Markus Miettinen

Curriculum Vitae

☎ +49(0)6151 16 25339
✉ markus.miettinen@trust.tu-darmstadt.de
scholar.google.de/citations?user=mdixRsMAAAAJ

Biography

Markus Juhani Miettinen, (born May 20th, 1976 in Helsinki, Finland) obtained his M.Sc. in Computer Science in 2002 from the University of Helsinki, after which he pursued a career in industrial research at the Nokia Research Center in Helsinki, Finland and Lausanne, Switzerland. During this time he was involved in numerous international industrial research projects related to data mining methods and data analysis in log database systems of mobile cellular networks as well as large-scale contextual data analysis of mobile applications. In 2012, he joined the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany and in 2013 he became a member of the System Security Lab of the Department of Computer Science at the Technical University of Darmstadt, where he pursued his PhD studies. He also acted as the main representative of the System Security Lab in several international EU and nationally funded projects. After obtaining his doctorate from the Technical University of Darmstadt in 2018, he applied for and received an offer for the position of Professor of Practice at the Aalto University in Finland. Concurrently he was, however, also involved in establishing the OpenS3 laboratory, an open industry-sponsored research laboratory in the field of sustainable security and safety, and decided to continue his career in Germany at the Technical University of Darmstadt, as the technical manager of the OpenS3 Lab. As lab manager, he coordinates the research activities in the OpenS3 lab, overseeing projects with a total volume exceeding 3M € during the years 2020-2022. During his academic career, his research endeavours have been centred around the use of data analysis and data mining for realising user-friendly, secure and resilient applications in areas like mobile network management, context-based mobile applications and Internet of Things, in which areas he is an author of a number of highly-cited works. Apart from his academic competencies, he has also profound experience in the technology transfer of research findings into industrial applications. He is inventor or co-inventor of 19 granted international patents in ten patent families.

Education

2018 **Doktor Ingenieur (Dr.-Ing.)**, *Technical University of Darmstadt*, Germany, Dissertation title: *Context and communication profiling for IoT security and privacy: techniques and applications.*
grade: "very good", "magna cum laude"

2002–2003 **Postgraduate scholarship with the German Academic Exchange Service DAAD**, *Ruhr-Universität Bochum*, Germany, Ten-month study and research scholarship.
Studies focusing on IT-security at chair of Prof. Christoph Paar

2002 **Master of Science (computer science)**, *University of Helsinki*, Finland, Specialisation area: Distributed systems and data communications, Additional subjects: Mathematics and language technology.
MSc. Thesis title: *Security monitoring in mobile networks (Tietoturvan tarkkailu matkaviestinverkoissa)*

1995 **Prüfung der allgemeinen Hochschulreife**, *Deutsche Schule Helsinki*, Finland, grade average: 1.0.
Common matriculation examination for obtaining the right to university studies in Germany

Current Position

Since 2019 **Postdoctoral Researcher**, *Technical University of Darmstadt, System Security Lab*, Germany.
Senior researcher and Lab manager of the third-party-funded OpenS3 lab for sustainable security and safety

Experience

Vocational

2013–2018 **Research Assistant**, *Technical University of Darmstadt, System Security Lab*, Germany.
Researcher and project manager, work package leader and executive board representative in EU and national projects

2012–2013 **Research Assistant**, *Fraunhofer Institute for Secure Information Technology (SIT)*, Darmstadt, Germany.
Researcher and project manager, deputy team leader

2011–2012 **Senior Researcher**, *Nokia Research Center Lausanne*, Switzerland.
Researcher and project leader

2007–2010 **Senior Researcher**, *Nokia Research Center Helsinki*, Finland.
Researcher and project leader

2002–2007 **Research Engineer**, *Nokia Research Center Helsinki*, Finland.

1999–2002 **Trainee**, *Nokia Research Center Helsinki*, Finland.

1999 **Teaching assistant**, *University of Helsinki, Department of Computer Science*, Finland.

1997–1998 **IT service assistant**, *Tietopiiri Oy*, Helsinki, Finland.

Previous Work Experience

2020– **Open Research Lab for Sustainable Security and Safety (OpenS3)**, *Lab manager*, Ongoing, Third-party-funded open research laboratory on sustainable security and safety hosted by the System Security Lab of the Department of Computer Science with a total volume exceeding 3M € for the years 2020–2022 .
`http://www.opens3-lab.com/`

2020–2021 **TraceCORONA**, *Project leader.*
Developed an improved Diffie-Hellman key exchange-based contact tracing app to fight the COVID-19 pandemic providing improved security and privacy properties.
`http://tracecorona.de`

2017–2020 **Intel Collaborative Research Institute for Collaborative Autonomous and Resilient Systems (ICRI-CARS)**, *Member of research institute.*
`http://www.icri-cars.org/`

2017–2018 **IoT Sense**, *Project leader.*
Project sponsored by CISCO Systems on automated IoT device identification and anomaly detection based on communication profiling of IoT devices [36].

