues (with a horizon of up to 20 years until practical applicability) and **applied research** (with time-to-market of 1-2 years) and act as a bridge between academic research results and their practical applicability in industry-driven projects.
- In teaching, we interpret and organize textbook knowledge and new research results primarily in the form of courses for university students, including significant parts of the Master curriculum with the **Major in Networks and Security**. Additionally, we offer special courses on secure coding practices and cryptography to companies and other organizations on request.
- As a publicly funded institute, we offer free community services in the form of documentation and open-source software **for the general public**.

Code of Ethics

In our research, we are regularly dealing with technologies and techniques that could potentially be misused to cause harm in all sorts of ways. We also demonstrate the application of those techniques and the necessary tools in class, in order to raise awareness and prepare our students for situations where they might be affected by said misuse. The team is committed to the ethical use of potentially harmful knowledge and technology and follows the codes of ethics of the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM). Additionally, we do not support any offensive use of physical force or other forms of abusive power against people or societies, weapons development, warfare, unwarranted mass surveillance, or other politically driven negative action against minorities.

HEAD

UNIV-PROF. PRIV.-DOZ. DI DR.

RENÉ MAYRHOFER

Institutsvorstand / Head of Institute
Head of Christian Doppler Laboratory for Private Digital Authentication in the Physical World (CDL Digidow)
Head of LIT Secure and Correct Systems Lab (LIT SCL)

Research Topics:

Digital Identity, Mobile and OS Security, Wide Area Networking, Network Privacy, Machine Learning based Authentication, Applied Cryptography, Software Supply Chain Security

01.09.2014

01.10.1997
Univ. Assistant

01.10.2010
Assoc. Prof.

ASSOC.PROF. MAG. DI DR.

MICHAEL SONNTAG

Stellvertretender Institutsvorstand / Vice Head of Institute

Research Topics:

Privacy, Web Security, Computer Forensics and IT Law

EM.O.UNIV.-PROF. DR.

JÖRG R. MÜHLBACHER

Ehemaliger Institutsvorstand für Informationsverarbeitung und Mikroprozessortechnik
Ehrenmitglied der Österreichischen Computergesellschaft (OCG)
Österreichischer Informatikpionier

1976-2012

2021

UNIV.-PROF. DI DI DR.

STEFAN RASS

Stellvertretender Institutsvorstand / Vice Head of Institute
Head of Secure Systems Group
Head of LIT Secure and Correct Systems Lab (LIT SCL)

Research Topics:

Decision Theory and Game-Theory, Robotics Security, Security of Artificial Intelligence, Complexity Theory, Cryptography, Data Science for Security

SENIOR LECTURER / SCIENTIST

2015
Externally funded researcher

2018
Univ. Assistant

DR.
MICHAEL ROLAND

Research Topics:
Digital Identity, Smart Cards & NFC, Mobile Security, Network Security and Privacy

SCIENTIFIC STAFF

2018

DR.
TOBIAS HÖLLER

2020

MARTIN SCHWAIGHOFER

2020

PHILIPP HOFER

2021

GERALD SCHOIBER

2021

ERNST LEIERZOPF

SCIENTIFIC STAFF

2022

GOODLET KUSI

2023

CINTIA MAYA BODI

CURRENT UNIV. ASSISTANTS

2021

DR.
JAN HORACEK

Research Topics:
Network Security, Side-channel Attacks

2021

MARIO LINS

Research Topics:
Supply Chain Security, Threat Modeling, System and Mobile Security

2022

STEFAN KEMPINGER

Research Topics:
Usable Security, Usable Privacy

FORMER UNIV. ASSISTANTS

1985-2023

DR.
RUDOLF HÖRMANSEDER

2011-2015

DR.
FLORIAN KÖNIG

2014-2018

DR.
MICHAEL HÖLZL

2015-2016

DR.
HEINRICH SCHMITZBERGER

2016-2019

DR.
BINH NGUYEN

2018

DR.
MUHAMMAD MUAAZ

ADMINISTRATION

1986

FRANZ BAUER

Techniker

2001

SABINE LINK

LVA-Administration, Forschungsdokumentation, Webredaktion

2014

SEVERINA KEHAYOVA

Institutsreferentin Administration, Projekte

2020

MAXIMILLIAN KOKALJ

Institutsreferent

FORMER TEAM MEMBERS

OSAMAH GHALEB ALI AL-GHAMMARI

HAMIDEH AYATI

MICHAEL BARTH

FELIX DIETZ

RAINHARD FINDLING

ROBERT HOLZINGER

MURAD HUSEYNZADE

GEORGIOS KANAKIS

JOEL KLIMONT

MICHAEL MAIRINGER

OMID MIR

PATRICK NOLTE

MANUEL PÖLL

MICHAEL PREISACH

THOMAS RAAB

STEPHANIE STEININGER

MARKUS VOGL

IRIS WALCHSHOFER

EXTERNAL LECTURERS

STEFAN BAUMGARTNER, MSC.
(DYNATRACE, AT)

GEORG BEHAM
(PWC ÖSTERREICH, AT)

DR. PETER DIETMÜLLER
(IT-CONSULTANT, AT)

DR. DANIEL DORFMEISTER
(FH HAGENBERG, AT)

FELIX EBERSTALLER, MSC.
(LIMES SECURITY, AT)

DR. GERHARD ESCHELBECK
(US)

RENÉ FREINGRUBER
(SEC-CONSULTANT, AT)

EXTERNAL LECTURERS

PROF. MICHAEL FUCHS
(KATHOLISCHE UNIVERSITÄT LINZ, AT)

DR. PAUL KNOLL
(IT-CONSULTANT, IT)

DR. LUDEK NOVAK
(IT SECURITY AND RISK MANAGEMENT CONSULTANT, CZ)

PROF. GERALD OSTERMAYER
(FH HAGENBERG, AT)

PETER PANHOLZER, MSC.
(LIMES SECURITY, AT)

DR. CHRISTIAN PRAHER-KÖPPL
(DYNATRACE, AT)

DR. HELMUT RENÖCKL
(KATHOLISCHE UNIVERSITÄT LINZ, AT; UNIVERSITÄT BUDWEIS, CZ)

PROF. EDGAR WEIPPL
(UNIVERSITÄT WIEN, AT)

EXTERNAL PHD SUPERVISORS

PROF. N. ASOKAN
(UNIVERSITY OF WATERLOO, CA)

PROF. ALASTAIR BERESFORD
(CAMBRIDGE UNIVERSITY, UK)

PROF. LOTHAR FICKERT
(TU GRAZ, AT)

PROF. KRISTOF VAN LAERHOVEN
(UNIVERSITÄT SIEGEN, DE)

PROF. GERALD QUIRCHMAYR
(UNIVERSITÄT WIEN, AT)

PROF. STEPHAN SIGG
(AALTO UNIVERSITY, FI)

PROF. VANESSA TEAGUE
(AUSTRALIAN NATIONAL UNIVERSITY, AU)

TEACHING / THESIS SUPERVISION FOR EXTERNAL UNIVERSITIES

AAALTO UNIVERSITY (FI)

EÖTVÖS LORÁND UNIVERSITY BUDAPEST (HU)

FH JOANNEUM KAPFENBERG / UNIVERSITY OF APPLIED SCIENCES JOANNEUM KAPFENBERG (AT)

FH OÖ HAGENBERG / UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA AT HAGENBERG (AT)

JÁNOS SELYE UNIVERSITY KOMÁRNO (SK)

OXFORD UNIVERSITY (UK)

ÖSTERREICHISCHE AKADEMIE DER VERWALTUNGSGERICHTSBARKEIT (AT)

SORBONNE UNIVERSITÉ (FR)

STANFORD UNIVERSITY (US)

TECHNICAL UNIVERSITY KOSICE (SK)

TU DARMSTADT (DE)

TU WIEN (AT)

UNIVERSITY OF BAMENDA (CM)

UNIVERSITY OF BIRMINGHAM (UK)

UNIVERSITY GRAZ (AT)

WIRTSCHAFTSUNIVERSITÄT PRAG (CZ)

PUBLICATION HIGHLIGHTS

01 **Practical Delegatable Anonymous Credentials From Equivalence Class Signatures**

in Proceedings on Privacy Enhancing Technologies (PoPETs) 2023(3), pp. 488-513, 2023

Mir O., Slamanig D., Bauer B., Mayrhofer R.

02 **Adversary Models for Mobile Device Authentication**

in ACM Computing Surveys 54(9), pp. 198:1-35, 2022

Mayrhofer R., Sigg S.

03 **Digitale Identitäten in der physischen Welt: Eine Abwägung von Privatsphäreschutz und Praktikabilität**

in HMD Praxis der Wirtschaftsinformatik 60(2), Springer Fachmedien Wiesbaden, pp. 283-307, 2023

Roland M., Höller T., Mayrhofer R.

04 **Supervised Machine Learning with Plausible Deniability**

Computers & Security 112, pp. 102506:1-20, 2022

Rass S., König S., Wachter J., Egger M., Hobisch M.

05 **Disposable Dynamic Accumulators: Toward Practical Privacy-Preserving Mobile eIDs with Scalable Revocation**

in International Journal of Information Security 19, Springer, pp. 401-417, 2020

Hölzl M., Roland M., Mir O., Mayrhofer R.

06 **Traffic Statistics of a High-Bandwidth Tor Exit Node**

in Proceedings of 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017), Porto, Portugal, SciTePress, pp. 270-277, 2017

Sonntag M., Mayrhofer R.

07 **The Android Platform Security Model**

in ACM Transactions on Privacy and Security 24(3), pp. 19:1-35, 2021

Mayrhofer R., Stoep J. V., Brubacker C., Kralevich N.

08 **Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics**

in IEEE Transactions on Mobile Computing 17(11), pp. 2578-2590, 2018

Findling R. D., Hölzl M., Mayrhofer R.

09 **Smartphone-Based Gait Recognition: From Authentication to Imitation**

in IEEE Transactions on Mobile Computing 16(11), 2017

Muaaz M., Mayrhofer R.

10 **Kriterien zur Beurteilung der Beweiskraft von Daten**

in International Trends in Legal Informatics - Festschrift Erich Schweighofer, Jusletter IT, pp. 171-199, 2020

Sonntag M.

11 **A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics**

in Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1(2), pp. 13:1-21, 2017

Hintze D., Findling R. D., Hintze P., Mayrhofer R.

PUBLICATIONS

2014

Chong M., Mayrhofer R., Gellersen H.:
A Survey of User Interaction for Spontaneous Device Association, in ACM Computing Surveys 47(1), pp. 8:1-40, 2014

Findling R. D., Muaaz M., Hintze D., Mayrhofer R.: ShakeUnlock: Securely Unlock Mobile Devices by Shaking them Together, in MoMM 2014: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, Kaohsiung, Taiwan, ACM, pp. 165-174, 2014

Hintze D., Findling R. D., Muaaz M., Scholz S., Mayrhofer R.:
Diversity in Locked and Unlocked Mobile Device Usage, in Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp 2014), Seattle, WA, USA, ACM, pp. 379-384, 2014

Hintze D., Findling R. D., Scholz S., Mayrhofer R.:
Mobile Device Usage Characteristics: The Effect of Context and Form Factor on Locked and Unlocked Usage, in MoMM 2014: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, Kaohsiung, Taiwan, ACM, pp. 105-114, 2014

Hölzl M., Asnake E., Mayrhofer R., Roland M.:
Mobile Application to Java Card Applet Communication using a Password-authenticated Secure Channel, in MoMM 2014: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, Kaohsiung, Taiwan, ACM, pp. 147-156, 2014

Hörmanseder R., Jäger M.:
Cloud Security Problems Caused By Virtualization Technology Vulnerabilities And Their Prevention, in Doucek P. et al. (Eds): IDIMT-2014 Networking Societies - Cooperation and Conflict, Schriftenreihe Informatik 43, Trauner Verlag, Linz, pp. 373-383, 2014

Mayrhofer R., Hlavacs H.:
Optimal Derotation of Shared Acceleration Time Series by Determining Relative Spatial Alignment, in iiWAS 2014: Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services, Kaohsiung, Taiwan, ACM, pp. 71-78, 2014

Muaaz M., Mayrhofer R.:
Orientation Independent Cell Phone Based Gait Authentication, in MoMM 2014: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, Kaohsiung, Taiwan, ACM, pp. 161-164, 2014

Sonntag M.:
Cheats aus rechtlicher Sicht, in Tagungsband IRIS 2014, Jusletter IT, pp. 683-692, 2014

Sonntag M.:
Cloud Computing: Risks and Chances, in Doucek P. et al. (Eds): IDIMT-2014. Networking Societies - Cooperation and Conflict, Schriftenreihe Informatik 43, Trauner Verlag, Linz, pp. 355-364, 2014

Sonntag M.:
Die EU-Richtlinie über Angriffe auf Informationssysteme, in jusIT 1/2014, Lexis-Nexis, Article 2, pp. 8-14, 2014

Sonntag M.:
Die Technizität von Programmlogiken im Gebrauchsmusterschutz, in jusIT 4/2014, Lexis-Nexis, Article 58, pp. 129-133, 2014

Sonntag M.:
Einführung in das Internetrecht, Linde, Wien, 2014

Sonntag M.:
Multimediawerke und der Rechtsschutz technischer Schutzmaßnahmen im Urheberrecht, in jusIT 2/2014, Lexis-Nexis, Article 20, pp. 41-45, 2014

Sonntag M.:
OGH 4 Ob 5/14k: Rechtzeitigkeit des Rücktritts bei baldigem Leistungsbeginn, in jusIT 4/2014, Lexis-Nexis, Article 62, pp. 128-129, 2014

Sonntag M.:
OGH 6 Ob 58/14v: Zum Auskunftsanspruch nach § 18 Abs 4 ECG bei dynamischen IP-Adressen, in jusIT 6/2014, Lexis-Nexis, Article 102, p. 217, 2014

Sonntag M., Schaitl J.:
Das individuelle Gesetzbuch - Open Government Data aus dem RIS, in Schweighofer E. et al. (Eds): Zeichen und Zauber des Rechts. Festschrift für Friedrich Lachmayer, Editions Weblaw, Bern, pp. 403-426, 2014

2015

Findling R. D., Mayrhofer R.:
Towards Device-to-User Authentication: Protecting Against Phishing Hardware by Ensuring Mobile Device Authenticity using Vibration Patterns, in MUM '15: Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia, Linz, Austria, ACM, pp. 131-136, 2015

Hintze D., Findling R. D., Muaaz M., Koch E., Mayrhofer R.:
Cormorant: Towards Continuous Risk-aware Multi-modal Cross-device Authentication, in UbiComp/ISWC'15 Adjunct: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka, Japan, ACM, pp. 169-172, 2015

Hintze D., Muaaz M., Findling R. D., Scholz S., Koch E., Mayrhofer R.:
Confidence and Risk Estimation Plugins for Multi-Modal Authentication on Mobile Devices using CORMORANT, MoMM 2015: Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia, Brussels, Belgium, ACM, pp. 384-388, 2015

Hölzl M., Asnake E., Mayrhofer R., Roland M.:
A Password-authenticated Secure Channel for App to Java Card Applet Communication, in International Journal of Pervasive Computing and Communications 11(4), pp. 374-397, 2015

Hölzl M., Neumeier R., Ostermayer G.:
Localization in an Industrial Environment: A Case Study on the Difficulties for Positioning in a Harsh Environment, in International Journal of Distributed Sensor Networks 11(8), 2015

Holzmann C., Mayrhofer R., Häkkilä J., Rukzio E., Roland M. (Eds.):
Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia (MUM '15), Linz, Austria, ACM, 2015

Hörmanseder R.:
Computernetzwerke, 2. Auflage, Schriftenreihe Informatik 34, Trauner Verlag, Linz, 2015

Mayrhofer R.:
An Architecture for Secure Mobile Devices, in Security and Communication Networks 2015(8), Wiley, pp. 1958-1970, 2015

Mayrhofer R., Hlavacs H., Findling R. D.:
Optimal derotation of shared acceleration time series by determining relative spatial alignment, in International Journal of Pervasive Computing and Communications 11(4), pp. 454-466, 2015

Muaaz M., Mayrhofer R.:
Cross Pocket Gait Authentication using Mobile Phone Based Accelerometer Sensor, Computer Aided Systems Theory – EUROCAST 2015, Las Palmas de Gran Canaria, Spain, LNCS 9520, Springer, pp. 731-738, 2015

Riedl P., Mayrhofer R., Möller A., Kranz M., Lettner F., Holzmann C., Koelle M.:
Only play in your comfort zone: interaction methods for improving security awareness on mobile devices, in Personal and Ubiquitous Computing 19, Springer, pp. 941-954, 2015

Roland M., Hölzl M.:
Evaluation of Contactless Smartcard Antennas, Computing Research Repository, arXiv:1507.06427 [cs.CR], 2015

Sonntag M.:
Die e-Identifizierungs- und Vertrauensdienste-Verordnung der EU - Teil I, in jusIT 1/2015, Lexis-Nexis, Article 2, pp. 3-8, 2015

Sonntag M.:
Die e-Identifizierungs- und Vertrauensdienste-Verordnung der EU - Teil II, in jusIT 2/2015, Lexis-Nexis, Article 17, pp. 45-50, 2015

PUBLICATIONS

2015

Sonntag M.:
Rechtsfragen im Zusammenhang mit dem Betrieb eines Anonymisierungsdienstes, in jusIT 6/2015, Lexis-Nexis, Article 89, pp. 215-222, 2015

Sonntag M.:
Smart-Home Security, in Doucek P. et al (Eds): IDIMT-2015 Information Technology and Society, Schriftenreihe Informatik 44, Trauner Verlag, Linz, pp. 401-412, 2015

Sonntag M.:
Zum Verbot von Produktempfehlungen per E-Mail, in Tagungsband IRIS 2015, Jusletter IT, pp. 623-630, 2015

2016

Aichhorn A., Krammer H., Kern T. , Mayrhofer R.:
IP-based Communications for Line Current Differential Protection, in pac world 036 (June 2016), pp. 18-25, 2016

Aichhorn A., Mayrhofer R., Krammer H., Kern T.:
Realization of Line Current Differential Protection over IP-based networks using IEEE 1588 for synchronous sampling, in 13th International Conference on Development in Power System Protection 2016 (DPSP), Edinburgh, UK, IET, 2016

Baader F., Nguyen T. B., Borgwardt S., Morawska B.:
Deciding Unifiability and Computing Local Unifiers in the Description Logic EL without Top Constructor, in Notre Dame Journal of Formal Logic 57(4), Duke University Press, pp. 443-476, 2016

Findling R. D., Hölzl M., Mayrhofer R.:
Mobile Gait Match-on-Card Authentication from Acceleration Data with Offline-Simplified Models, in MoMM 2016: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multimedia, Singapore, ACM, pp. 250-260, 2016

Hintze D., Rice A.:
Picky: Efficient and Reproducible Sharing of Large Datasets using Merkle-Trees, in 2016 IEEE 24rd International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), London, UK, IEEE, pp. 30-38, 2016

Hintze D., Scholz S., Koch E., Mayrhofer R.:
Location-based Risk Assessment for Mobile Authentication, in UbiComp'16: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, ACM, pp. 85-88, 2016

Hölzl M., Roland M., Mayrhofer R.:
Real-World Identification: Towards a Privacy-Aware Mobile eID for Physical and Offline Verification, in MoMM 2016: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multimedia, Singapore, ACM, pp. 280-283, 2016

Muaaz M., Mayrhofer R.:
Accelerometer based Gait Recognition using Adapted Gaussian Mixture Models, in MoMM 2016: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multimedia, Singapore, ACM, pp. 288-291, 2016

Praher C., Sonntag M.:
Applicability of keystroke dynamics as a biometric security feature for mobile touchscreen devices with virtualised keyboards, in International Journal of Information and Computer Security 8(1), pp. 72-91, 2016

Roland M.:
Executing Arbitrary Code in the Context of the Smartcard System Service, Computing Research Repository, arXiv:1601.05833 [cs.CR], 2016

Roland M., Hölzl M.:
Open Mobile API: Accessing the UICC on Android Devices, Computing Research Repository, arXiv:1601.03027 [cs.CR], 2016

Schoiber G., Mayrhofer R., Hölzl M.:
DAMN - A Debugging and Manipulation Tool for Android Applications, in MoMM 2016: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multimedia, Singapore, ACM, pp. 40-44, 2016

Sonntag M.:
Anonymisierung: Methoden und Zulässigkeit, in Tagungsband IRIS 2016, Jusletter IT, pp. 465-474, 2016

Sonntag M.:
Cyber Security, in Doucek P. et al. (Eds): IDIMT-2016 Information Technology, Society and Economy, Schriftenreihe Informatik 45, Trauner Verlag, Linz, pp. 313-323, 2016

Sonntag M.:
Keine Bearbeitung des Datenbank-Programms durch einen Datenbank-Link, in jusIT 6/2017, Lexis-Nexis, Article 88, pp. 214-218, 2017

Sonntag M.:
OGH 4 Ob 142/15h: Zur Schutzfähigkeit von Schriftarten, in jusIT 3/2016, Lexis-Nexis, Article 47, pp. 102-104, 2016

Sonntag M.:
Third Person Data, in Kronmann L. and Zingerle A. (Eds): Behind the Smart World, servus.at, Linz, pp. 102-120, 2016

2017

Aichhorn A., Etzlinger B., Hutterer S., Mayrhofer R.:
Secure communication interface for line current differential protection over Ethernet-based networks: 2017 IEEE Manchester PowerTech, Manchester, UK, IEEE, pp. 1-6, 2017

Aichhorn A., Etzlinger B., Mayrhofer R., Springer A.:
Accurate clock synchronization for power systems protection devices over packet switched networks, in Computer Science – Research and Development 32, Springer, pp. 147-158, 2017

Carvalho Ota F. K., Hölzl M., Roland M., Mayrhofer R., Manacero A.:
Protecting Touch: Authenticated App-To-Server Channels for Mobile Devices Using NFC Tags, in Information 8(3), pp. 81:1-18, 2017

Findling R. D., Muaaz M., Hintze D., Mayrhofer R.:
ShakeUnlock: Securely Transfer Authentication States Between Mobile Devices, in IEEE Transactions on Mobile Computing 16(4), pp. 1163-1175, 2017

Hintze D., Findling R. D., Hintze P., Mayrhofer R.:
A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics, in Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1(2), pp. 13:1-21, 2017

Hölzl M., Roland M., Mayrhofer R.:
An Extensible and Privacy-preserving Mobile eID System for Real-world Identification and Offline Verification, in IFIP Summer School 2017: Privacy and Identity Management – the Smart World Revolution (Extended Abstracts), Ispra, Italy, 2017

Hölzl M., Roland M., Mayrhofer R.:
Extensibility in a Privacy-preserving eID: Towards a Mobile eID System for Real-world Identification and Offline Verification, in IFIP Summer School 2017: Privacy and Identity Management – the Smart World Revolution (Pre-proceedings), Ispra, Italy, pp. 19:1-16, 2017

Mayrhofer R.:
Security for Medical Data and Processes, in Hagelauer R. and Pomberger G. (Eds): Whitebook Medical Technology, pp. 56-57, 2017

Mayrhofer R., Reisner H., Haidinger A.:
Cybercrime: Darknet, in MEPA-Fachjournal 2017(1), MEPA – Mitteleuropäische Polizeiakademie, pp. 41-46, 2017

Muaaz M., Mayrhofer R.:
Smartphone-Based Gait Recognition: From Authentication to Imitation, in IEEE Transactions on Mobile Computing 16(11), 2017

Sonntag M.:
Die "Neuheit" einer Öffentlichkeit im Urheberrecht - Zugleich Anmerkung zu OGH 4 Ob 249/15v, in Tagungsband IRIS 2017, Jusletter IT, pp. 613-620, 2017

Sonntag M.:
OGH 4 Ob 84/17g: Ein Datenbank-Link ist keine Bearbeitung des Datenbank-Computerprogramms, in jusIT 6/2017, Lexis-Nexis, Article 94, 2017

Sonntag M.:
Privacy and Security - Friends or Enemies?, in Doucek P. et al. (Eds): IDIMT-2017 Digitalization in Management, Society and Economy, Schriftenreihe Informatik 46, Trauner Verlag, Linz, pp. 271-280, 2017

Sonntag M.:
Zur Technizität von Software-Patenten, insb. Ansprüchen auf Datenstrukturen, in jusIT 2/2017, Lexis-Nexis, Article 22, pp. 45-49, 2017

Sonntag M., Mayrhofer R.:
Traffic Statistics of a High-Bandwidth Tor Exit Node, in Proceedings of 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017), Porto, Portugal, SciTePress, pp. 270-277, 2017

2018

Aichhorn A., Etzlinger B., Unterweger A., Mayrhofer R., Springer A.:
Design, implementation, and evaluation of secure communication for line current differential protection systems over packet switched networks, in International Journal of Critical Infrastructure Protection 23, Elsevier, pp. 68-78, 2018

Aichhorn A., Unterweger A., Mayrhofer R., Engel D.:
Investigating the impact of network security on the line current differential protection system, in The Journal of Engineering 2018(15), IET, pp. 1199-1203, 2018

Findling R. D., Hölzl M., Mayrhofer R.:
Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics, in IEEE Transactions on Mobile Computing 17(11), pp. 2578-2590, 2018

PUBLICATIONS

2018

Hölzl M., Roland M., Mayrhofer R.:
Real-world Identification for an Extensible and Privacy-preserving Mobile eID, in Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017, Ispra, Italy, IFIP AICT 526, Springer, pp. 354-370, 2018

Hölzl M., Roland M., Mir O., Mayrhofer R.:
Bridging the Gap in Privacy-Preserving Revocation: Practical and Scalable Revocation of Mobile eIDs, in SAC'18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, ACM, pp. 1601-1609, 2018

Irshad A., Naqvi H., Chaudhry S. A., Hashmi M., Shafiq M., Mir O., Kanwal A.:
Cryptanalysis and improvement of a Multi-Server Authenticated Key Agreement by Chen and Lee's Scheme, in Information Technology and Control 47(3), pp. 431-446, 2018

Irshad A., Naqvi H., Chaudhry S. A., Hashmi M., Shafiq M., Mir O., Kanwal A.:
Cryptanalysis and improvement of a Multi-Server Authenticated Key Agreement by Chen and Lee's Scheme, in Information Technology and Control 47(3), pp. 431-446, 2018

Mir O., Mayrhofer R., Hölzl M., Nguyen B.:
Recovery of Encrypted Mobile Device Backups from Partially Trusted Cloud Servers, in ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, ACM, pp. 38:1-10, 2018

Nguyen B. T., Sprenger C., Cremers C.:
Abstractions for security protocol verification, in Journal of Computer Security 26(4), IOS Press, pp. 459-508, 2018

Rigger M., Mayrhofer R., Schatz R., Grimmer M., Mössenböck H.:
Introspection for C and its Applications to Library Robustness, The Art, Science, and Engineering of Programming 2(2), Article 4, 31 pages, 2018

Rigger M., Schatz R., Mayrhofer R., Grimmer M., Mössenböck H.:
Sulong, and Thanks For All the Bugs: Finding Errors in C Programs by Abstracting from the Native Execution Model, in APLOS '18: Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems, Williamsburg, VA, USA, ACM, pp. 377-391, 2018

Sonntag M.:
Black-Box-Testing von Software abgeschafft? Eine Anmerkung zu BGH 6. Oktober 2016, I ZR 25/15 [World of Warcraft I], in Tagungsband IRIS 2018, Jusletter IT, pp. 569-574, 2018

Sonntag M.:
DNS Traffic of a Tor Exit Node - An Analysis, in Wang G. et al. (Eds): Security, Privacy and Anonymity in Computation, Communication and Storage, Melbourne, NSW, Australia, LNCS 11342, Springer, pp. 33-45, 2018

Sonntag M.:
Ein Tor Exit-Knoten in Österreich - geht das?, in ACOnet Jahresbericht 2017, Universität Wien, pp. 53-55, 2018

Sonntag M.:
Pseudonymizing Log Entries with time-selective Disclosure, in Czarnecki C. et al. (Eds): Workshops der INFORMATIK 2018 - Architekturen, Prozesse, Sicherheit und Nachhaltigkeit, GI-Edition Lecture Notes in Informatics P285, pp. 119-127, 2018

Sonntag M.:
Technische Grenzen der Anonymisierung, in jusIT 4/2018, Lexis-Nexis, Article 54, pp. 137-143, 2018

Sonntag M.:
Ubiquitous Security Needs Ubiquitous Evidence, in Doucek P. et al. (Eds): IDIMT-2018. Strategic Modeling in Management, Economy and Society, Schriftenreihe Informatik 47, Trauner Verlag, Linz, pp. 333-341, 2018

Sonntag M., Hofstätter M.:
Durchblick - Combining Sensor Outputs and Supporting Forensic Investigations in Robot-Assisted Analysis of Suspicious Objects, in ERCIM News 113, pp. 51-52, 2018

2019

Alloulah M., Radivojevic Z., Mayrhofer R., Huang H.:
KinPhy: A kinetic in-band channel for millimetre-wave networks, in SenSys '19 Proceedings of the 17th Conference on Embedded Networked Sensor Systems, New York, NY, USA, ACM, pp. 364-377, 2019

Höller T.:
Towards establishing the link between a person's real-world interactions and their decentralized, self-managed digital identity in the Digidow architecture, in Doucek P. et al. (Eds): IDIMT-2019. Innovation and Transformation in a Digital World, Schriftenreihe Informatik 48, Trauner Verlag, Linz, pp. 327-332, 2019

Sonntag M.:
Das Netz- und Informationssystemsicherheitsgesetz, in jusIT 2/2019, Lexis-Nexis, Article 17, pp. 43-49, 2019

Sonntag M.:
Der Nachweis von Urheberrechtsverletzungen in Computerprogrammen, Tagungsband IRIS 2019, Jusletter IT, pp. 607-622, 2019

Sonntag M.:
Malicious DNS Traffic in Tor: Analysis and Countermeasures, Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), Prague, Czech Republic, SciTePress, pp. 536-543, 2019

Sonntag M.:
Missbräuchliche Nutzung des Tor-Netzwerks, in ACOnet Jahresbericht 2018, Universität Wien, pp. 50-52, 2019

Sonntag M.:
The End of the Blockchain, in Doucek P. et al. (Eds): IDIMT-2019. Innovation and Transformation in a Digital World, Schriftenreihe Informatik 48, Trauner Verlag, Linz, pp. 311-318, 2019

2020

Berner F., Mayrhofer R., Sametinger J.:
Dynamic Taint Tracking Simulation, in Obaidat M. S. (Ed): E-Business and Telecommunications, ICETE 2019, Prague, Czech Republic, Communications in Computer and Information Science (CCIS) 1247, Springer, pp. 223-227, 2020

Groza B., Berdich A., Jichici C., Mayrhofer R.:
Secure Accelerometer-based Pairing of Mobile Devices in Multi-modal Transport, in IEEE Access 8, pp.9246-9259, 2020

Hölzl M., Roland M., Mir O., Mayrhofer R.:
Disposable Dynamic Accumulators: Toward Practical Privacy-Preserving Mobile eIDs with Scalable Revocation, in International Journal of Information Security 19, Springer, pp. 401-417, 2020

Lau B., Zhang J., Beresford A. R., Thomas D., Mayrhofer R.:
Uraniborg's Device Preloaded App Risks Scoring Metrics, Whitepaper, 2020

Mayrhofer R., Mohan V., Sigg S.:
Adversary Models for Mobile Device Authentication, Computing Research Repository, arXiv:2009.10150 [cs.CR], 2020

Mayrhofer R., Roland M., Höller T.:
Poster: Towards an Architecture for Private Digital Authentication in the Physical World: Network and Distributed System Security Symposium (NDSS Symposium 2020), Posters, San Diego, CA, USA, 2020

Mayrhofer R., Roland M., Hollick M., Lou W., Maaß M., Zheng Y. (Eds):
WiSec '20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz (Virtual Event), Austria, ACM, 2020

Mayrhofer R., Roland M., Gunduz D., Jalaian B., Kurz M., Moser B., Sagduyu Y. E., Shi Y., Stantchev G., Maaß M., Zheng Y. (Eds):
WiseML '20: Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, Linz (Virtual Event), Austria, ACM, 2020

Mir O., Roland M, Mayrhofer R.:
DAMFA: Decentralized Anonymous Multi-Factor Authentication, in BSCI '20: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Taipei, Taiwan, ACM, pp. 10-19, 2020

Roland M., Höller T., Sonntag M., Mayrhofer R.:
The not so private way of tracing contacts: A first analysis of the NOVID20 Android SDK, Analysis Report, Johannes Kepler University Linz, 2020

Roland M., Mayr M., Holzinger R., Vogl M.:
Exposed Building, in Stocker G. et al. (Eds): In Kepler's Gardens – A global journey mapping the 'new' world, Hatje Cantz Verlag, Berlin, 2020

Sonntag M.:
Der Beweiswert von mittels Remote Forensic Software gesammelten Daten, in Tagungsband IRIS 2020, Jusletter IT, 2020

Sonntag M.:
Identity and Privacy, in Doucek P. et al. (Eds): IDIMT-2020. Digitalized Economy, Society and Information Management, Schriftenreihe Informatik 49, Trauner Verlag, Linz, pp. 315-324, 2020

Sonntag M.:
Informationstechnologie: Grundlagen, in Jahnel D. et al. (Eds): IT-Recht, 4. Auflage, Verlag Österreich, pp. 1-46, 2020

Sonntag M.:
Kriterien zur Beurteilung der Beweiskraft von Daten, in International Trends in Legal Informatics - Festschrift Erich Schweighofer, Jusletter IT, pp. 171-199, 2020

2021

Hofer P.:
Analysis of state-of-the-art off-the-shelve face recognition pipelines, Technical Report, Johannes Kepler University Linz, 2021

PUBLICATIONS

2021

Hofer P.:
Face recognition: Combining embeddings, Technical Report, Johannes Kepler University Linz, 2021

Hofer P.:
Face recognition: Increase accuracy by filtering images with heuristics, Technical Report, Johannes Kepler University Linz, 2021

Hofer P., Roland M., Schwarz P., Schwaighofer M., Mayrhofer R.:
Importance of different facial parts for face detection networks, in 2021 9th IEEE International Workshop on Biometrics and Forensics (IWBF), Rome, Italy, IEEE, pp. 1-6, 2021

Höller T.:
Collecting statistical information on v3 onion services, Technical Report, Johannes Kepler University Linz, 2021