2012–2017 **Intel Collaborative Research Institute for Secure Computing (ICRI-SC)**, *Member of research institute.*
`http://www.icri-sc.org/`

2016–2018 **SUPERCLOUD**, *Work Package Leader, Executive Board Representative.*
Horizon 2020 research project funded by the European Union on Multi-cloud security [18] developing a virtualized "cloud-of-clouds" architecture providing a cloud-based middleware for network, compute and data storage services.
`https://supercloud-project.eu/`

2016–2018 **IoT Security Lab**, *Project leader.*
Several research projects on IoT device security focusing on profiling-based identification and machine learning-based anomaly detection of IoT devices [29, 30, 36]

2016–2017 **Wearable Fitness Trackers Security Analysis**, *Project supervisor.*
Hands-on-security analysis of a representative sample of more than 15 popular fitness tracker devices using both protocol and hardware reverse-engineering techniques [8, 6]

2015–2017 **SPLITCloud**, *Work Package Leader.*
Research project funded by the German ministry for education and resarch (BMBF) on Cloud Service security

2014–2017 **ConXpair**, *Project leader.*
Research project on the use of context information for establishing a secure pairing between IoT devices [26, 28, 31].

2014–2015 **ConXPoP**, *Project leader.*
Research project on the use of context information in security protocols for proofs-of-presence [25].

2012–2013 **ConXsense**, *Project leader.*
Co-ordination of a cross-disciplinary research effort involving sociological studies on security perceptions of users and implementation and execution of a contextual data collection-based evaluation of novel algorithms for estimating security-relevant context parameters [27].

2011–2012 **Mobile Data Challenge 2012 by Nokia**, *Programme committee member.*
Participation in the Technical Programme Committee and practical organisation of the Nokia Mobile Data Challenge 2012 (`http://research.nokia.com/mdc`). The challenge was targeted at the academic research community and attracted more than 500 researchers all around the world to participate in four different challenge categories (one open challenge and three dedicated challenges). The programme committee reviewed the challenge contributions and arranged a two-day scientific workshop presenting the best submissions to the challenge in conjunction with the Pervasive 2012 conference in Newcastle [19].

2011–2012 **Contextual Intelligence research**, *Project leader.*
Planning and co-ordination of the execution of a contextual intelligence research project involving the contributions of ca. ten researchers in four different teams in Europe and Asia, involving the integration and development of novel algorithms, application concepting, usability testing, software implementation and integration.

2009–2012 **Intuitive and Sensible Access Control (ISAC)**, *Research project.*
Innovation of algorithms and participation in the implementation of a proof-of-concept demonstration for Nokia N900 (awarded the best demonstration award at PerCom 2011 [10]) and N9 on using machine learning methods for assisting users of mobile devices to set-up and maintain security and privacy policies automatically or semi-automatically, initial main focus being on context information monitored by the mobile device [24, 10]. Initial Assessment and further development of algorithmic approach [11]. Development of technologies for enabling privacy-respecting detection of designated persons in the proximity [12].

2008–2010 **Mobile Financial Services project (MoFS)**, *Flexible Services research programme.*

Joint research collaboration with Tieto corporation, Nordea bank and Aalto University/TKK sponsored by Tekes, the Finnish funding agency for technology and innovation. Nokia's main contact person towards the MoFS project and member of the project's steering board. Also co-ordinated the preparation of Nokia Research Center project proposals for the continuation phase of the Flexible Services strategic research programme and the continuation planning of the MoFS project in the Services for the Real-Time Economy (SeRTE) programme.

2009–2010 **Tivit Mobile Certification Task Force**, *Industry collaboration.*

Joint task force co-ordinated by Tivit Oy, a corporation co-ordinating the research activities of the strategic centre of excellence in ICT (SHOK) sponsored by Tekes. The task force included the Finnish mobile operators, the Federation of Finnish Financial Services (Finanssialan keskusliitto) and Nokia. Participated as one of Nokia's representants in the task force's work, successfully advocating the adoption of Nokia Research Center's On-board Credentials (ObC) technology in the mobile certification solution driven by the task force to speed up the up-take of mobile signatures in the Finnish market.