Höller T.:
V3 onion services usage, in The Tor Project Blog, 2021

Höller T., Raab T., Roland M., Mayrhofer R.:
On the feasibility of short-lived dynamic onion services, in 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, IEEE, pp. 25-30, 2021

Höller T., Roland M., Mayrhofer R.:
Analyzing inconsistencies in the Tor consensus, in The 23rd International Conference on Information Integration and Web Intelligence (iiWAS2021), Linz, Austria, ACM, pp. 487-496, 2021

Höller T., Roland M., Mayrhofer R.:
On the state of V3 onion services, in Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet (FOCI '21), Virtual, ACM, pp. 50-56, 2021

Mayrhofer R., Roland M., Höller T., Schwaighofer M.:
Towards Threat Modeling for Private Digital Authentication in the Physical World, Technical Report, Johannes Kepler University Linz, 2021

Mayrhofer R., Stoep J. V., Brubacker C., Kralevich N.:
The Android Platform Security Model, in ACM Transactions on Privacy and Security 24(3), pp. 19:1-35, 2021

Pöll M., Roland M.:
Analyzing the Reproducibility of System Image Builds from the Android Open Source Project, Technical Report, Johannes Kepler University Linz, 2021

Preisach M., Roland M.:
Group Signature Applications: Direct Anonymous Attestation, Technical Report, Johannes Kepler University Linz, 2021

Schoiber G.:
Privacy Preserving Hash for Biometrics, Technical Report, Johannes Kepler University Linz, 2021

Schwaighofer M.:
Case Study: Building and testing programming assignments with Nix, in 1st Workshop on Configuration Languages (CONFLANG21), Virtual, 2021

Schwarz P., Scharinger J., Hofer P.:
Gait Recognition with DensePose Energy Images, in Rozinaj G., Vargic R. (Eds): Systems, Signals and Image Processing, IWSSIP 2021, Bratislava, Slovakia, Communications in Computer and Information Science (CCIS) 1527, Springer, pp. 65-70, 2021

Sonntag M.:
Anonymous Proof of Liveness, in Doucek P. et al. (Eds): DIMT -2020. Pandemics: Impacts, Strategies and Responses, Schriftenreihe Informatik 50, Trauner Verlag, Linz, pp. 325-341, 2021

Sonntag M.:
Datensicherheit: Änderungen durch Home Office, in Tagungsband IRIS 2021, Jusletter IT, pp.375-383, 2021

2022

Berdich A., Groza B., Levy E., Shabtai A., Elovici Y., Mayrhofer R.:
Fingerprinting Smartphones Based on Microphone Characteristics from Environment Affected Recordings, in IEEE Access 10, pp. 122399-122413, 2022

Hofer P.:
Poster: Die Bedeutung verschiedener Gesichtsteile für Gesichtserkennung und dessen Zusammenführung, in IKT-Sicherheitskonferenz 2022, Vienna, Austria, 2022

Hofer P., Roland M., Schwarz P., Mayrhofer R.:
Efficient aggregation of face embeddings for decentralized face recognition deployments (extended version), Computing Research Repository, arXiv:2212.10108 [cs.CR], 2022

Höller T., Roland M., Mayrhofer R.:
Evaluating Dynamic Tor Onion Services for Privacy Preserving Distributed Digital Identity Systems, in Journal of Cyber Security and Mobility 11(2), River Publishers, pp. 141-164, 2022

Mayrhofer R., Sigg S.:
Adversary Models for Mobile Device Authentication, in ACM Computing Surveys 54(9), pp. 198:1-35, 2022

Mir O., Roland M., Mayrhofer R.:
Decentralized, Privacy-Preserving, Single Sign-On, in Security and Communication Networks 2022, Article 9983995, 18 pages, 2022

Mir O., Slamanig D., Bauer B., Mayrhofer R.:
Practical Delegatable Anonymous Credentials From Equivalence Class Signatures, Cryptology ePrint Archive, Paper 2022/680, 2022

Pöll M., Roland M.:
Automating the Quantitative Analysis of Reproducibility for Build Artifacts derived from the Android Open Source Project in WiSec '22: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, ACM, pp. 6-19, 2022

Rass S., König S., Wachter J., Egger M., Hobisch M.:
Supervised Machine Learning with Plausible Deniability, Computers & Security 112, pp. 102506:1-20, 2022

Roland M.:
NFC-Zahlungen und mögliche Sicherheitsrisiken, in Recht der Zahlungsdienste (RdZ), Heft 1/2022, Deutscher Fachverlag, pp. 66-69, 2022

Schwaighofer M.:
Reproducibly building artifacts that contain embedded signatures, in NixCon 2022, Paris, France, 2022

Sonntag M.:
Datenmodelle im Urheberrecht, in Tagungsband IRIS 2022, Jusletter IT, pp. 365-372, 2022

Sonntag M.:
Legal Pitfalls of SW Replacement and their Security Implications, in Chroust G. et al. (Eds): IDIMT-2022. Digitalization of Society, Business and Management in a Pandemic, Schriftenreihe Informatik 51, Trauner Verlag, Linz, pp. 259-268, 2022

2023

Ahmad S., Rass S., Schartner P.:
False-Bottom Encryption: Deniable Encryption from Secret Sharing, in IEEE Access 11, pp. 62549-62564, 2023

Berdich A., Groza B., Mayrhofer R.:
A Survey on Fingerprinting Technologies for Smartphones based on Embedded Transducers, in IEEE Internet Things of Journal 10(16), pp. 14646-14670, 2023

Deng G., Liu Y., Mayoral-Vilches V., Liu P., Li Y., Xu Y., Zhang T., Liu Y., Pinzger M., Rass S.:
PentestGPT: An LLM-empowered Automatic Penetration Testing Tool, Computing Research Repository, arXiv:2308.06782 [cs.SE], 2023

Doucek P., Sonntag M., Nedomova L. (Eds):
IDIMT-2023: New Challenges for ICT and Management, 31st Interdisciplinary Information Management Talks, Schriftenreihe Informatik 52, Trauner Verlag, Linz, 2023

Hofer P.:
Dezentrale Gesichtserkennung, in OCG Journal 48(1), pp. 14-15, 2023

Hofer P., Roland M., Mayrhofer R., Schwarz P.:
Optimizing Distributed Face Recognition Systems through Efficient Aggregation of Facial Embeddings, in Advances in Artificial Intelligence and Machine Learning 3(1), Shimur Publications, pp. 693-711, 2023

Hofer P, Roland M., Schwarz P., Mayrhofer R.:
Efficient Aggregation of Face Embeddings for Decentralized Face Recognition Deployments, in ICISSP 2023: Proceedings of the 9th International Conference on Information Systems Security and Privacy, Lisbon, Portugal, SciTePress, pp. 279-286, 2023

Hofer P., Roland M., Schwarz P., Mayrhofer R.:
Face to Face with Efficiency: Real-Time Face Recognition Pipelines on Embedded Devices, in in Delir Haghighi, P. et al. (Eds): Advances in Mobile Computing and Multimedia Intelligence. 21st International Conference, MoMM 2023, Bali, Indonesia, LNCS 14417, pp. 129-143, 2023

Kahlhofer M., Kern P., Henning S., Rass S.:
Benchmarking Function Hook Latency in Cloud-Native Environments, in Softwaretechnik-Trends 43(4), Gesellschaft für Informatik e.V., pp. 11-13, 2023

PUBLICATIONS

2023

Leierzopf E., Roland M., Putz F., Mayrhofer R.:
A Large-Scale Data Collection and Evaluation Framework for Android Device Security Attributes, in Doucek P. et al. (Eds): IDIMT-2023. New Challenges for ICT and Management, Schriftenreihe Informatik 52, Trauner Verlag, Linz, pp. 63-72, 2023

Lins M., Mayrhofer R., Roland M., Beresford A.:
Mobile App Distribution Transparency (MADT): Design and Evaluation of a System to Mitigate Necessary Trust in Mobile App Distribution Systems, in Fritsch L. et al. (Eds): Secure IT Systems 28th Nordic Conference, NordSec 2023, LNCS 14324, Springer, pp. 185-203, 2023

Mayoral-Vilches V., Deng G., Liu Y., Pinzger M., Rass S.:
ExploitFlow, cyber security exploitation routes for Game Theory and AI research in robotics, Computing Research Repository, arXiv:2308.02152 [cs.RO], 2023

Mir O., Bauer B., Griffy S., Lysyanskaya A., Slamanig D.:
Aggregate Signatures with Versatile Randomization and Issuer-Hiding Multi-Authority Anonymous Credentials, Cryptology ePrint Archive, Paper 2023/1016, 2023

Mir O., Bauer B., Griffy S., Lysyanskaya A., Slamanig D.:
Aggregate Signatures with Versatile Randomization and Issuer-Hiding Multi-Authority Anonymous Credentials, in CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, ACM, pp. 30-44, 2023

Mir O., Slamanig D., Bauer B., Mayrhofer R.:
Practical Delegatable Anonymous Credentials From Equivalence Class Signatures, in Proceedings on Privacy Enhancing Technologies (PoPETs) 2023(3), pp. 488-513, 2023

Rass S.:
Perfectly Secure Communication, based on Graph-Topological Addressing in Unique-Neighborhood Networks, Computing Research Repository, arXiv:1810.05602 [cs.CR], 2023

Rass S., König S., Wachter J., Mayoral-Vilches V., Panaousis E.:
Game-theoretic APT defense: An experimental study on robotics, in Computers & Security 132, Elsevier, Article 103328, 19 pages, 2023

Rass S., Pinzger M.:
Incentive-Based Software Security: Fair Micro-Payments for Writing Secure Code, Computing Research Repository, arXiv:2309.05338 [cs.SE], 2023

Roland M., Höller T., Hofer D., Pekarek D., Preisach M.:
An analysis of PoS/ cashIT! cash registers, Vulnerability Report, Johannes Kepler University Linz, 2023

Roland M., Höller T., Mayrhofer R.:
Digitale Identitäten in der physischen Welt: Eine Abwägung von Privatsphäreschutz und Praktikabilität, in HMD Praxis der Wirtschaftsinformatik 60(2), Springer Fachmedien Wiesbaden, pp. 283-307, 2023

Schwarz P., Scharinger J., Hofer P.:
Gait Recognition Using 3D View-Transformation Model, in Moreno-Díaz R. et al. (Eds): Computer Aided Systems Theory – EUROCAST 2022, Las Palmas de Gran Canaria, Spain, LNCS 13789, Springer, pp. 452-459, 2023

Shahzad A., Rass S.:
How to Plausibly Deny Steganographic Secrets, in Proceedings of the 20th International Conference on Security and Cryptography, SECRYPT, Rome, Italy, SciTePress, pp. 731-737, 2023

Sonntag M.:
Aktuelle Rechtsaspekte des DNS: Anmerkungen zu 4 Ob 44/22g, NIS2-RL, Eigentümer-Identifikation sowie Sperrverfügungen, in Tagungsband IRIS 2023, Jusletter IT, pp. 335-342, 2023

Sonntag M., Schraml S.:
An Evidence Collection System for Robot-Supported Inspection of Critical Infrastructure, in Doucek P. et al. (Eds): IDIMT-2023. New Challenges for ICT and Management, Schriftenreihe Informatik 52, Trauner Verlag, Linz, pp. 51-63, 2023

Sonntag M., Mayrhofer R., Rass S.:
Anonymously Publishing Liveness Signals with Plausible Deniability, in Delir Haghighi, P. et al. (Eds): Advances in Mobile Computing and Multimedia Intelligence. 21st International Conference, MoMM 2023, Bali, Indonesia, LNCS 14417, Springer, pp. 3-19, 2023

Sonntag M.:
Der Personenbezug von IP-Adressen, in Schefbeck G. et al. (Eds): Strukturen und Symbole des Rechts - Festschrift für Friedrich Lachmayer, Jusletter IT, pp. 195-216, 2023

Sonntag M., Mayrhofer R., Schraml S.:
INFRASPEC – Automated Inspection of Critical Infrastructure, in ERCIM News 135, pp. 41-42, 2023

2024

Hofer P., Roland M., Mayrhofer R.:
BioDSSL: A Domain Specific Sensor Language for Global, Distributed, Biometric Identification Systems, in 2024 IEEE 12th International Conference on Intelligent Systems (IS), Varna, Bulgaria, IEEE, 2024

Hofer P., Roland M., Schwarz P., Mayrhofer R.:
Shrinking embeddings, not accuracy: Performance-preserving reduction of facial embeddings for complex face verification computations, in 2024 14th International Conference on Pattern Recognition Systems (ICPRS), London, UK, IEEE, 2024

Höller T., Mayrhofer R.:
A case study on DDoS attacks against Tor relays, in Free and Open Communications on the Internet 2024(2), pp. 64-67, 2024

Kempinger S.:
Implementing a Digidow-compatible Sensor for UWB Indoor Positioning, Technical Report, Johannes Kepler University Linz, 2024

Lins M., Mayrhofer R., Roland M., Hofer D., Schwaighofer M.:
On the critical path to implant backdoors and the effectiveness of potential mitigation techniques: Early learnings from XZ, Computing Research Repository, arXiv:2404.08987 [cs.CR], 2024

Mayoral-Vilches V., Jabbour J., Hsiao Y.-S., Wan Z., Crespo-Álvarez M., Stewart M., Reina-Munoz J. M., Nagras P., Vikhe G., Bakhshalipour M., Pinzger M., Rass S., Panigrahi S., Corradi G., Roy N., Gibbons P. B., Neuman S. M., Plancher B., Reddi V. J.:
RobotPerf: An Open-Source, Vendor-Agnostic, Benchmarking Suite for Evaluating Robotics Computing System Performance, Computing Research Repository, arXiv:2309.09212 [cs.RO], 2024

Mayrhofer R., Stoep J. V., Brubacker C., Hackborn D., Bonné B., Tuncay G. S., Jover R. P., Specter M. A.:
The Android Platform Security Model (2023), Computing Research Repository, arXiv:1904.05572v3 [cs.CR], 2024

Mir O., Slamanig D., Mayrhofer R.:
Threshold Delegatable Anonymous Credentials with Controlled and Fine-Grained Delegation, in IEEE Transactions on Dependable and Secure Computing 21(4), pp. 2312-2326, 2024

Rass S.:
Tell me who you are friends with and I will tell you who you are: Unique neighborhoods in random graphs, in Theoretical Computer Science 988, Elsevier, Article 114386, 14 pages, 2024

Rass S., König S., Ahmad S., Goman M.:
Metricizing the Euclidean Space towards Desired Distance Relations in Point Clouds, IEEE Transactions on Information Forensics and Security 19, pp. 7304-7319, 2024

Sonntag M.:
KI-Sprachmodelle: IT-Sicherheit und Einsatz in der Programmierung, in Schweighofer E. et al. (Eds): Tagungsband IRIS 2024. Sprachmodelle: Jurstische Papageien oder mehr?, Jusletter IT, pp. 47-55, 2024

CVEs

2015

Roland M.:
CVE-2015-6606: The Secure Element Evaluation Kit (aka SEEK or SmartCard API) plugin in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 22301786, 2015

2023

Roland M., Höller T., Hofer D., Pekarek D., Preisach M.:
CVE-2023-3654: Bypass of origin check, 2023

Roland M., Höller T., Hofer D., Pekarek D., Preisach M.:
CVE-2023-3655: Unauthenticated remote database exfiltration, 2023

Roland M., Höller T., Hofer D., Pekarek D., Preisach M.:
CVE-2023-3656: Unauthenticated remote code execution, 2023

Hofer D.:
CVE-2023-25825: XSS/JS-RCE in log viewing, 2023

THESES

DIPLOMA/MASTER THESES

Eisner C.:
Portable Sicherungs- und Analysesoftware für E-Mail und Office-Dokument, 2014

Jäger M.:
Sicherheitsaspekte bei Virtualisierungen, 2014

Wurm P.:
Gesicherte Kommunikation von iOS Anwendungen mit SAP Systemen unter ortsabhängiger Zugriffskontrolle, 2014

Schwarz A.:
Introduction of an ISM-process prototype at a foreign site of an international corporation, Advisors: Sonntag M., Simunek W., 2015

Söllner R.:
Cypherpunk Anonymous Remailer focusing on Natural Language Processing, Advisor: Sonntag M., 2015

Wiesner C.:
Nagios für Android: Monitoring von Android-Geräten mittels Nagios, Advisor: Sonntag M., 2015

Bachmair S.:
External Security Analysis of Existing Windows Software based on a Case Study, Advisors: Mayrhofer R., Proksch S., Praher C., 2016

Försterling T.:
Threat Modeling for Data Protection in the Cloud, Advisor: Mayrhofer R., 2016

Haffner G.:
Development and Introduction of a Web based Software for the Administration of Inventions at the University, Advisor: Sonntag M., 2016

Hengstberger M.:
Steganography in File Systems for Mobile Environments with Plausible Deniability, Advisor: Mayrhofer R., 2016

Kapfer P.:
PhonyKeyboard: Sensor-enhanced Keystroke Dynamics Authentication on Mobile Devices, Advisors: Mayrhofer R., Scharinger, J., 2016

Majer J.:
Social Engineering in Information Security – Awareness and Training Program, Advisor: Sonntag M., 2016

Themessl-Huber P.:
A Peer-to-Peer Based Cloud Storage File Synchronization System, Advisor: Sonntag M., 2016

Fisecker F.:
Information security of industrial automation products and measures of improvement, Advisor: Mayrhofer R., 2017

Höller T.:
Automatic Updates for IoT devices exemplified by OpenWRT, Advisor: Mayrhofer R., 2017

Jaguzovic D.:
Who is looking for me online?, Advisor: Sonntag M., 2017

Neuhuber S.:
802.1x for home users and guest networks, Advisor: Mayrhofer R., 2017

Praher M.:
Utilizing Bluetooth keyboard emulation and optical character recognition to securely transfer passwords, Advisors: Mayrhofer R., Hölzl M., 2017

Lemmé A.:
Extension of an existing P2P-Client for Evidence Collection, Advisor: Sonntag M., 2018

Ortner G.:
Mapping The Internet World: An Alternative To IP Geolocation, Advisor: Mayrhofer R., 2018

Reinthaler S.:
A disaster and crisis alerting approach employing home automation systems, Advisor: Sonntag M., 2018

Falhout N.:
Asterisk VoIP over TOR, Advisor: Sonntag M., 2019

Kienbauer P.:
Investigating Web-based Attacks on Tor Onion Services using Honeypots, Advisor: Sonntag M., 2019

Prinz K.:
Next Place Prediction with Hidden Markov Models, Advisors: Mayrhofer R., Muaaz M., 2019

Schöppl P.:
Personal Agent Prototype in Rust, Advisor: Mayrhofer R., 2019

Voglhuber C.:
Security attacks and countermeasures in DOCSIS networks, Advisor: Sonntag M., 2019

Dworschak K.:
Automating the anonymization of personal data in court judgments, Advisor: Sonntag M., 2020

Gründling B.:
App-based (Im)plausible Deniability for Android, Advisor: Mayrhofer R., 2020

Klopf M.:
Detection of vulnerable software components using runtime analysis, Advisor: Sonntag M., 2020

Knabl K. K.:
Design, Implementation and Evaluation of a Mobile Security Scanner App for Smart Home Users, Advisors: Sonntag M., Hummel K. A., 2020

Buchner P.:
Enabling Real-Time Analytics of Web Requests through a Scalable, High-Throughput Platform, Advisor: Sonntag M., 2021

Christof T.:
DJI Wi-Fi Protocol Reverse Engineering, Advisors: Mayrhofer R., Roland M., 2021

Fraundorfer T.:
Cloud Interchangeability, Advisor: Sonntag M., 2021

Raab T.:
Unlinkable Onion Services: Improved Resilience against Metadata Analysis, Advisors: Mayrhofer R., Höller T., 2021

Pöll M.:
Towards a Privacy-focused Biometric Identity System Through a Personal Identity Agent for Android, Advisors: Mayrhofer R., Roland M., 2022

Preisach M.:
System Integrity and Attestation for Biometric Sensors, Advisors: Mayrhofer R., Roland M., 2022

Wagenhuber P.:
A Decentralized, Resilient and Secure Sensor Network, Advisor: Sonntag M., 2022

Wandl P.:
Hidden Glider Finder, Advisor: Sonntag M., 2022

Fixl S.:
Access control for a peer-to-peer filesystem based on cryptographic capabilities, Advisors: Mayrhofer R., Schwaighofer M., Roland M., 2023

Klimont J.:
Design and Implementation of a Data Recording System for Court-Admissible Forensic Evidence, Advisor: Sonntag M., 2024

Kempinger S.:
Assessing the Feasibility of Developing a Secure Digital Identity Wallet for Android, Advisors: Mayrhofer R., Roland M., 2024

Mader F.:
Evaluation of technologies to build a trustworthy directory for sensors for an identity management system, Advisors: Mayrhofer R., Roland M., 2024

PHD DISSERTATIONS

Findling R. D.:
Unobtrusive Mutual Mobile Authentication with Biometrics and Mobile Device Motion, Advisors: Mayrhofer R., Sigg S., Scharinger J., 2017

Hauer B.:
DLP und ILP im Anwendungsbereich der Informationssicherheit, Advisors: Mayrhofer R., Quirchmayr G., 2017

Muaaz M.:
Implicit biometric authentication for smartphones, Advisors: Mayrhofer R., Van Laerhoven K., Scharinger J., 2017

Aichhorn A.:
Secure Protection Interface Communication for Line Current Differential Protection Systems, Advisors: Mayrhofer R., Fickert L., 2018

Hölzl M.:
Applying Smart Cards for Security Critical Mobile Applications, Advisors: Mayrhofer R., Asokan, Scharinger J., 2018

Hintze D.:
Continuous risk-aware multi-modal authentication across mobile devices, Advisors: Mayrhofer R., Beresford A., Scharinger J., Koch E., 2019

Höller T.:
A Privacy Preserving Networking Approach for Distributed Digital Identity Systems, Advisors: Mayrhofer R., Beresford A., Roland M., 2022

Mir O.:
Privacy Preserving Credentials via Novel Primitives, Advisors: Mayrhofer R., Teague V., Slamanig D., 2023

Hofer P.:
Enhancing Privacy-Preserving Biometric Authentication through Decentralization, Advisors: Mayrhofer R., Van Larhoven K., Roland M., 2024

INFRASTRUCTURE

The Institute of Networks and Security has been hosting a network laboratory and associated infrastructure for teaching and research. This lab is being updated continuously to evolve with the changing network landscape, and in 2021 has been transformed into a hybrid lab integrating physical and virtualized network components.

TOPICS AND SCENARIOS

Hybrid Lab
with Integration of Physical
and Virtualized components

IPv4 & IPv6 Dual Stack

Virtual Private Network
connection for work-from-home
hybrid teaching

Central Administration using SNMP & WMI; Monitoring

Server Administration
Virtualization, CIFS/Samba, DFS, DHCP, DNS, NTP, HTTP + FTP, ADS, SMTP + IMAP

Security
802.1X + RADIUS, WLAN-security, Firewall, VPNs, PKIs, IDS/IPS, Spam-, Virus- & Malware-detection, Security scanner, DHCP-Snooping, ARP protection

PC Configuration
Error Analysis, Disk Analysis, BIOS & UEFI-Firmware, SecureBoot

TCP Performance Tests

Switching
VLANs, Q-in-Q, STP/RSTP/MSTP, ERP, LACP+FEC, LLD+CDP, PoE

IPv4 & IPv6 Routing
Static, VRRP+HSRP, BFD, NAT/NAPT, RIP, OSPF, IS-IS, BGP, MPLS

Load-Sharing, Clustering, QoS
ECMP, Web load-balancing, Firewall clustering, VLAN priorities, IP DSCP

HARDWARE EQUIPMENT

Teaching and Network Infrastructure

OPNsense firewall to JKU network, Proxmox virtualization nodes with 4x10 CPU cores and more than 2 TB RAM in total for hybrid lectures, central switches and patch panel, 8 x CAT6 connections to each PC, 8 IP KVMs, 2 display projectors, fileserver for manuals and white-papers

8 Exercise Groups with each

2 PCs (incl. swappable HDs, four Gigabit NICs per PC), Cisco router, HP Layer-2 switch, HP Layer-3 switch, Juniper Layer-3 switch, WLAN Access-Point, Sophos firewall, Foundry Load balancer

Operating Infrastructure

Proxmox virtualization cluster with 3 nodes (each with 2x10 CPU cores, 256 GB RAM), 12 TB Ceph Storage, 44 TB NAS Storage

Open Hardware Lab for Experiments

Cisco Layer-3 switches, Cisco PIX, Lantronix console server, LAN Splitters (100BASE-TX, 1000BASE-SX), Console management controller (Remote power, temperature, smoke, and contact detectors), hubs, cut-through switch, iSCSI storage, PC hardware and ESD environment for laboratory experiments, various OpenWRT (WLAN APs) embedded devices for embedded software development, smart phones, Software Defined Radio Kit (70 MHz-6GHz), security research hardware (MavicPro M1p drone, Crazyradio, ProxmarkPro, Flipper Zero…), Ultra-Wideband (UWB) Development Kit, single-board computers (Odroid, RaspberryPi, NVIDIA Jetson Nano)

PROJECTS

DIGIDOW

DIGiDOW

8 MASTER STUDENTS

8 PHD STUDENTS

2 (SENIOR) POSTDOCS

Christian Doppler Laboratory for Private Digita Authentication in the Physical World (Digidow)

PROJECT LEAD
Prof. René Mayrhofer

PROJECT TIMEFRAME
2020 2026

PROJECT PARTNERS
3 Banken IT GmbH, ekey biometric systems GmbH, Kepler Universitätsklinikum GmbH, NXP Semiconductors Austria GmbH & Co KG, Österreichische Staatsdruckerei GmbH

PROJECT FUNDING
2.278.000€

FUNDING AGENCY
Christian Doppler Forschungsgesellschaft

Bundesministerium Arbeit und Wirtschaft

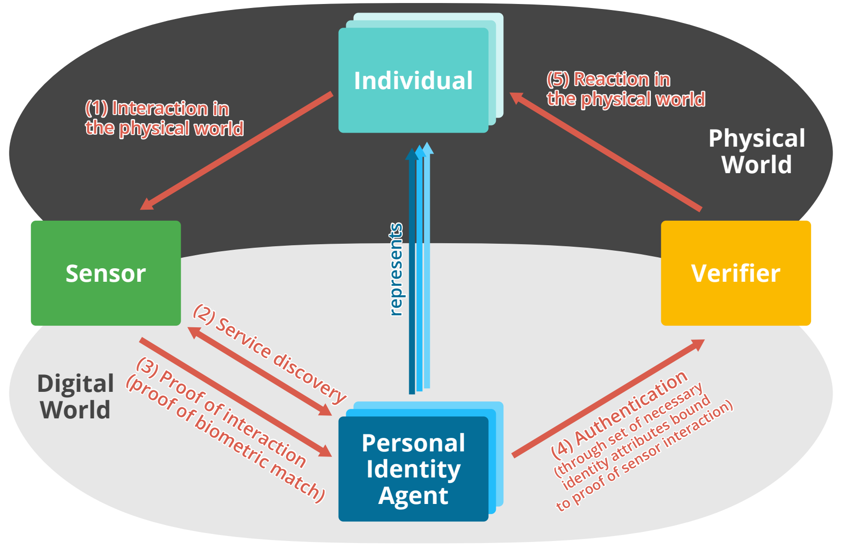
Christian Doppler Forschungsgesellschaft (aus Mitteln des Bundesministeriums für Arbeit und Wirtschaft)

PROJECT WEBPAGE
https://digidow.eu

DIGITAL SHADOW: PRIVATE DIGITAL AUTHENTICATION FOR THE PHYSICAL WORLD

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.


Individual
(1) Interaction in the physical world
(5) Reaction in the physical world
Physical World
Sensor
Verifier
represents
(2) Service discovery
(3) Proof of interaction (proof of biometric match)
Digital World
Personal Identity Agent
(4) Authentication (through set of necessary identity attributes bound to proof of sensor interaction)

In project Digidow, we 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 solve these issues based on private tracking of user location and behavior, implementing it in **personal identity agents (PIA) with a complete chain of trust over multiple parties**, and building yearly prototypes for benchmark use cases like physical door access.

Within the scope of CDL Digidow, we aim to solve the particular combination of three aspects of digital identity as a focal point:

- **Usage of digital identity for physical world interactions** requires a strong binding between the physical world verifier (such as a door), the human being authenticated for this interaction (e.g., through a camera), and their digital identity representation. The derived objective is related to security:

  “How to create a secure binding across the physical/digital world divide based on a limited set oftrust anchors?”

- **Device-less authentication,** in the sense of allowing human users to interact with services without having to carry any form of physical identification document or device, requires storage of the digital identity representation in cloud systems as well as relying on biometric authentication with the implied objective related to availability:

  “How to store and process digital identity attributes and biometric templates in cloud environments and discover the associated network service and digital identity under (soft) real time constraints?”

- **Sovereignty over personal data and interactions for all users of the system** requires technical measures of assigning control to the actual users if we do not want to rely only on organizational/legal/social measures (which can often change more quickly than technical standards and implementations). This implies an architecture (in the sense of a system design) that avoids single points of control and the main objective related to privacy:

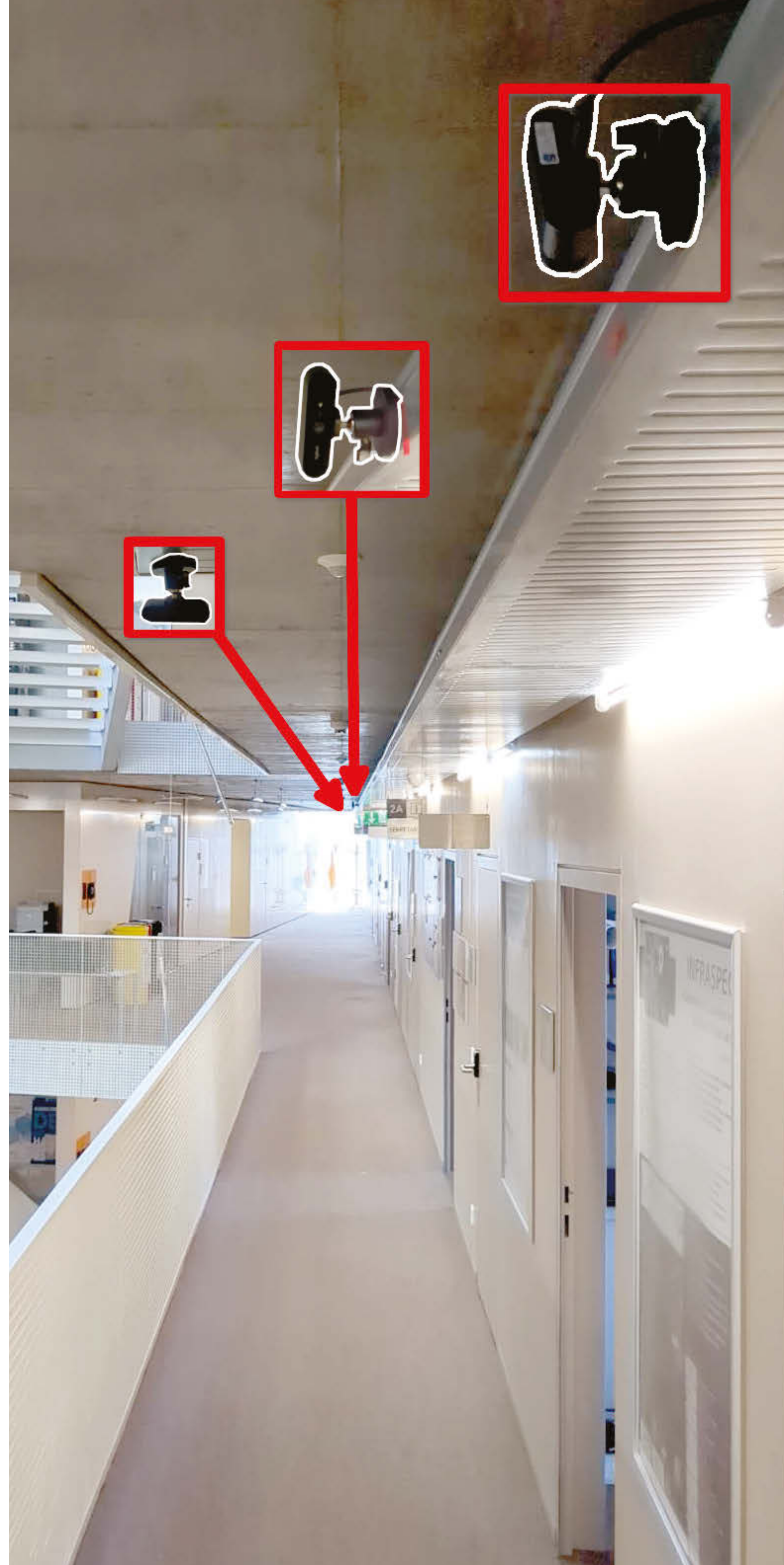
  “How to effectively decentralize the digital identity system architecture to put individuals in control over their data and interactions?”

MAJOR ACHIEVEMENTS

1 We have completed a first version of our Digidow distributed system architecture and associated network protocols between the different main components.

2 The living lab prototype for physical access control of our own office doors implementing this architecture has been established and kept actively running throughout the last 2 years. All prototype code in this living lab is consistently written in memory-safe languages, and within the last 12–18 months has been extended to be built automatically and reproducibly with a continuous integration system maintained within the CDL. Some of the core components are also automatically updating in their live instances, prototyping how in-production deployments could be securely maintained. Moreover, a few of the core components—notably the PIA code—is also automatically logged in a binary transparency log to demonstrate future best practice for supply chain security of such critical components.

3 Scientific results dissemination includes 9 journal articles, 16 conference and workshop papers, 14 technical reports, 38 talks (excluding paper presentations), 2 finished PhD theses, and 15 associated bachelor and master theses. In addition, we presented the CDL Digidow and our living lab demonstrator at the Lange Nacht der Forschung 2022.