2009–2010 **Call graphs project**, *Future Internet research programme, security work package.*

Joint research collaboration between Nokia Research Center, F-Secure Corporation and Aalto University/TKK funded by Tekes. Research work on machine learning methods to automatically classify samples of malware, utilising data extracted from the call graphs of malware samples.

2006–2007 **Privacy & Trust**, *Integrated project MobiLife*, EU IST-FP6.

Participated as one of Nokia's representatives in the EU project *MobiLife*. Worked on issues related to trust, privacy, policy management and enforcement [43]

2002–2006 **Audit Trail product**, *Nokia Reseach Center.*

Several projects undertaken by Nokia Research Center for Nokia Networks covering the concepting and proof-of-concept studies for implementing data mining algorithms for compressing log databases of cellular network management systems to improving their security monitoring capabilities for human network administrators. Participated in the development and technology transfer of algorithms which were incorporated in the implementation of Nokia Networks' Audit Trail security monitoring product.

2004–2005 **Mobile Security Monitoring (MoSu)**, *Nokia Research Center.*

Exploratory project investigating investigating the feasibility of security monitoring and intrusion detection systems for mobile devices.

2000–2001 **Unix Anomaly Detection System (UADS)**, *Nokia Reseach Center.*

Research project aimed at creating a proof-of-concept demonstrator for the application of Self-Organizing Map-based anomaly detection on UNIX system log databases for detecting intruders.

2000–2004 **Traffica Clustering and Anomaly Detection System (TCADS)**, *Nokia Research Center.*

Participated in a project undertaken by NRC for Nokia Networks studying the applicability of Self-Organizing Maps for anomaly detection of Real Time Traffic (RTT) report data for the Nokia Traffica product.

1999 **Neural Network Based Anomaly Detection in Telecommunications Network and Service Monitoring**, *Nokia Telecommunications*, Summer internship.

Module and integration testing of the NCADS neural network anomaly detection library developed by NRC for Nokia Telecommunications.

Awards

2017 Best Demo Award, ICDCS 2017 for Markus Miettinen, Samuel Marchal, Ibbad Hafeez, Tommaso Frassetto, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. "IoT Sentinel Demo: Automated Device-Type Identification for Security Enforcement in IoT". in: *Proc. 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017)*. Best poster/demo award. Atlanta, GA, USA: IEEE, June 2017. DOI: 10.1109/ICDCS.2017.284

2014 Best Paper Award, ASIACCS 2014 for Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, and N. Asokan. "ConXsense – Context Profiling and Classification for Context-Aware Access Control". In: *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)*. Best paper award. ACM. Kyoto, Japan, June 2014. DOI: 10.1145/2590296.2590337

2011 Best Demo Award, PerCom 2011 for A. Gupta, M. Miettinen, and N. Asokan. "Using context-profiling to aid access control decisions in mobile devices". In: *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. Best demo award. Mar. 2011, pp. 310–312. DOI: 10.1109/PERCOMW.2011.5766891

Grants

2022 One-year start-up grant (85.000 €) by the Pioneer Fund of ENTEGA and the Technical University of Darmstadt for the further development and productization of the DÏoT intrusion detection system based on federated machine learning [36].

Service to the Scientific Community

WiSec 2019 Tutorial and Workshop co-chair, 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks

Programme Committee Memberships - Conferences

NDSS 2023 Network and Distributed System Security Symposium (NDSS) 2023

NDSS 2022 Network and Distributed System Security Symposium (NDSS) 2022

NDSS 2021 Network and Distributed System Security Symposium (NDSS) 2021

WiSec 2022 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks

Programme Committee Memberships - Workshops

COSDEO 2020 7thWorkshop on Context System Design, Evaluation and Optimization

SIoT 2019 International Workshop on Secure Internet of Things 2019

COSDEO 2018 6thWorkshop on Context System Design, Evaluation and Optimization

IoTPTS 2017 3rdInternational Workshop on IoT Privacy, Trust, and Security

SIoT 2017 International Workshop on Secure Internet of Things 2017

IoTPTS 2016 2nd International Workshop on IoT Privacy, Trust, and Security

SIoT 2016 International Workshop on Secure Internet of Things 2016

IW5GS 2016 2nd International Workshop on 5G Security

SIoT 2015 International Workshop on Secure Internet of Things

IW5GS 1st IEEE International Workshop on 5G Security

IoTPTS 2015 Workshop on IoT Privacy, Trust and Security

SPME 2014 Workshop on Security and Privacy aspects of Mobile Environments

Service as Reviewer

-ACM Transactions on Design Automation of Electronic Systems

-ACM Transactions on Internet of Things

-ACM Transactions on Privacy and Security

-Computers & Security Journal (Elsevier)

-IEEE Internet of Things Journal

-IEEE Transactions on Dependable and Secure Computing

-IEEE Transactions on Information Forensics and Security

-IEEE Transactions on Mobile Computing

-IEEE Transactions on Network and Service Management

-Internet of Things Journal (Elsevier)

-Pervasive and Mobile Computing Journal (Elsevier)

-Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies

Supervision and Mentoring

2021 *Practical Analysis of User Traceability in Digital Contact Tracing Apps Using the Exposure Notification API of Google and Apple*, Joshua Kühlberg, B.Sc. Thesis, Technische Universität Darmstadt

2020 *End-to-End Private Neural Network*, Pascal Petsch, B.Sc. Thesis, Technische Universität Darmstadt

2019 *Defending against poisoning attacks in federated learning*, Phillip Rieger, M.Sc. Thesis, Technische Universität Berlin

2018 *Lyin' Alexa: Silent man-in-the-middle attack against virtual assistants* , Richard Mitev, MSc. Thesis, Technische Universität Darmstadt

2014 *Secure Context-based Zero-Interaction Pairing of Advanced Internet-of-Things Devices*, Majid Sobhani, MSc. Thesis, Technische Universität Darmstadt

Teaching

2021 Betriebssysteme (Operating Systems), lecture course

2020 Betriebssysteme (Operating Systems), lecture course

2019 Betriebssysteme (Operating Systems), lecture course

2019 System and IoT Security Seminar

2017–2018 Practical lab on System and IoT Security

2016 Seminar on System and IoT Security (Mobile Security)

Granted Patents

Inventor or co-inventor in 19 international granted patents in ten patent families.

1. Markus Miettinen and Kimmo Hätönen

TWI291109 "Method and apparatus for storing data records on a database system", Taiwanese patent, December 11th, 2007

KR100829977 "Method for ensuring the integrity of a data record set", Korean patent, May 19th, 2008

RU2351978 "Method for provision of data records set integrity", Russian patent, April 10th, 2009

---

2. Kimmo Hätönen, Albert Höglund, Markus Miettinen, Jyrki Berg, Kari Kulmala and Sampo Torikka

US7519860 "System, device and method for automatic anomaly detection", U.S. patent, April 14th, 2009

---

3. Kimmo Hätönen and Markus Miettinen

EP1490769 "Method and apparatus for compressing log record information", European patent, February 24th, 2010

DE60235503 "Verfahren und Vorrichtung zum Komprimieren von Protokollierungsaufzeichnungsinformationen", German patent, April 8th, 2010

US7778979 "Method and apparatus for compressing log record information", U.S. patent, August 17th, 2010

---

4. Markus Miettinen and Kimmo Hätönen

US8331904 "Apparatus and a security node for use in determining security attacks", U.S. patent, December 12th, 2012

CN101548506 "Apparatus and a security node for use in determining security attacks", Chinese patent, January 16th, 2013

EP2080317 "Apparatus and a security node for use in determining security attacks", European patent, November 21st, 2018

---

5. Markus Miettinen

US8397304 "Privacy management of data", U.S. patent, March 12th, 2013

---

6. Markus Miettinen and N. Asokan

US8621656 Markus Miettinen and N. Asokan, "METHOD AND APPARATUS FOR SELECTING A SECURITY POLICY", U.S. patent, December 31st, 2013

---

7. Markus Miettinen

US8880663 "METHOD AND APPARATUS FOR SHARING USER INFORMATION", U.S. patent, November 4th, 2014

US9055020 Markus Miettinen, Eugen Palnau and Jens Dissman, "METHOD AND APPARATUS FOR SHARING USER INFORMATION", U.S. patent, June 5th, 2015

---

8. Markus Miettinen, N. Asokan and Aditi Gupta

US88988793 "Method and apparatus for adjusting context-based factors for selecting a security policy", U.S. patent, November 24th, 2014

---

9. N. Asokan and Markus Miettinen

US9003486 "Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests", U.S. patent, April 7th, 2015

EP2805298 "Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests", European patent, January 23rd, 2019

---

10. Markus Miettinen

US9449175 Markus Miettinen, "METHOD AND APPARATUS FOR ANALYZING AND DETECTING MALICIOUS SOFTWARE", U.S. patent, September 20th, 2016

CN103038777 Markus Miettinen, "Method and apparatus for analyzing and detecting malicious software", Chinese patent, September 28th, 2016