LIT SECURE AND CORRECT SYSTEMS LAB

Phase 1

11 TEAM MEMBERS

9 PHD STUDENTS

Phase 2

10 TEAM MEMBERS

8 PHD STUDENTS

PROJECT LEAD

Prof. Daniel Große, Prof. Josef Küng, Prof. René Mayrhofer, Prof. Stefan Rass (in **Phase 2**), Prof. Robert Wille (in **Phase 1**)

PROJECT TIMEFRAME

Phase 1		**Phase 2**	
04.2019	12.2022	01.2023	12.2025

PROJECT FUNDING

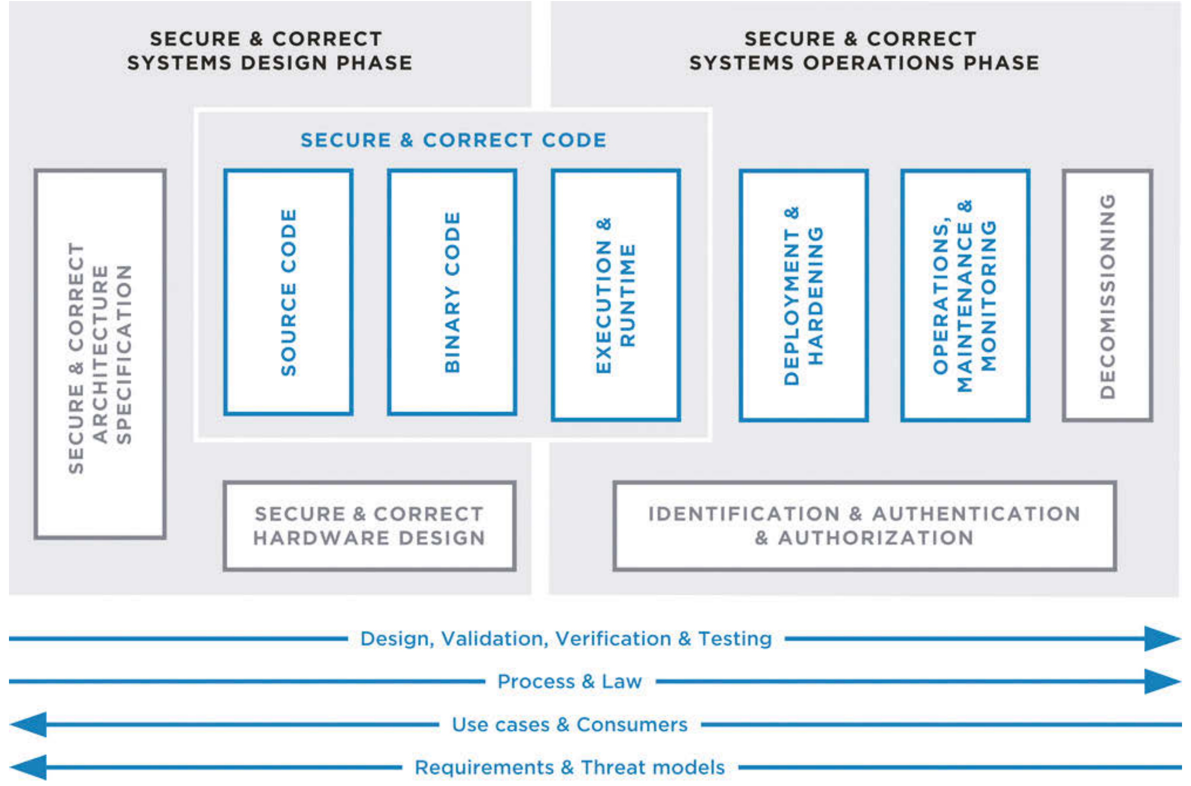
Phase 1	**Phase 2**
2.500.000€	1.995.000€

FUNDING AGENCY

Land OÖ

PROJECT WEBPAGE

https://www.jku.at/en/lit-secure-and-correct-systems-lab/


SECURE & CORRECT SYSTEMS DESIGN PHASE
SECURE & CORRECT SYSTEMS OPERATIONS PHASE
SECURE & CORRECT CODE
SECURE & CORRECT ARCHITECTURE SPECIFICATION
SOURCE CODE
BINARY CODE
EXECUTION & RUNTIME
DEPLOYMENT & HARDENING
OPERATIONS, MAINTENANCE & MONITORING
DECOMISSIONING
SECURE & CORRECT HARDWARE DESIGN
IDENTIFICATION & AUTHENTICATION & AUTHORIZATION
Design, Validation, Verification & Testing
Process & Law
Use cases & Consumers
Requirements & Threat models

Both in terms of supporting operational security and combating deliberate attacks, secure IT systems are essential in today's heavily connected societies. At the same time, the ever-increasing complexity of circuits and systems makes it increasingly difficult to guarantee the correctness of the resulting systems. These developments will become even more decisive for future fields of application.

The **LIT Secure and Correct Systems Lab**, established in 2019, addresses these challenges by combining the expertise of several JKU institutes across different fields. The resulting synergies allow to not only concentrate on a single aspect, but to take the entire lifecycle of secure and correct IT systems into account – from specification to implementation, use and finally decommissioning. In addition to current problems, the focus is on the challenges of the coming years and decades.

More precisely, the LIT Secure and Correct Systems Lab addresses challenges that arise:

1

During design & implementation (Secure and Correct Systems Design),i.e., we address

secure and correct specification,

secure and correct software development, and

secure and correct hardware design.

2

During operation (Secure and Correct Systems Operations) i.e., covering

techniques for the operation of secure and correct systems, e.g., in the areas of execution and runtime as well as deployment and hardening,

identification, authentication and authorisation, and

decommissioning – often neglected, but indispensable for a holistic procedure, operation, maintenance and monitoring also with regard to newly emerging threats.

3

With an interdisciplinary focus that goes beyond the previous topics

validation, verification and testing,

processes and legal questions (law),

case studies / use cases and users / consumers, and

corresponding requirements and threat models.

In an effort to pool expertise, expand on existing competencies, and support junior scholars and reseachers, the LIT Secure and Correct Systems Lab created two main pillars:

- The Graduate School for Secure and Correct Systems. i.e., a JKU PhD program at the Faculty of Engineering and Natural Sciences (TNF) focusing especially on secure and correct systems.
- Fundamental and applied research conducted together with partners in the industry/business community and in academia.

U’SMILE

u'smile

21 TEAM MEMBERS

6 PHD STUDENTS

11 MASTER STUDENTS

4 POSTDOCS

Josef Ressel Center for User-friendly Secure Mobile Environments (u’smile)

PROJECT LEAD

Prof. René Mayrhofer

PROJECT TIMEFRAME

2012 ○—○ 2017

PROJECT PARTNERS

A1 Telekom Austria AG, 3 Banken EDV GmbH, LG Nexera, NXP Semiconductors Austria GmbH, Österreichische Staatsdruckerei GmbH, SBA Research

PROJECT FUNDING

1.430.000€ über
FH Hagenberg

FUNDING AGENCY

Christian Doppler
Forschungsgesellschaft

PROJECT WEBPAGE

https://usmile.at

MISSION

The mission of this Josef Ressel Center for User-friendly Secure Mobile Environments (u’smile) was the analysis of security issues in current and future mobile applications; the design, development, and evaluation of concepts, methods, protocols, and prototypical implementations for addressing them; and communication and co-ordination with industry partners and standardization organizations towards establishing globally accepted standards for secure, interoperable, mobile services.

VISION

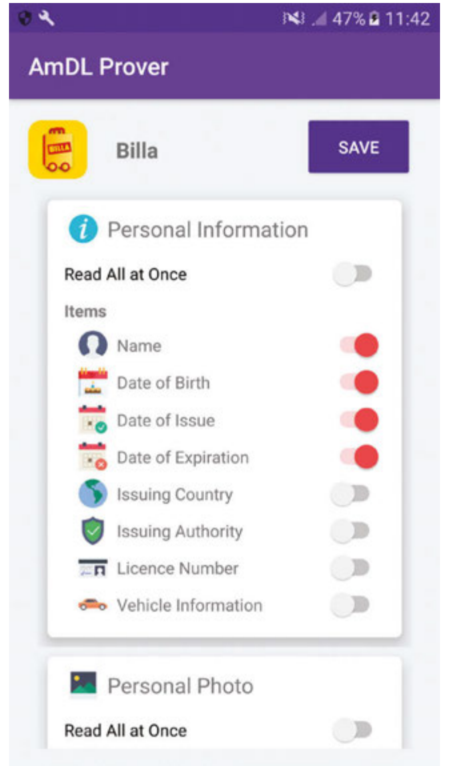
The motivating vision of the JRC u’smile was to – globally, securely, and intuitively usably – substitute current wallets and key chains by suitable services and applications on mobile phones without weakening their security and privacy guarantees. This includes typical credit, debit, and store card functionality, secure and anonymous cash transactions, locking and unlocking doors and other resources, as well as passports, identity cards, licenses, and insurance cards. This vision promises improvements in terms of usability and security: instead of taking care of all these physical identity tokens, users only need to take care of their (single) smartphone. In addition, the smartphone is fully aware of its user and owner and can actively mitigate abuse.

U’SMILE

RESULTS

The JRC u’smile succeeded with many specific contributions towards this vision, and in producing a final prototype of the Austrian mobile driving license on Android smartphones, which brings together the lines of research pursued within the 5 years of the research lab. The demonstrator allows to store and display a driving license on a smartphone (the so-called “prover”) and to present and verify the license document to a second smartphone (the so-called “verifier”) via NFC and WiFi. Both prover and verifier may be offline during verification, and the driving license fully supports selective disclosure of identity attributes and unlinkability of interactions to maintain high privacy guarantees. This project result led to direct participation in international standardization of mobile driving licenses and mobile identity documents in ISO (particularly ISO/IEC 18013-5). It has also helped define the generic Identity Credentials framework released in Android 11.

Within the duration of the lab, we published 18 journal articles, 61 papers in conference proceedings, 5 PhD theses, 2 books, and 22 technical reports and specification documents. Further, a total number of 24 master’s and 14 bachelor’s theses have been completed within the scope of the JRC u’smile.



Billa

Personal Information

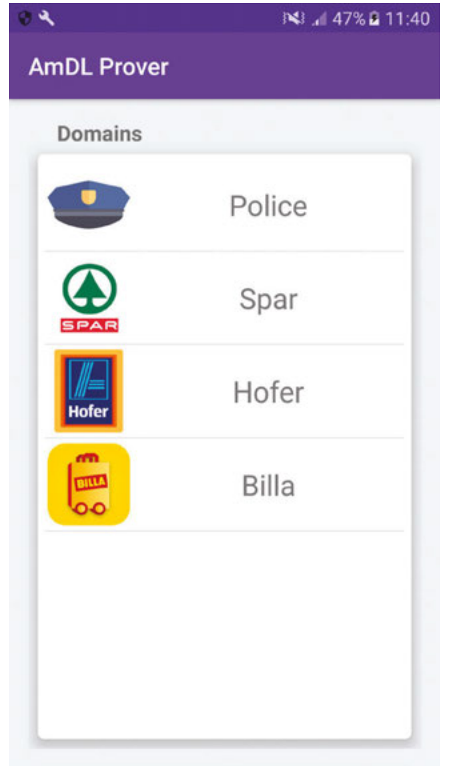
Read All at Once ○

Items

- Name ●
- Date of Birth ●
- Date of Issue ●
- Date of Expiration ●
- Issuing Country ○
- Issuing Authority ○
- Licence Number ○
- Vehicle Information ○

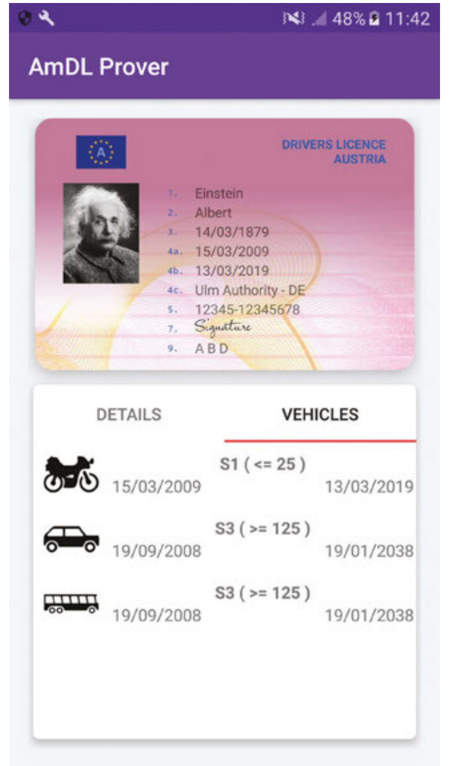
Personal Photo

Read All at Once ○



Domains

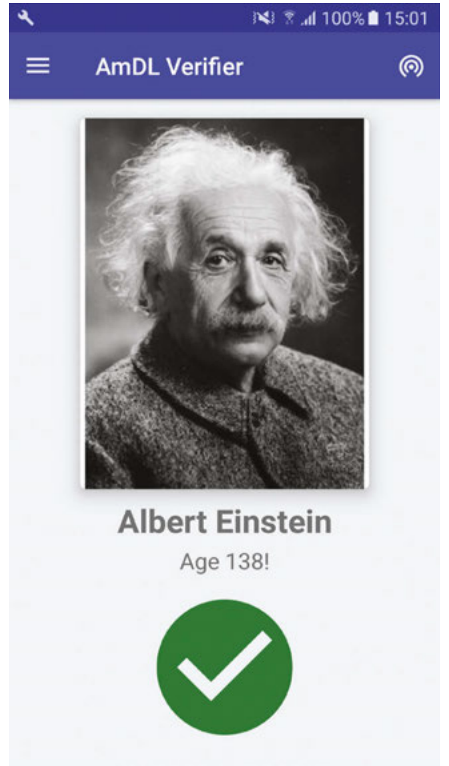
- Police
- Spar
- Hofer
- Billa



1. Einstein
2. Albert
3. 14/03/1879
4a. 15/03/2009
4b. 13/03/2019
4c. Ulm Authority - DE
5. 12345-12345678
7. Signature
9. A B D

DETAILS VEHICLES

15/03/2009	S1 (<= 25)	13/03/2019
19/09/2008	S3 (>= 125)	19/01/2038
19/09/2008	S3 (>= 125)	19/01/2038



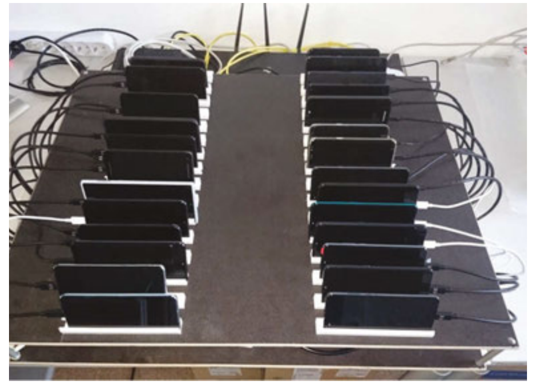
Albert Einstein

Age 138!

ANDROID DEVICE SECURITY DATABASE

1 TEAM MEMBERS

1 PHD STUDENTS



PROJECT PARTNERS

University of Cambridge (United Kingdom), Fraunhofer AISEC (Germany), Secure Systems Engineering GmbH (Germany), University of Strathclyde (United Kingdom), and TU Darmstadt (Germany)

PROJECT TIMEFRAME

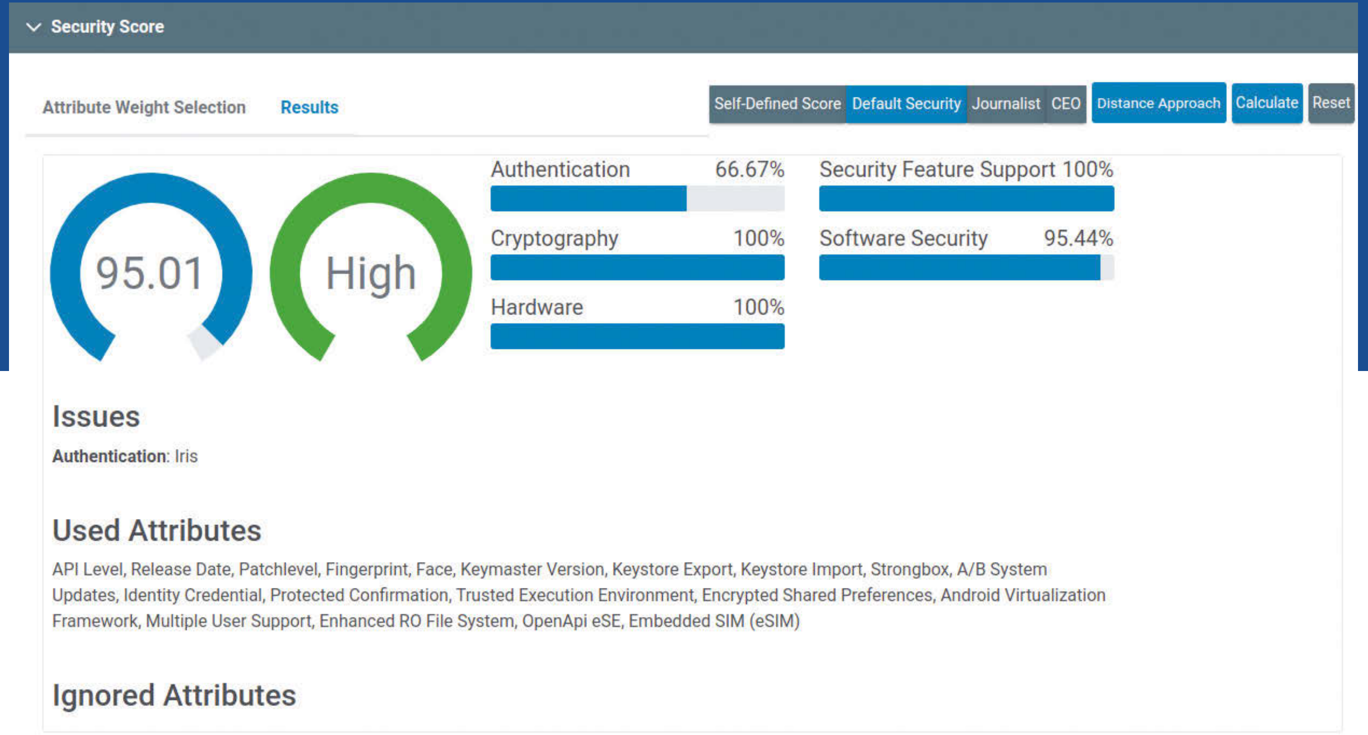
2022 – ONGOING

PROJECT WEBPAGE

https://www.android-device-security.org

ESTABLISHED AS AN OUTPUT OF THE RESEARCH PROJECT ONCE

(funded within the program "IKT der Zunkunft" by the Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK)), the Android Device Security Database evolved into a joint research project to gather and publish relevant data about the security posture of off-the-shelf Android devices.