Languages

Finnish	mother tongue	
German	native proficiency	
English	full professional proficiency	
Swedish	good	*fluent oral and writing skills*
Estonian	fair	*fluent oral skills*
French	basic	*basic oral skills*

Most Important Publications

1. Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. "IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT". in: *Proc. 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017)*. June 2017. DOI: 10.1109/ICDCS.2017.283
2. Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. "DÏoT: A Federated Self-learning Anomaly Detection System for IoT". in: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. July 2019, pp. 756–767. DOI: 10.1109/ICDCS.2019.00080
3. Thien Duc Nguyen et al. "FLAME: Taming Backdoors in Federated Learning". In: *Proc. 31st USENIX Security Symposium*. 2022
4. Markus Miettinen, N. Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. "Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices". In: *Proc. ACM Conference on Computer and Communications Security*. Scottsdale, AZ, USA: ACM, Nov. 2014. DOI: 10.1145/2660267.2660334
5. Samuel Marchal, Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and N. Asokan. "AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication". In: *IEEE Journal on Selected Areas in Communications* 37.6 (June 2019), pp. 1402–1412. ISSN: 1558-0008. DOI: 10.1109/JSAC.2019.2904364
6. Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, and N. Asokan. "ConXsense – Context Profiling and Classification for Context-Aware Access Control". In: *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)*. Best paper award. ACM. Kyoto, Japan, June 2014. DOI: 10.1145/2590296.2590337
7. Phillip Rieger, Thien Duc Nguyen, Markus Miettinen, and Ahmad-Reza Sadeghi. "DeepSight: Mitigating Backdoor Attacks in Federated Learning Through Deep Model Inspection". In: *Proceedings of the Network and Distributed System Security Symposium 2022 (NDSS 2022)*. San Diego, USA,

2022

8. Juha K. Laurila, Daniel Gatica-Perez, Imad Aad, Jan Blom, Olivier Bornet, Trinh Minh Tri Do, Olivier Dousse, Julien Eberle, and Markus Miettinen. "From big smartphone data to worldwide research: The Mobile Data Challenge". In: *Pervasive and Mobile Computing* 9.6 (2013). Mobile Data Challenge, pp. 752–771. ISSN: 1574-1192. DOI: http://dx.doi.org/10.1016/j.pmcj.2013.07.014. URL: http://www.sciencedirect.com/science/article/pii/S1574119213000965
9. Markus Miettinen, Thien Duc Nguyen, N. Asokan, and Ahmad-Reza Sadeghi. "Revisiting Context-Based Pairing in IoT". in: *Proceedings of the 55th Design Automation Conference (DAC)*. ACM, June 2018. DOI: 10.1145/3195970.3196106
10. Richard Mitev, Markus Miettinen, and Ahmad-Reza Sadeghi. "Alexa Lied to Me: Skill-based Man-in-the-Middle Attacks on Virtual Assistants". In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. Asia CCS '19. Auckland, New Zealand: ACM, 2019, pp. 465–478. ISBN: 978-1-4503-6752-3. DOI: 10.1145/3321705.3329842. URL: http://doi.acm.org/10.1145/3321705.3329842

Full List of Publications

[1] Hossein Fereidooni, Alexandra Dmitrienko, Phillip Rieger, Markus Miettinen, Ahmad-Reza Sadeghi, and Felix Madlener. "FedCRI: Federated Mobile Cyber-Risk Intelligence". In: *Proceedings of the Network and Distributed System Security Symposium 2022 (NDSS 2022)*. San Diego, USA, 2022.

[2] Thien Duc Nguyen et al. "FLAME: Taming Backdoors in Federated Learning". In: *Proc. 31st USENIX Security Symposium*. 2022.

[3] Phillip Rieger, Thien Duc Nguyen, Markus Miettinen, and Ahmad-Reza Sadeghi. "DeepSight: Mitigating Backdoor Attacks in Federated Learning Through Deep Model Inspection". In: *Proceedings of the Network and Distributed System Security Symposium 2022 (NDSS 2022)*. San Diego, USA, 2022.

[4] Hossein Fereidooni et al. "SAFELearn: Secure Aggregation for private FEderated Learning". In: *2021 IEEE Security and Privacy Workshops (SPW)*. 2021, pp. 56–62. DOI: 10.1109/SPW53761.2021.00017.

[5] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. "Peek-a-boo: I see your smart home activities, even encrypted!" In: *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2020, pp. 207–218.

[6] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Richard Mitev, Markus Miettinen, Anel Muhamedagic, et al. "Mind the GAP: Security & privacy risks of contact tracing apps". In: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. 2020, pp. 458–467.

[7] Richard Mitev, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. "LeakyPick: IoT Audio Spy Detector". In: *Annual Computer Security Applications Conference*. ACSAC '20. Austin, USA: Association for Computing Machinery, 2020, pp. 694–705. ISBN: 9781450388580. DOI: 10.1145/3427228.3427277. URL: https://doi.org/10.1145/3427228.3427277.

[8] Thien Duc Nguyen, Markus Miettinen, and Ahmad-Reza Sadeghi. "Long Live Randomization: On Privacy-Preserving Contact Tracing in Pandemic". In: *Proceedings of the 7th ACM Workshop on Moving Target Defense*. MTD'20. Virtual Event, USA: Association for Computing Machinery,

2020, pp. 1–9. ISBN: 9781450380850. DOI: 10.1145/3411496.3421229. URL: https://doi.org/10.1145/3411496.3421229.

[9] Thien Duc Nguyen, Phillip Rieger, Markus Miettinen, and Ahmad-Reza Sadeghi. "Poisoning attacks on federated learning-based IoT intrusion detection system". In: *Proc. Workshop Decentralized IoT Syst. Secur.(DISS)*. 2020, pp. 1–7.

[10] Samuel Marchal, Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and N. Asokan. "AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication". In: *IEEE Journal on Selected Areas in Communications* 37.6 (June 2019), pp. 1402–1412. ISSN: 1558-0008. DOI: 10.1109/JSAC.2019.2904364.

[11] Richard Mitev, Markus Miettinen, and Ahmad-Reza Sadeghi. "Alexa Lied to Me: Skill-based Man-in-the-Middle Attacks on Virtual Assistants". In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. Asia CCS '19. Auckland, New Zealand: ACM, 2019, pp. 465–478. ISBN: 978-1-4503-6752-3. DOI: 10.1145/3321705.3329842. URL: http://doi.acm.org/10.1145/3321705.3329842.

[12] Reham Mohamed, Terrence O'Connor, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. "HONEYSCOPE: IoT Device Protection with Deceptive Network Views," in: *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*. Ed. by E. Al-Shaer, J. Wei, K.W. Hamlen, and C. Wang. Springer, Oct. 2019. DOI: https://doi.org/10.1007/978-3-030-02110-8_9.

[13] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. "DÏoT: A Federated Self-learning Anomaly Detection System for IoT". In: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. July 2019, pp. 756–767. DOI: 10.1109/ICDCS.2019.00080.

[14] TJ O'Connor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. "HomeSnitch: Behavior Transparency and Control for Smart Home IoT Devices". In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '19. Miami, Florida: ACM, 2019, pp. 128–138. ISBN: 978-1-4503-6726-4. DOI: 10.1145/3317549.3323409. URL: http://doi.acm.org/10.1145/3317549.3323409.

[15] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. "HomeSnitch: Behavior Transparency and Control for Smart Home IoT Devices". In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '19. Miami, Florida: Association for Computing Machinery, 2019, pp. 128–138. ISBN: 9781450367264. DOI: 10.1145/3317549.3323409. URL: https://doi.org/10.1145/3317549.3323409.

[16] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and A. Selcuk Uluagac. "Peek-a-Boo: I see your smart home activities, even encrypted!" In: *ArXiv e-prints* (Aug. 2018). arXiv: 1808.02741 [cs.CR].

[17] M. Miettinen, P. C. van Oorschot, and A.-R. Sadeghi. "Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management". In: *ArXiv e-prints* (Aug. 2018). arXiv: 1808.03071 [cs.CR].

[18] Markus Miettinen and N. Asokan. "Ad-hoc key agreement: A brief history and the challenges ahead". In: *Computer Communications* 131 (2018). COMCOM 40 years, pp. 32–34. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2018.07.030. URL: http://www.sciencedirect.com/science/article/pii/S0140366418302007.

[19] Markus Miettinen, Thien Duc Nguyen, N. Asokan, and Ahmad-Reza Sadeghi. "Revisiting Context-Based Pairing in IoT". In: *Proceedings of the 55th Design Automation Conference (DAC)*. ACM, June 2018. DOI: 10.1145/3195970.3196106.

[20] Markus Miettinen and Ahmad-Reza Sadeghi. "Internet of Things or Threats?: On Building Trust in IoT (Keynote)". In: *Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis*. CODES '18. Turin, Italy: IEEE Press, 2018, 1:1–1:9. ISBN: 978-1-5386-5562-7. URL: http://dl.acm.org/citation.cfm?id=3283568.3283569.