Authentication 66.67%

Cryptography 100%

Hardware 100%

Security Feature Support 100%

Software Security 95.44%

Issues

Authentication: Iris

Used Attributes

API Level, Release Date, Patchlevel, Fingerprint, Face, Keymaster Version, Keystore Export, Keystore Import, Strongbox, A/B System Updates, Identity Credential, Protected Confirmation, Trusted Execution Environment, Encrypted Shared Preferences, Android Virtualization Framework, Multiple User Support, Enhanced RO File System, OpenApi eSE, Embedded SIM (eSIM)

Ignored Attributes

ONCE

Once
Deine Daten in Deiner Hand

3 TEAM MEMBERS

1 PHD STUDENTS

1 MASTER STUDENTS

ONCE - Online einfach anmelden

PROJECT LEAD

Dr. Michael Roland

PROJECT TIMEFRAME

2021 ○—○ 2023

PROJECT FUNDING

224.500€

FUNDING AGENCY

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

FFG

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

FUNDING PROGRAM

FFG IKT der Zukunft

PROJECT PARTNERS

Schaufenster “Sichere Digitale Identitäten”
Projektkonsortium ONCE (Deutschland)

BACKGROUND

The larger ONCE project consortium aimed to build decentralized, human-centric, open ID wallets to unify and manage multiple different identities of an individual and to use them to securely authenticate to online services. While the use of digital services with identities issued by trusted governmental entities is the main focus, the evolving ecosystem should remain open to other (potentially less trusted) issuers and users/verifies of such identities (also called relying parties) in the sense of self-sovereign identity (SSI). The CDL Digidow, a project running in parallel, primarily focuses on the use of digital identities in the physical world, e.g. to open doors or travel on public transport. While ONCE and Digidow share all of the most important core principles – particularly an explicit, self-sovereign, data minimization driven approach to digital identity with-out massive, centralized instances of data collection – and put privacy and individual control in their focus, they are orthogonal in their respective research focus areas.

ONCE

GOALS

Our main goal is to bridge these two projects to enable optimal and obvious synergies in the creation, management, and use of digital identities for a broad population. We research methods to combine the distributed, decentralized "Personal Identity Agents" developed in the CDL Digidow with the ONCE wallet approach, in order to unify the goals and usability of both projects. Besides merging two novel mobile ID concepts with diverging requirements, a resulting essential research question is how to securely store and use digital identities on current smartphone platforms, in particular when a wallet should be able to host various identities with different protection profiles covering the whole ID ecosystem without always enforcing the highest protection requirements (and thus, opening the ID wallet ecosystem to a broader set of devices and users).

This results in the requirement to quantitatively measure and evaluate security properties of (Android) smartphones, in order to estimate if the security features of a device qualify for specific ID use-cases. At the same time, such metrics offer a basis for a transparent longitudinal presentation of security aspects of smartphones and their continuous maintenance by manufacturers (e.g. in the form of security updates). This novel opportunity to transparently assess and compare smartphone security aspects may even incentivize continued and sustainable maintenance of smartphone products.

RESULTS

As a main outcome, the project resulted in the launch of the Android Device Security Database (https://www.android-device-security.org/), as a public, freely accessible database for quantifying security properties of Android smartphones. The database collects security-relevant properties of Android devices form various sources (dedicated device farms for long-term data collection from a small sample of devices under controlled conditions; web scraping of various other public sources; and in future planned to be extended towards crowd sourcing from a broad range of devices). A graphical representation of security updates over time permits variance comparison of actual software updates with vendor-promised update guarantees. Besides searching for devices with specific properties, a novel method for security scoring allows for benchmarking and comparison of devices based on user-defined criteria.

EXPOSED BUILDING

Exposed Building: Verwundbarkeit intelligenter Gebäude
Project lead: Dr. Michael Roland
Project timeframe: 2020
Project partners: Michael Mayr (3D / Animation / Sound Design)
Project funding: 23.816€
Funding agency: Land Oberösterreich
Funding program: LIT Ars Electronica
Team members: 4
Master students: 2
Postdocs: 1

By opening a maintenance hatch and hacking into the network infrastructure behind it, we acquire access to the electronic locking system. By controlling the buzzers built into the office door locks, we transform the Science Park 2 building at Johannes Kepler University into an orchestra and it resounds like a huge walk-in instrument. The installation playfully provokes thought about the vulnerability of modern technology and its growing risks for society.

In this project, we created an art installation for the Ars Electronica Festival 2020 that turned JKU Science Park 2 into one giant sound sculpture for the duration of the festival (9.-13. September 2020).

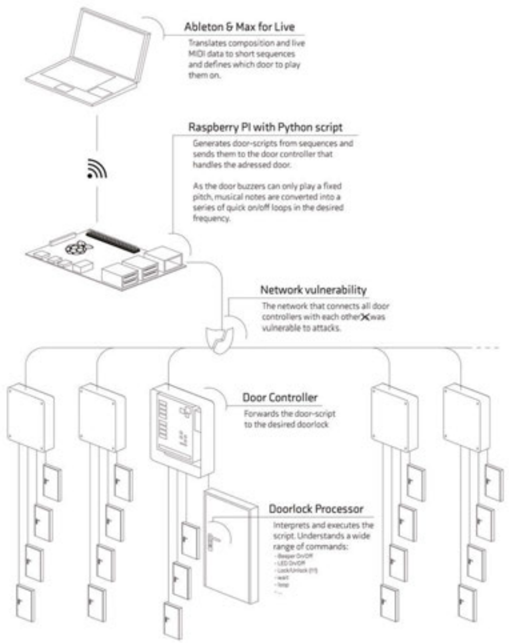
CONCEPT:

Initially, we expected the door lock system to be rather limited in what sounds wecould play. Each door lock is equipped with a 2 kHz constant-frequency buzzer. Thus, we expected to play patterns distributed across the building but we did not expect to be able to play (complex) melodies. However, after initial technical experiments, we found that we could modulate tones over the buzzer base-frequency by pulse-width modulation in very fine-granular steps. This allowed us to play complex sounds consisting of several different tones with each door. After negotiations with Johannes Kepler University Linz (which provided the venue for the Ars Electronica Festival) and the artistic lead of the festival, we got the offer to use a whole building as a standalone art installation without disturbance from other parts of the exhibition. Therefore, we designed the artistic concept to turn all door locks of the Science Park 2 building into one giant musical instrument that played a complex musical composition throughout the festival.

With this concept we were even able to attract the team of Sounding Linz (Linzer Klangwolke 2020) for our project. This lead to our sound sculpture being recorded and integrated into the live stream of Sounding Linz on 12. September 2020.

IMPLEMENTATION:

We developed software that allows us to automatically hack into the physical access control system of the building (abusing vulnerabilities discovered in our previous research). Our software implements the Open Sound Control (OSC) protocol to allow attaching standard music composition software (as used by our artistic partner) to our new musical instrument. The software then turns these commands (essentially consisting of instructions which sub-instrument, i.e. door lock, should play which tone) into commands that can be injected into the electronic locking system to let the buzzers of specific locks play a tone.
Besides the actual instrumentation of the electronic locking system, we also created a 3D visualization of the building showing which door locks currently play a tone. Michael Mayr leveraged this OSC interface to create a composition played during the festival.


Ableton & Max for Live
Translates composition and live MIDI data to short sequences and defines which door to play them on.
Raspberry PI with Python script
Generates door-scripts from sequences and sends them to the door controller that handles the adressed door.
As the door buzzers can only play a fixed pitch, musical notes are converted into a series of quick on/off loops in the desired frequency.
Network vulnerability
The network that connects all door controllers with each other was vulnerable to attacks.
Door Controller
Forwards the door-script to the desired doorlock
Doorlock Processor
Interprets and executes the script. Understands a wide range of commands:
- Beeper On/Off
- LED On/Off
- Lock/Unlock (!!!)
- wait
- loop
- ...

JKU NETWORK SCANS

Project lead: Dr. Tobias Höller and Dr. Michael Roland
Project timeframe: 2022-ongoing
Team members: 6

Employees of the INS along with colleagues from the LIT Lab for Secure and Correct Systems conduct (in tight cooperation with the JKU IT-Department) scans of the JKU network infrastructure. The JKU network (AS1205) exists since the 90's and includes a public B-class network with more than 65.000 IP addresses along with several smaller networks. To encourage research on IT across different fields, all IP departments were provided with publicly reachable IP ranges. This distributed nature requires strong segmentation of different organizational units, institutes and research projects which are all assigned individual network segments with unique permissions.
The project analyzes the network both on a logical and a physical level and raises questions regarding the security of publicly (or just internally) reachable services, maintenance of project infrastructure after funding has ended or physical accessibility of restricted network segments due to infrastructure changes on a university campus.
A sideline of this research resulted in the public disclosure of several serious vulnerabilities in an Austrian cash registry software (CVE-2023-3654, CVE-2023-3655, CVE-2023-3656).

TOR

Project lead: Prof. Michael Sonntag
Project timeframe: 2015-2018
Project funding: Bereitstellung der Bandbreite durch ACOnet
Team members: 1

This project has been realized in cooperation with the **Information Management (IM)** department of the Johannes Kepler University Linz and the **ACOnet**, the Austrian academic network.

INS runs a so-called "Exit Node" within the Tor anonymization network. This network service is used by many whistleblowers (including Edward Snowden), journalists, critical NGOs, dissidents and just plain normal people from stringent state regimes to safeguard their Internet communication from snooping by Internet service providers (ISPs), application providers (such as Facebook, Google, and many others) and countries, and we believe that the right to and possibility for free, unmonitored exchange of information and opinion (sometimes referred to as freedom of speech) is a cornerstone of open, democratic societies. Therefore, we support this anonymization network with an exit node that transports any traffic to and from the Tor network and with the open Internet in an unfiltered manner with up to 200 MBit/s over the Johannes Kepler University network as connected to the Austrian ACONet.

On the 4.12.2015 the project was publicly unveiled during the event **"Privatsphäre im Internet - Der TOR Exit-Node an der JKU, opens an external URL in a new window"**. Technical as well as legal questions were presented and discussed.

EMENTIO

Innovatives Tool zur Prüfung von Unterschriften mittels Künstlicher Intelligenz (EMENTIO)
Project lead: Prof. Stefan Rass (partner, coordinator: Albatross Consulting)
Project timeframe: 2023-2024
Project partners: Albatross Consulting e.U.
Project funding: 15.000€ (Project total 148.413€)
Funding agency: FFG Basisprogramm, Grant Nr. FO999900071
Project webpage: https://www.jku.at/lit-secure-and-correct-systems-lab/secure-systems-group/projekte/
Master students: 1

The main aim of the project is to develop a toolset for the fast, secure and automated verification of handwritten signatures. Statistical methods and artificial intelligence processes are to be evaluated and utilised for this purpose. Recognition involves recognising duplicates (the same signature on behalf of different people without their consent) as well as assigning people to unknown handwriting based on handwriting characteristics.

INFRASPEC

Project lead: Prof. Michael Sonntag
Project timeframe: 2022-2024
Project funding: 53.500€ (Project total 759.908€, funding 403.573€)
Project partners: AIT Austrian Institute of Technology GmbH, CBRN Protection GmbH, Disaster Competence Network Austria - Kompetenznetzwerk für Katastrophenprävention, Flughafen Wien Aktiengesellschaft, Rosenbauer International AG, WIENER NETZE GmbH, Republik Österreich (Bund) vertreten durch das Bundesministerium für Inneres/Bundeskriminalamt sowie Bundesministerium für Landesverteidigung/Abteilung Wissenschaft, Forschung und Entwicklung
Funding agency: FFG-KIRAS
Team members: 2
Master students: 1

Critical infrastructures such as power plants or public transport (airport, subway, etc.) form the basis for supplying the population with vital services and goods such as transport, energy, water and data.

A failure or impairment can lead to significant disruptions to public safety. These structures include extensive and complex networks of supply shafts (so-called collector passages) extending up to several hundred kilometers. These offer a high risk of incidents, but can also be targets for deliberate manipulation or actions with criminal intent.

The difficult environmental conditions, such as long corridors with small dimensions or limited accessibility, pose particular challenges for the responsible personnel in the prescribed, regular checks of the technical operating conditions (tightness, heat loss, etc.) and the structural substance. In addition, the vulnerability of critical pipe and cable ducts is also of central importance with regard to the terrorist threat.

Attacks on such infrastructures can have fatal consequences. For example, large-scale and long-lasting failures in the power or water supply inevitably lead to enormous costs and even health-damaging consequences for the affected population.

Attacks on such infrastructures can have fatal consequences. For example, large-scale and long-lasting failures in the power or water supply inevitably lead to enormous costs and even health-damaging consequences for the affected population.

The KIRAS project INFRASPEC is researching new methods to inspect critical infrastructure with the help of robots by subjecting them to a 3D scan.

On the one hand, this is used for automated evaluation and visualization for the operating personnel, on the other hand, it enables a comparison with previous checks. In addition to manipulations, damage to the building structure, leaks, both removed (e.g. safety elements such as fire extinguishers) and added (e.g. forgotten tool boxes, but also potential explosive devices) should be automatically recognized and highlighted in the display.

This supports and relieves security personnel in the prescribed, regular checks.

It also includes the remote-controlled detailed examination using a robotic arm with additional sensors, e.g. on the back of pipes or in the case of unexpected objects, as well as the measurement of any hazardous substances (gas/liquid leaks from pipes, CO2 concentration, etc.).

DURCHBLICK

Project lead: Prof. Michael Sonntag
Project timeframe: 2017-2018
Project funding: 32.000€ (Project total 960.177€, funding 796.967€)
Project partners: AIT Austrian Institute of Technology GmbH, VICESSE-Vienna Centre for Societal Security, IQSOFT-Gesellschaft für Informationstechnologie, Ionicon-Analytik Gesellschaft m.b.H., Stancon - DI Dr. Heinz Stanek, CBRN Protection GmbH; BMLVS (Federal Ministry of Defence and Sports)
Funding agency: FFG KIRAS
Team members: 1
Master students: 1

In this project, various sensor technologies are investigated and combined for robotic analysis of suspicious objects (e.g., luggage, trash cans) in public spaces and their forensic examination. The primary focus is on developing methods for sensor data fusion and visualization within minutes to better assess the potential risks and damage. This additional information can also contribute significantly to determining the procedure for eliminating the hazard source. At the end of the project, results will be demonstrated using a robot prototype based on the scenarios defined in the project.

The specific task of INS is to ensure secure communication between the mobile platform and the evaluation station, as well as to examine the implications for data protection and data security.

The project DURCHBLICK is funded under the Austrian security research program KIRAS by the Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK).

MAJOR ACHIEVEMENTS:

- Optimized sensor data fusion and rapid visualization: Methods for combining sensor data to enable comprehensive and precise analysis of suspicious objects. A system for quick visualization of sensor data within minutes, allowing for immediate assessment of potential hazards and damage.
- Enhanced Forensic Investigation: Detailed forensic analysis of suspicious objects to help authorities better understand the nature and origin of objects. Secure recording of data for potential legal proceedings.
- Secure Communication and Data Privacy: Implementation and validation of secure communication protocols between the mobile platform and the evaluation station to ensure data integrity and confidentiality. Examination of privacy and security implications and implementation of measures to protect personal data.

SOPHIE

reSilienz vOn supPly cHaIns gegenüber kaskadEneffekten aus dem digitalen Raum (SOPHIE)
Project lead: Prof. Stefan Rass (partner; coordinator: Austrian Institute of Technology)
Project timeframe: 2023-2025
Project partners: AIT Austrian Institute of Technology GmbH (lead), Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik, Bundesministerium für Finanzen, Bundesministerium für Inneres (BMI), Bundesministerium für Landesverteidigung, Bundesministerium für Land- und Forstwirtschaft, Digital Factory Vorarlberg GmbH, Gebrüder Weiss Gesellschaft m.b.H., h2 projekt. beratung KG, Institut für empirische Sozialforschung (IFES) Gesellschaft mbH, FH OÖ Forschungs & Entwicklungs GmbH, Wiener Lokalbahnen Cargo GmbH
Project funding: 111.559€ (Project total 1.094.000€, funding 929.900€)
Funding agency: FFG/KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte, Grant Nr. FO999905291
Project webpage: https://www.kiras.at/gefoerderte-projekte/detail/sophie-resilienz-von-supply-chains-gegenueber-kaskadeneffekten-aus-dem-digitalen-raum/
Master students: 1

The resilience of ICT infrastructures is fundamental to the functioning of supply chains. The more reliable these infrastructures are, the greater the predictability for production and supply chains, and consequently for buyers and customers. Securing such systems against threats from cyberspace is central to the functioning of a “smart economy”, which is based on the principle of “just in time” and must optimise transport routes with as little intermediate storage as possible. In the event of a cyber attack, it is essential to be able to rely on proven structures and processes, sufficient early detection and appropriate decision-making models in order to avoid or minimise disruption to ICT systems.

The SOPHIE project therefore aims to raise awareness of cyber security issues in the supply chain and incident response, particularly for key technical and non-technical personnel in the supply chain, and to support and improve relevant processes with suitable tools and reference processes in terms of resilience.

CAVE-PNP

Project lead: Prof. Stefan Rass
Project timeframe: 2020-2023
Project funding: 113.313€
Funding agency: Fond zur Förderung wissenschaftlicher Forschung (FWF)
Project webpage: https://www.jku.at/lit-secure-and-correct-systems-lab/secure-systems-group/projekte/
Master students: 1

The famous P/NP question is one of the most challenging open problems in computer science and is one of the Clay Institute's remaining six unsolved millennium problems. Despite the progress that has been made in the decades since the problem was posed, the question remains unsolved. Intuitively, it is easy to describe: Consider only problems whose answer is simply "yes" or "no". Among them are also those for which a yes/no answer can be calculated in "reasonable" time, depending on the size of the problem. We call the class of all these problems P. Suppose we do not ask for the solution, since a solution is already given. Then the task is to check whether the given solution is correct or incorrect. Many problems allow such a check in an efficient way. These problems form the class NP. The P/NP question is: is P = NP, P ≠ NP, or (as a third possibility), is this provable at all?

The apparent simplicity of the problem has led many researchers to tackle the question, from professional scientists to amateur mathematicians, who have proposed a variety of solutions, none of which have yet been recognised by the scientific community. A few barriers and "dead ends" on the way to an answer are known, but the sheer number of published proofs is growing faster than the scientific community can verify them. In the long term, this could lead to the correct answer being found but remaining unrecognised amid many failed attempts. To date, there are around 120 attempts at proof, of which a small majority claim inequality, a minority claim equality, and a small remainder claim the unprovability of any answer.

In view of the fact that today's scientific quality management is heavily dependent on peer reviews, which are often carried out voluntarily and without payment, the project aims to help researchers obtain an independent and objective review of their work by computer. Specifically, the project will select papers from all three categories (equality/inequality/unprovability), convert them into a machine-readable representation and subject them to automated verification by computers. Such proof assistants make it possible to objectively check complex mathematical/logical arguments without the need for voluntary reviewers.

Regardless of its importance for science, the study of P/NP is a fruitful field of research that has provided many new concepts and ideas that have been applied elsewhere. The machine verifiability of P/NP evidence (analogous to the nature of the NP class itself) may not only be a step towards an answer to the question, but in any case also contributes to the importance of proof assistants as powerful tools for research.

ODYSSEUS

Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten (ODYSSEUS)
Project lead: Prof. Stefan Rass (partner; coordinator: Austrian Institute of Technology)
Project timeframe: 2019-2021
Project partners: Austrian Institute of Technology (lead), cubido business solutions GmbH, IFES Institut für Empirische Sozialforschung, Bundesministerium für Inneres, Bundesministerium für Landesverteidigung und Sport, Magistratsdirektion der Stadt Wien, Universität Wien
Project funding: 121.454€ (Project total 813.282€; funding 691.289€)
Funding agency: FFG/KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte, Grant Nr. 873539
Project website: https://www.ait.ac.at/themen/cyber-security/projects/odysseus
Master students: 2

Cities and their urban agglomerations are home to a large number of critical infrastructures (CI) that provide essential services in a geographically confined space and are therefore physically and logically dependent on each other. This results in a sensitive network of organisations and connections in which incidents within a single infrastructure can have an impact on the entire system. In particular, critical infrastructures in the areas of supply (electricity, gas, water, etc.), communication (ICT), goods distribution (food, fuel, etc.) and transport (road, rail, etc.) operate extensive networks that have special requirements in terms of security measures. Against the background of the Network and Information System Security Act (NISG), a detailed risk analysis with a strong focus on the interaction of these networks and potential cascading effects for the population is therefore a central aspect of protecting these critical supply infrastructures. However, the increasing focus on so-called "soft targets", i.e. targets in public space that are attractive for terrorist attacks, would also have an impact on the above-mentioned networks in the event of an attack.

The aim of the ODYSSEUS project is to create a simulation-based, cross-domain risk model using the example of the city of Vienna, which describes the networks of the central supply infrastructures (electricity, gas, water, food and telecommunications including ICT) as well as the transport networks (road and rail) up to a sufficient level of abstraction. This level of abstraction should be kept as low as possible in order to achieve a representation that is as close to reality as possible (depending on the available data quantity and quality). Potential threats (both natural disasters and man-made incidents) are simulated on the basis of this model. In contrast to existing solutions from literature and practice, ODYSSEUS focusses on the dynamic relationships between the networks and mathematical models from stochastics (e.g. Markov chains, probabilistic automata) are developed for a realistic representation.

The central output of ODYSSEUS is a framework that enables a detailed assessment of both the impact of threats on individual critical infrastructures and the possible cascading effects within the entire network of critical supply infrastructures, taking into account the urban population. The simulations describe which potential compensation and displacement mechanisms can be expected within the multi-layered network of supply infrastructures or on public spaces in the event of an incident (intentional, technical or natural hazard). From this knowledge, targeted preventive security measures can be derived, presented and evaluated, the implementation of which minimises the effects in the event of an incident.

COMPAC

Computing Partitions by Analog Circuits (COMPAC)
Project lead: Prof. Stefan Rass
Project timeframe: 2024-2026
Project partners: Institute for Integrated Circuits (JKU)
Project funding: 184.332€
Funding agency: Linz Institute of Technology / Land Oberösterreich
Master students: 4

In spite of remarkable achievements in computational power, the notorious class of NP-complete problems has escaped all attempts to find efficient algorithms for the worst-case instances. The vast majority of work relies on Turing machines or equivalent models, all of which relate to digital computing. This raises the question of whether a (partially) non-digital computer could provide a new door to an efficient solution. Indeed, the partition problem, as one NP-complete sibling of the famous Boolean satisfiability problem, could be open to efficient solutions via analogue computing. This seed project shall explore the (physical) limits of computing set partitions by analogue computing. This shall help to get a better understanding of computational intractability (and the physical Church Turing hypothesis), by studying physical barriers, to which logical/digital counterparts may exist (e.g., such as pseudopolynomial complexity bounds, which, based on precursor results of the project, seem to exist in the physical and the digital realm). As such, the COMPAC project is a feasibility study to pave the way towards subsequent deeper studies of analog computing to possibly solve instances of problems that are intractable on digital computing architectures.

TAHITI

Trends in Current Challenges in IT Security
Project lead: Prof. Michael Sonntag
Project timeframe: 2021
Project partners: Limes Security GmbH, Software Competence Center, Business Upper Austria - OÖ
Project funding: 50.000€
Funding agency: FFG
Team members: 7

TAHITI QUALIFICATION SEMINAR: "TRENDS AND CURRENT CHALLENGES IN IT SECURITY" – A FIVE-DAY QUALIFICATION SEMINA

OVERVIEW:
IT security in companies that develop or operate their own software and digital products is a highly dynamic field. Companies must constantly prepare for new challenges. IT security experts are also hard to come by, as skilled professionals in this area are scarce. Therefore, it is crucial to retain and upskill existing staff.

The new five-day qualification seminar "Trends and Current Challenges in IT Security" has been developed by Johannes Kepler University Linz, the Software Competence Center Hagenberg, and Limes Security in collaboration with the IT-Cluster of Business Upper Austria and numerous Upper Austrian companies. The seminar offers a comprehensive training format that is precisely tailored to the needs of businesses.

OBJECTIVE OF THE SEMINAR:
The seminar aims to address current IT security topics. The practical content is introduced through lectures and then deepened through practical exercises. This approach not only enhances understanding but also improves the implementation of the learned concepts in the company context.

The development of the seminar is funded by the Federal Ministry for Digital and Economic Affairs (BMDW) under the "Research Competencies for the Economy" program.

The seminar was repeated in updated form in cooperation with Business Upper Austria as a commercial offering in2023.

CONTENTS OVERVIEW:

- **IT Security Overview:** Basics of IT security, attacker classification, threat models, classical cryptography, user authentication (biometrics, secure tokens), Single Sign-On, security management, network security (firewalls, IDS, etc.), VPNs
- **Web Security:** Security of web applications and frameworks; types of attacks and their defenses; security features in modern browsers and how to configure them; specific types of attacks and their countermeasures: injection, XSS, CSRF, misconfiguration, etc.
- **Cloud Security:** Challenges, threats, and countermeasures; virtualization security; container technologies; Secure Enclave (SGX) Software Analysis/Secure Coding: Coding practices, static dependency analysis, software/dependency management
- **Mobile Device Security:** Smartphone security compared to desktop systems; Android Security, especially its security concepts; secure use of mobile devices
- **Equality:** Equality in IT security and software development

PRACTICAL EXERCISES:

- Creating a threat model, configuring firewalls, setting up VPNs
- Web Security: "Hacking" a test server, fixing security issues, and verifying success
- Penetration Testing: What constitutes a good penetration test, proper preparation, and reporting, typical tests and findings
- Cloud Security: Securing containers and their management/orchestration
- Quantum Cryptography: Principles of quantum encryption, main protocols, experimental demonstrations
- Software Analysis/Secure Coding: Static code analysis

QUALIFICATION GOALS:

- Training IT-experienced individuals, e.g., software developers, on new challenges in IT security
- Providing an overview of current development and research topics
- Assessing the relevance of potential future developments for one's own company

JOINT INTERNATIONAL PHD-PROGRAM IN INFORMATICS

Project lead: Prof. René Mayrhofer
Project timeframe: 2016-2018
Project partners: FH OÖ Hagenberg
Project funding: 204.000€
Funding agency: Land OÖ
Team members: 2
PhD students: 3

The Joint International PhD program in Informatics was a collaboration between JKU and FH Hagenberg to provide research opportunities specifically for incoming international students. By providing a full scholarship to aspiring young researchers, the program was successful in attracting 4 PhD students from outside the European Union to relocate to Austria and pursue their research in collaboration between JKU und FH Hagenberg.

LIT ARTIFACT: JKU SOUNDWAVE - ACOUSTIC DATA TRANSMISSION VIA APP

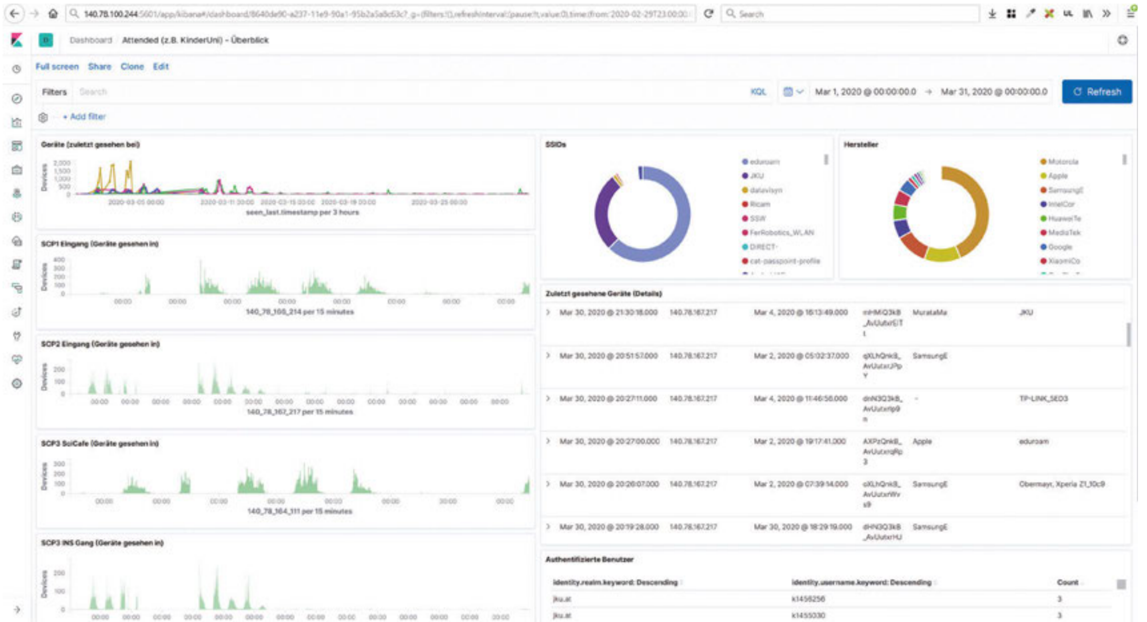
Project lead: Prof. Michael Sonntag
Project timeframe: 2019-2020
Project funding: 9.500€
Funding agency: Land Oberösterreich
Funding program: LIT Artifact Call 2019
Team members: 1
Master students: 1

The artifact is an App for Android devices that allows to transfer data (short texts) via audible tones. This is done at the transmitter by encoding the data, converting it into sounds and outputting it. The receiver records the sounds via the built-in microphone, converts them back into data and displays them. Two coding methods and several "security variants" can be selected by the user. Encoding is performed via the volume (amplitude modulation) or via frequency shift keying (FSK), which is significantly less sensitive to interference. The transmission can be secured using parity bits (1 - detection only, 3 - correction of 1-bit errors) or a checksum (CRC32 or SHA256). Encryption (simple only: Caesar cipher) is available too. Obfuscation is possible using steganography (additional permanent background noise).

LIT ARTIFACT: YOUR DIGITAL TRACES

Your Digital Traces: The potential of tracking individuals carrying smart phones
Project lead: Dr. Michael Roland
Project timeframe: 2019-2020
Project funding: 14.660€
Funding agency: Land Oberösterreich
Funding program: LIT Artifact Call 2019
Team members: 1
Master students: 1

The artifact "Your Digital Traces" visualizes how persons (or rather their mobile devices) can be tracked by passively observing data that mobile devices continuously broadcast in order to discover and maintain Wi-Fi access. Such leaked data may include unique device information, names of Wi-Fi networks a device had been connected to in the past, etc. Based on pre-existing research in the area of Wi-Fi security and privacy, this project developed an environment to collect, analyze, and visualize data obtained through data leaks in current Wi-Fi technology. The visualization should raise awareness about such hidden data leaks. The artifact "Your Digital Traces" primarily aims at integration into mini-lectures such as KinderUni and FIT-Infotage.



Dashboard / Attended (z.B. KinderUni) - Überblick

Filters: Search — KQL — Mar 1, 2020 @ 00:00:00.0 → Mar 31, 2020 @ 00:00:00.0

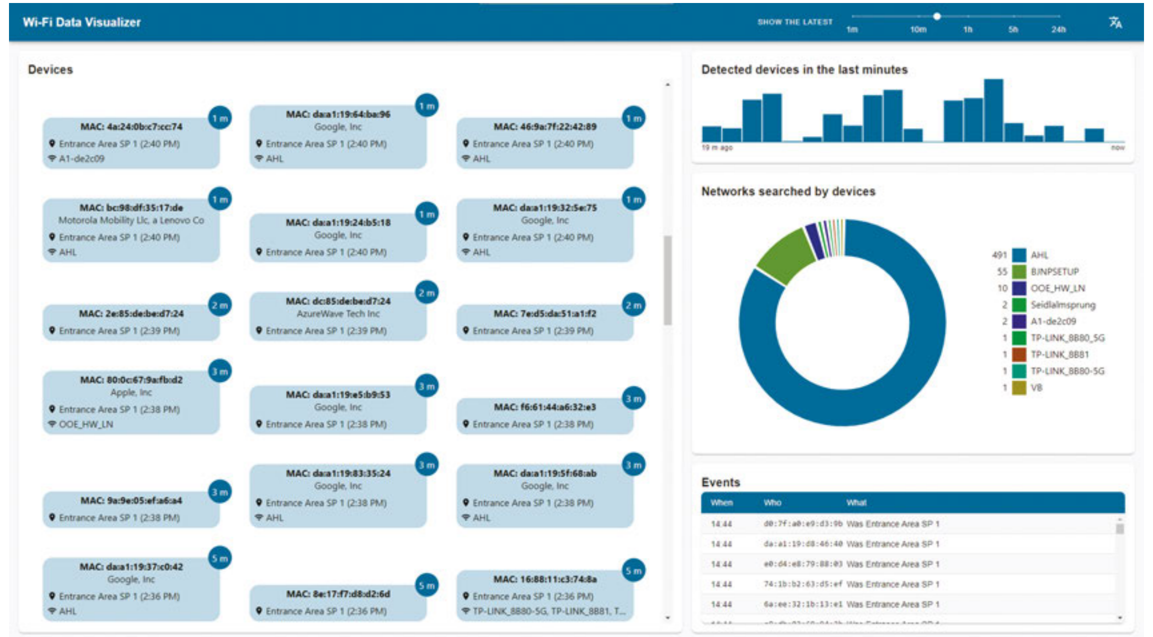
140.78.100.244:5601/app/kibana#/dashboard/...
Search
Full screen
Share
Clone
Edit
Refresh
+ Add filter
Geräte (zuletzt gesehen bei)
Devices
2,000
1,500
1,000
500
0
2020-03-05 00:00
2020-03-11 00:00
2020-03-15 00:00
2020-03-19 00:00
2020-03-25 00:00
seen_last.timestamp per 3 hours
SCP1 Eingang (Geräte gesehen in)
140_78_105_214 per 15 minutes
SCP2 Eingang (Geräte gesehen in)
140_78_167_217 per 15 minutes
SCP3 SciCafe (Geräte gesehen in)
140_78_164_111 per 15 minutes
SCP3 INS Gang (Geräte gesehen in)
SSIDs
eduroam
JKU
datavisyn
Ricam
SSW
FerRobotics_WLAN
DIRECT-
cat-passpoint-profile
Hersteller
Motorola
Apple
SamsungE
IntelCor
HuaweiTe
MediaTek
Google
XiaomiCo