[21] Hossein Fereidooni, Jiska Classen, Tom Spink, Paul Patras, Markus Miettinen, Ahmad-Reza Sadeghi, Matthias Hollick, and Mauro Conti. "Breaking Fitness Records Without Moving: Reverse Engineering and Spoofing Fitbit". In: *Research in Attacks, Intrusions, and Defenses*. Ed. by Marc Dacier, Michael Bailey, Michalis Polychronakis, and Manos Antonakakis. Springer International Publishing, 2017, pp. 48–69. ISBN: 978-3-319-66332-6.

[22] Hossein Fereidooni, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, and Mauro Conti. "Fitness Trackers: Fit for Health but Unfit for Security and Privacy". In: *The Second IEEE International Workshop on Safe, Energy-Aware, & Reliable Connected Health (CHASE-SEARCH)*. Philadelphia, Pennsylvania, USA, July 2017. DOI: 10.1109/CHASE.2017.54.

[23] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. "IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT". In: *Proc. 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017)*. June 2017. DOI: 10.1109/ICDCS.2017.283.

[24] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, Tommaso Frassetto, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. "IoT Sentinel Demo: Automated Device-Type Identification for Security Enforcement in IoT". In: *Proc. 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017)*. Best poster/demo award. Atlanta, GA, USA: IEEE, June 2017. DOI: 10.1109/ICDCS.2017.284.

[25] M. Lacoste, M. Miettinen, N. Neves, F. M. V. Ramos, M. Vukolic, F. Charmet, R. Yaich, K. Oborzynski, G. Vernekar, and P. Sousa. "User-Centric Security and Dependability in the Clouds-of-Clouds". In: *IEEE Cloud Computing* 3.5 (Sept. 2016), pp. 64–75. ISSN: 2325-6095. DOI: 10.1109/MCC.2016.110.

[26] Markus Miettinen, Jialin Huang, Thien Duc Nguyen, N. Asokan, and Ahmad-Reza Sadeghi. "POSTER: Friend or Foe? Context Authentication for Trust Domain Separation in IoT Environments". In: *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '16. Darmstadt, Germany: ACM, 2016, pp. 225–226. ISBN: 978-1-4503-4270-4. DOI: 10.1145/2939918.2942422.

[27] Trinh Minh Tri Do, Olivier Dousse, Markus Miettinen, and Daniel Gatica-Perez. "A probabilistic kernel method for human mobility prediction with smartphones". In: *Pervasive and Mobile Computing* 20 (2015), pp. 13–28. ISSN: 1574-1192. DOI: http://dx.doi.org/10.1016/j.pmcj.2014.09.001. URL: http://www.sciencedirect.com/science/article/pii/S1574119214001539.

[28] Markus Miettinen, N. Asokan, Farinaz Koushanfar, Thien Duc Nguyen, Jon Rios, Ahmad-Reza Sadeghi, Majid Sobhani, and Sudha Yellapantula. "I know where you are: Proofs of Presence resilient to malicious provers". In: *10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)*. Apr. 2015. DOI: 10.1145/2714576.2714634.

[29] Markus Miettinen, N. Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. "Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices". In: *Proc. ACM Conference on Computer and Communications Security*. Scottsdale, AZ, USA: ACM, Nov. 2014. DOI: 10.1145/2660267.2660334.

[30] Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, and N. Asokan. "ConXsense – Context Profiling and Classification for Context-Aware Access Control". In: *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)*. Best paper award. ACM. Kyoto, Japan, June 2014. DOI: 10.1145/2590296.2590337.

[31] Juha K. Laurila, Daniel Gatica-Perez, Imad Aad, Jan Blom, Olivier Bornet, Trinh Minh Tri Do, Olivier Dousse, Julien Eberle, and Markus Miettinen. "From big smartphone data to worldwide research: The Mobile Data Challenge". In: *Pervasive and Mobile Computing* 9.6 (2013). Mobile Data Challenge, pp. 752–771. ISSN: 1574-1192. DOI: http://dx.doi.org/10.1016/j.pmcj.2013.07.014. URL: http://www.sciencedirect.com/science/article/pii/S1574119213000965.

[32] Aditi Gupta, Markus Miettinen, N. Asokan, and Marcin Nagy. "Intuitive security policy configuration in mobile devices using context profiling". In: *Proceedings of the 2012 ASE International Conference on Social Computing (SocialCom 2012)*. IEEE, Sept. 2012. DOI: 10.1109/SocialCom-PASSAT.2012.60.

[33] Aditi Gupta, Markus Miettinen, Marcin Nagy, N Asokan, and Alexandre Wetzel. "PeerSense: Who is near you?" In: *2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE. Lugano, Switzerland: IEEE, 2012. ISBN: 978-1-4673-0906-6. DOI: 10.1109/PerComW.2012.6197553. URL: http://dx.doi.org/10.1109/PerComW.2012.6197553.

[34] A. Gupta, M. Miettinen, and N. Asokan. "Using context-profiling to aid access control decisions in mobile devices". In: *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. Best demo award. Mar. 2011, pp. 310–312. DOI: 10.1109/PERCOMW.2011.5766891.

[35] Yiyun Shen, M. Miettinen, P. Moen, and L. Kutvonen. "Privacy Preservation Approach in Service Ecosystems". In: *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2011 15th IEEE International*. Helsinki, Finland: IEEE, Aug. 2011, pp. 283–292. DOI: 10.1109/EDOCW.2011.59.

[36] Markus Miettinen and N. Asokan. "Towards Security Policy Decisions Based on Context Profiling". In: *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security*. AISec '10. Chicago, Illinois, USA: ACM, 2010, pp. 19–23. ISBN: 978-1-4503-0088-9. DOI: 10.1145/1866423.1866428.

[37] Perttu Halonen, Markus Miettinen, and Kimmo Hätönen. "Computer Log Anomaly Detection Using Frequent Episodes". In: *Artificial Intelligence Applications and Innovations III*. Ed. by L. Illiadis, I. Vlahavas, and M. Bramer. Vol. 296. IFIP Advances in Information and Communication Technology. Boston: Springer, 2009, pp. 417–422. DOI: 10.1007/978-1-4419-0221-4_49. URL: http://dx.doi.org/10.1007/978-1-4419-0221-4_49.

[38] Heikki Kokkinen, Mikko V. J. Heikkinen, and Markus Miettinen. "Post-Payment Copyright System versus Online Music Shop: Business Model and Privacy". In: *International Journal on Advances in Security* 2.2&3 (2009), pp. 112–128. URL: http://www.iariajournals.org/security/sec_v2_n23_2009_paged.pdf.

[39] A. Battestini, C. Del Rosso, A. Flanagan, and M. Miettinen. "Creating Next Generation Applications and Services for Mobile Devices: Challenges and Opportunities". In: *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*. 2007, pp. 1–4. DOI: 10.1109/PIMRC.2007.4394846. URL: http://dx.doi.org/10.1109/PIMRC.2007.4394846.

[40] Göran Schultz, Olivier Coutand, Ronald van Eijk, Johan Hjelm, Silke Holtmanns, Markus Miettinen, and Rinaldo Nani. "Enabling technologies for mobile services : the MobiLife book". In: Wiley, 2007. Chap. Privacy, Trust and Group Communications, pp. 185–225.

[41] Kimmo Hätönen, Mika Klemettinen, and Markus Miettinen. "Remarks on the Industrial Application of Inductive Database Technologies". In: *Constraint-Based Mining and Inductive Databases*. Vol. 3848. Lecture Notes in Computer Science. Springer, 2006, pp. 196–215. DOI: 10.1007/11615576_10.

[42] M. Miettinen, P. Halonen, and K. Hätonen. "Host-Based Intrusion Detection for Advanced Mobile Devices". In: *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA 2006)*. Vol. 2. IEEE Computer Society, Apr. 2006, pp. 72–76. DOI: 10.1109/AINA.2006.192. URL: http://doi.ieeecomputersociety.org/10.1109/AINA.2006.192.

[43] Kimmo Hätönen, Jean François Boulicaut, Mika Klemettinen, Markus Miettinen, and Cyrille Masson. "Comprehensive Log Compression with Frequent Patterns". In: *Data Warehousing and Knowledge Discovery*. Vol. 2737. Lecture Notes in Computer Science. 10.1007/978-3-540-45228-7_36. Springer Berlin / Heidelberg, 2003, pp. 360–370. URL: http://dx.doi.org/10.1007/978-3-540-45228-7_36.

[44] Kimmo Hätönen, Perttu Halonen, Mika Klemettinen, and Markus Miettinen. "Queryable lossless log compression". In: *Proceedings of the Second International Workshop on Knowledge Discovery in Inductive Databases, 22 September, Cavtat-Dubrovnik, Croatia*. Ed. by Jean-François Boulicaut and Saso Dzeroski. Rudjer Boskovic Institute, Zagreb, Croatia, 2003, pp. 70–79. ISBN: 953-6690-34-9. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7619&rep=rep1&type=pdf.