Zuletzt gesehene Geräte (Details)

Mar 30, 2020 @ 21:30:18.000	140.78.167.217	Mar 4, 2020 @ 16:13:49.000	mHMiQ3kB_AvUutxrEiTt	MurataMa	JKU
Mar 30, 2020 @ 20:51:57.000	140.78.167.217	Mar 2, 2020 @ 05:02:37.000	qXLhQnkB_AvUutxrJPpY	SamsungE	
Mar 30, 2020 @ 20:27:11.000	140.78.167.217	Mar 4, 2020 @ 11:46:56.000	dnN3Q3kB_AvUutxrlp9n	-	TP-LINK_5E03
Mar 30, 2020 @ 20:27:00.000	140.78.167.217	Mar 2, 2020 @ 19:17:41.000	AXPzQnkB_AvUutxrqRp3	Apple	eduroam
Mar 30, 2020 @ 20:26:07.000	140.78.167.217	Mar 2, 2020 @ 07:39:14.000	oXLhQnkB_AvUutxrWvs9	SamsungE	Obermayr, Xperia Z1_10c9
Mar 30, 2020 @ 20:19:28.000	140.78.167.217	Mar 30, 2020 @ 18:29:19.000	dHN3Q3kB_AvUutxrHU	SamsungE	

Authentifizierte Benutzer

identity.realm.keyword: Descending	identity.username.keyword: Descending	Count
jku.at	k1456256	3
jku.at	k1455030	3



MAC: 4a:24:0b:c7:cc:74 Entrance Area SP 1 (2:40 PM) A1-de2c09	1 m
MAC: da:a1:19:64:ba:96 Google, Inc Entrance Area SP 1 (2:40 PM) AHL	1 m
MAC: 46:9a:7f:22:42:89 Entrance Area SP 1 (2:40 PM) AHL	1 m
MAC: bc:98:df:35:17:de Motorola Mobility Llc, a Lenovo Co Entrance Area SP 1 (2:40 PM) AHL	1 m
MAC: da:a1:19:24:b5:18 Google, Inc Entrance Area SP 1 (2:40 PM)	1 m
MAC: da:a1:19:32:5e:75 Google, Inc Entrance Area SP 1 (2:40 PM) AHL	1 m
MAC: 2e:85:de:be:d7:24 Entrance Area SP 1 (2:39 PM)	2 m
MAC: dc:85:de:be:d7:24 AzureWave Tech Inc Entrance Area SP 1 (2:39 PM)	2 m
MAC: 7e:d5:da:51:a1:f2 Entrance Area SP 1 (2:39 PM)	2 m
MAC: 80:0c:67:9a:fb:d2 Apple, Inc Entrance Area SP 1 (2:38 PM) OOE_HW_LN	3 m
MAC: da:a1:19:e5:b9:53 Google, Inc Entrance Area SP 1 (2:38 PM)	3 m
MAC: f6:61:44:a6:32:e3 Entrance Area SP 1 (2:38 PM)	3 m
MAC: 9a:9e:05:ef:a6:a4 Entrance Area SP 1 (2:38 PM)	3 m
MAC: da:a1:19:83:35:24 Google, Inc Entrance Area SP 1 (2:38 PM) AHL	3 m
MAC: da:a1:19:5f:68:ab Google, Inc Entrance Area SP 1 (2:38 PM) AHL	3 m
MAC: da:a1:19:37:c0:42 Google, Inc Entrance Area SP 1 (2:36 PM) AHL	5 m
MAC: 8e:17:f7:d8:d2:6d Entrance Area SP 1 (2:36 PM)	5 m
MAC: 16:88:11:c3:74:8a Entrance Area SP 1 (2:36 PM) TP-LINK_8880-5G, TP-LINK_8881, T...	5 m

491	AHL
55	BJNPSETUP
10	OOE_HW_LN
2	Seidlalmsprung
2	A1-de2c09
1	TP-LINK_8880_5G
1	TP-LINK_8881
1	TP-LINK_8880-5G
1	V8

Events

When	Who	What
14:44	d0:7f:a0:e9:d3:9b	Was Entrance Area SP 1
14:44	da:a1:19:d8:46:40	Was Entrance Area SP 1
14:44	e0:d4:e8:79:88:03	Was Entrance Area SP 1
14:44	74:1b:b2:63:d5:ef	Was Entrance Area SP 1
14:44	6a:ee:32:1b:13:e1	Was Entrance Area SP 1

EVENTS

ACM WiSec 2020

The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2020) was held as virtual event (hosted from Linz, Austria) from July 8 to July 10, 2020. ACM WiSec is the leading ACM and SIGSAC conference dedicated to all aspects of security and privacy in wireless and mobile networks and their applications, mobile software platforms, Internet of Things, cyber-physical systems, usable security and privacy, biometrics, and cryptography. ACM WiSec is a very competitive, high quality conference, and is very-well attended by industry, government, and academia to share information, network, explore ideas, and learn about emerging trends and today's hottest and most provocative cybersecurity topics.

Android Security Symposium

The Android Security Symposium brings together people from different backgrounds (academic, industry, rooting/exploiting community) who are interested in and actively working on Android device security. The event features exciting expert talks on various topics around Android and mobile device security and privacy. The symposium is an ideal platform to discuss current and upcoming security developments in Android and provides various networking opportunities.

In collaboration between JKU, University of Applied Sciences Upper Austria at Hagenberg and SBA Research, we organized the Android Security Symposium in 2015, 2017 (both in Vienna) and 2020 (as virtual event) as an event series bringing expert talks to a broad audience (attendance free of charge). We started the event series in 2015 with 14 invited talks by international speakers and 3 talks by PhD students, and were able to attract more than 150 participants. In 2017, we reached over 240 participants listening to the talks by our 17 international speakers. The virtual edition in 2020 peaked at roughly 200-250 concurrent live participants listening to the 9 expert talks.

General Chairs: Dr. Michael Roland, Prof. René Mayrhofer, Dr. Edgar Weippl (2015 and 2017)

MUM 2015

The 14th International Conference on Mobile and Ubiquitous Multimedia (MUM 2015) was held in Linz, Austria from November 30th and December 2nd, 2015. It was organized by the Department of Mobile Computing of the University of Applied Sciences Upper Austria and the Institute of Networks and Security in cooperation with ACM SIGCHI. The International Conference on Mobile and Ubiquitous Multimedia (MUM) is a leading annual international conference, which provides a forum for presenting the latest research results on mobile and ubiquitous multimedia. The conference brings together experts from both academia and industry for a fruitful exchange of ideas and discussion on future challenges, in a comfortable and effective single-track conference format.

TEDx TALK on future Digital Identities

A Digital Revolution of Identity by René Mayrhofer

How can we leverage digital identity authentication while protecting our privacy?
René Mayrhofer leads the Institute of Networks and Security (INS) at Johannes Kepler University in Linz and the Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile). His research encompasses computer security, mobile devices, network communication, and machine learning technologies. René combines all these elements to secure spontaneous, mobile interactions.

The Idea? A vision for a new identity system where individuals can preserve and protect their identity, even in today's world. An identity that remains intact without needing to carry a physical ID or mobile device. Such a revolution could also assist and protect people on the run, without contributing to mass surveillance in a totalitarian regime.

And his talk? ... How can we travel, check into hotels, or make payments without presenting an ID—while still safeguarding our privacy?

COURSES

BACHELOR’S DEGREE IN COMPUTER SCIENCE

We offer courses in the standard Bachelor of Computer Science to introduce fundamental methods and principles common to all modern operating systems, to convey basic network concepts using the ISO/OSI and Internet models with particular focus on practical protocols like TCP/IP and Ethernet, as well as important aspects in distributed systems and to introduce students to basic legal rules regarding computer programs and the Internet.

INS compulsory courses in the Bachelor’s degree in Computer Science

- Betriebssysteme VO + UE
- Computernetzwerke VO + UE
- Rechtsgrundlagen der Informatik VO
- Projektpraktikum PR

MASTER'S DEGREE IN COMPUTER SCIENCE - NETWORKS AND SECURITY

The protection of IT systems against internal or external attacks is a strategically important task for planning and operating such systems. Industry depends on security experts with a profound knowledge in computer science and especially computer networks. Graduates of this specialization towards **Networks and Security** as part of the Master curriculum Computer Science area have broad job opportunities ranging from the design, implementation, and administration of security strategies, the administration of systems, networks, and security policies, the application of cryptography as well as knowledge of the legal environment in the security area.

INS compulsory courses in the Master's program

- Computer Forensics and IT Law VO
- Introduction to IT Security VO
- Network Management KV
- Network Security KV
- Secure Code KV
- System Administration KV
- Systems Security KV
- Projects in Networks and Security PR
- Master's Thesis Seminar SE

CTF TEAM SIGFLAG

SIGFLAG is a CTF (capture the flag) team organized by students of JKU Linz. The team regularly participates in CTF security competitions and organizes IT security workshops. The Institute of Networks and Security supports the CTF team with infrastructure and several current and past employees participate in and help to organize SIGFLAG activities such as the Become A Hacker workshop.

AWARDS

Kepler Award 2022 for Excellence in Digital Teaching

Preisträger: Dr. Michael Roland
Lehrveranstaltung: Special Topics: Smart Cards & NFC

Die abrupte Umstellung von Präsenzbetrieb auf Distance-Learning im Sommersemester 2020 führte insbesondere bei Übungen und kombinierten Lehrveranstaltungen zu teils erheblichen Qualitätseinbußen – nicht zuletzt durch das (notgedrungene) hineinpressen von Präsenzformaten in ungeeignete Onlineangebote. Nachdem die Strategie für das darauffolgende Wintersemester einen erneuten Start im Präsenzbetrieb (jedoch mit absehbarer Umstellung auf Distanzbetrieb) vorsah, galt es die Fehler des vergangenen Semesters nicht zu wiederholen. Gleichzeitig bot sich dadurch die Chance, neuartige Lehrkonzepte zu erproben und die eigenen Kompetenzen im Bereich innovativer Lehrmethoden zu erweitern.

Ziel war es, ein Lehrkonzept für eine kombinierte Lehrveranstaltung mit Vortrags- und Übungsteilen zu erstellen, das sowohl in Form von Präsenzunterricht, als auch in reinem Online-Distanzbetrieb funktioniert, einen flexiblen Wechsel sowie Hybridformen zwischen diesen Unterrichtsmodi zulässt, und sowohl auf kleine als auch auf große Lehrveranstaltungen (also egal ob 15 oder 150 Studierende) anwendbar ist. Darüber hinaus sollte das Konzept durch Blended-Learning-Methoden die zeitliche Flexibilität der Studierenden steigern, um das Lehrveranstaltungsangebot auch für berufstätige Studierende attraktiver zu machen. Die Kombination aus zeitlicher Flexibilität und (soweit möglich und zulässig) Präsenzelementen, deckt zwei wesentliche Studierendenwünsche ab, die sich aus Studierendenfeedback des ersten Pandemiesemesters ergaben.

Das erarbeitete Konzept sollte zunächst an der Lehrveranstaltung “Special Topics: Smart Cards & NFC” (kleine Wahllehrveranstaltung mit ca. 10-25 Studierenden) erprobt und anschließend in weiteren Lehrveranstaltungen zur Anwendung kommen. Diese Lehrveranstaltung wurde in der Vergangenheit vorwiegend in Form eines Frontalvortrags abgehalten. Mittels Flipped-Classroom und Blended-Learning-Angeboten, bestehend aus eigens erarbeiteten, kurzen Lehrvideos, Moodle-Aufgaben (wie Minitests über Verständnis der Lehrinhalte, praxisorientierte Übungsbeispiele und Foren zur reflektierten Vorbereitung auf Diskussionsrunden) und Live-Diskussionsrunden wird diese Lehrveranstaltung in einen Mix aus asynchronen und synchronen Elementen überführt. Die Beurteilung erfolgt in drei Säulen (Wissenserwerb, praktische Anwendung, Diskussionskompetenz) und ermöglicht Studierenden damit Defizite einer Säule durch Exzellenz in anderen Säulen auszugleichen (z.B. auch mangelnde Teilnahme an Live-Diskussionen aufgrund beruflicher Terminkollisionen). Nach der erfolgreichen Umsetzung im Rahmen dieser Lehrveranstaltung wurde das Konzept für die Lehrveranstaltung “Einführung in Linux” übernommen, welche dadurch erfolgreich von einer Gruppengröße von ca. 30 Studierenden auf über 150 Studierende ausgedehnt werden konnte, ohne ihren interaktiven Charakter zu verlieren.

WISSENSCHAFTSPREIS 2017

Preisträger: Muhammad Muaaz
Dissertation: Implicit Biometric Authentication for Smartphones

Smartphones bieten eine Reihe von Services, die sensible Daten beinhalten, beispielsweise Online-Banking, Fotodatenbanken oder Online-Handel. Aus diesem Grund werden neue biometrische Authentifizierungen für Smartphones entwickelt - diese beeinträchtigen aber oft die Benutzerfreundlichkeit und lassen durch das Einbetten von neuer Sensortechnologie die Preise für Smartphones nach oben schnellen. Die Dissertation von Muhammad Muaaz präsentiert eine Lösung für dieses Problem. In der Arbeit werden Methoden zur Authentifizierung vorgestellt, die auf kontinuierliche biometrische Daten zurückgreifen, basierend auf alltäglichen Aktivitäten der Benutzer:in. Der Begriff der fortlaufenden impliziten biometrischen Authentifizierung wird hier definiert als die Fähigkeit, Smartphone-Benutzer:innen unauffällig und kontinuierlich anhand der Aktivitäten authentifizieren zu können, die die Benutzer:innen ohnehin in ihrem Alltagsleben ausführen würden. In dieser Arbeit wurden biometrische Authentifizierungsmethoden für den Gang und die Sprache untersucht, die die Identität einer Person überprüfen können, ohne dass zum Zeitpunkt der Authentifizierung explizite Benutzerinteraktionen erforderlich sind.

ADOLF-ADAM-INFORMATIKPREIS 2016

Preisträger: Martin Hengstberger
Masterarbeit: Wie entkommt man der NSA? - Daten am Handy verstecken

Der Adolf-Adam-Informatikpreis wird jährlich von der JKU für die beste Informatik-Masterarbeit des vergangenen Studienjahres vergeben. Studierende stellen in allgemein verständlicher Form ihre Arbeit vor. Die Präsentationen vermitteln etwas von der Faszination der Informatik und zeigen, womit sich unsere Studierenden beschäftigen.

Bei einem Flug in die USA kann es passieren, dass die Einreisebehörden Reisende Handy und Laptop abnehmen, um sämtliche Daten, die sich darauf befinden, zu kopieren und an die Nationale Sicherheitsbehörde (NSA), den Auslandsgeheimdienst der USA, zuzuspielen. Der Frage, wie man sich vor einem derartigen Eindringen in die Privatsphäre schützen kann, hat der studierte Informatiker seine Masterarbeit an der JKU gewidmet. "Zusammengefasst geht es darum, dass die Daten, die sich auf den Geräten befinden, mithilfe eines Systems so versteckt werden, dass sie von den Behörden gar nicht erst gefunden werden", erklärt Hengstberger seine Arbeit.

COLLABORATION PARTNERS

- 3 Banken IT
- ACOnet
- AIT Austrian Institute of Technology
- Check Point Software Technologies
- CyberDanube - CD Security Technologies
- Dynatrace
- ekey biometric systems
- Energie AG
- FH OÖ Hagenberg
- Fraunhofer AISEC
- Google
- Kepler Universitätsklinikum
- NXP Semiconductors
- Österreichische Staatsdruckerei
- Primetals
- PWC
- Raiffeisen Software
- Sprecher Automation
- TU Darmstadt
- University of Cambridge
- University of Strathclyde
- WKO Oberösterreich

Contact / Impressum

Medieninhaber
Johannes Kepler Universität Linz
Institut für Netzwerke und Sicherheit
Univ.-Prof. Dr. René Mayrhofer
Altenberger Straße 69
4040 Linz / Austria
T +43 732 2468 4120
M office@ins.jku.at
W https://ins.jku.at

Herausgeber
René Mayrhofer
Michael Roland
Michael Sonntag

Organisation
Sabine Link
Severina Kehayova
Maximilian Kokalj

Bildmaterial
INS/JKU/raumpixel

Grafik & Design
nutshells.design

ISBN: 978-3-903480-08-7

Zitation: Mayrhofer, R., Roland, M., and Sonntag, M. (Eds.) (2024) *Networks and Security: 10 Years INS@JKU*, Johannes Kepler University Linz, ISBN 978-3-903480-08-7
https://doi.org/10.35011/978-3-903480-08-7