# Curriculum Vitæ: Nils Ole Tippenhauer


| | |
|---|---|
| Title: | PhD (Dr. Sc. ETH) |
| Email: | nils@tippenhauer.de |
| Contact No: | +49 681 302 71953 |
| Current Position: | Faculty, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany |
| Research Areas: | Physical-layer Security for Wireless Communications; Security of Cyber-Physical Systems; IoT Security |
| Citizenship: | Germany |
| Address: | Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany |


## Academic Employment History

| | |
|---|---|
| August 2018 – current | Faculty, CISPA Helmholtz Center for Information Security, Germany |
| April 2014 – July 2018 | Assistant Professor (tenure track), Information Systems Technology and Design Pillar, Singapore University of Technology and Design (established in collaboration with MIT) |
| January 2013 – March 2014 | Research Scientist, Advanced Digital Science Center, Singapore, Research Center of the University of Illinois at Urbana-Champaign |
| April 2012 – November 2012 | Postdoctoral Researcher, ETH Zurich, Switzerland |

## Academic Background

| | |
|---|---|
| 7/2007–3/2012 | PhD (Dr. Sc. ETH), Systems Security Group under Professor Srdjan Capkun, ETH Zurich. Title: "Physical-Layer Security Aspects of Wireless Localization" External committee members: N. Asokan, Christof Paar, Patrick Traynor |
| 10/2001–4/2007 | Dipl-Ing. Informatik Ingenieurwesen, Hamburg University of Technology, Germany. Thesis: "Design and Cryptanalysis of Multi-Precision Arithmetics on Smartcards using the 32-bit SmartMIPS Architecture", K-H Ditze Award for thesis 2007/08 Supervisor: Heike Neumann and Dieter Gollmann |
| 8/2004–7/2005 | One year of exchange studies at University of Waterloo, Ontario, Canada |

## Publications

Total number of peer-reviewed publications to date: 77. Citations (Google scholar): 7180, h-index: 43 (Last updated: June 10, 2024).

### Articles in Journals


[1] D. Berardi, N. O. Tippenhauer, A. Melis, M. Prandini, and F. Callegati, "Time sensitive networking security: Issues of precision time protocol and its implementation," *Cybersecur.*, vol. 6, no. 1, p. 8, 2023.

[2] X. Wang, X. Hou, R. Rios, N. O. Tippenhauer, and M. Ochoa, "Constrained proximity attacks on mobile targets," *ACM Trans. Priv. Secur.*, vol. 25, no. 2, 2022.

[3] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Key negotiation downgrade attacks on Bluetooth and Bluetooth Low Energy," *ACM Transactions on Privacy and Security (TOPS)*, Jun. 2020.

[4] R. Taormina, S. Galelli, H. Douglas, N. Tippenhauer, E. Salomons, and A. Ostfeld, "A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems," *Environmental Modelling & Software*, vol. 112, pp. 46 –51, 2019.

[5] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 1, no. 1, Jul. 2018.

[6] R. Taormina, S. Galelli, N. O. Tippenhauer, *et al.*, "The battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks," *Journal of Water Resources Planning and Management*, vol. 144, no. 8, Aug. 2018.

[7] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *Journal of Water Resources Planning and Management*, vol. 143, 5 2016.

[8] E. Wilhelm, S. Siby, Y. Zhou, X. J. S. Ashok, M. Jayasuriya, S. Foong, J. Kee, K. Wood, and N. O. Tippenhauer, "Wearable environmental sensors and infrastructure for mobile large-scale urban deployment," *Sensors*, vol. 16, no. 22, pp. 8111–8123, Nov. 2016.

[9] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," *Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, pp. 1–25, Dec. 2016.

[10] N. O. Tippenhauer, K. B. Rasmussen, and S. Capkun, "Physical-layer integrity for wireless messages," *Computer Networks*, vol. 109, no. 1, pp. 31–38, Nov. 2016.

[11] S. Čapkun, M. Čagalj, G. Karame, and N. O. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," *IEEE Transactions on Mobile Computing*, 2010.

## Conference Proceedings

[1] T. Schlüter, A. Choudhari, L. Hetterich, L. Trampert, H. Nemati, A. Ibrahim, M. Schwarz, C. Rossow, and N. O. Tippenhauer, "FetchBench: Systematic identification and characterization of proprietary prefetchers," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Jul. 2023.

[2] A. Bytes, P. H. N. Rajput, C. Doumanidis, N. O. Tippenhauer, M. Maniatakos, and J. Zhou, "FieldFuzz: In situ blackbox fuzzing of proprietary industrial automation runtimes via the network," in *Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Oct. 2023.

[3] A. Erba and N. O. Tippenhauer, "White-box concealment attacks against anomaly detectors for cyber-physical systems," in *Proceedings of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Springer, 2023, pp. 111–131.

[4] A. Ding, M. Chan, A. Hassanzadeh, N. O. Tippenhauer, S. Ma, and S. Zonouz, "Get your cyber-physical tests done! data-driven vulnerability assessment of robotic vehicle," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, 2023.

[5] A. Erba and N. O. Tippenhauer, "Assessing model-free anomaly detection in industrial control systems against generic concealment attacks," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2022.

[6] A. Ibrahim, H. Nemati, T. Schlüter, N. O. Tippenhauer, and C. Rossow, "Microarchitectural leakage templates and their application to cache-based side channels," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2022.

[7] H. Esquivel-Vargas, J. H. Castellanos, M. Caselli, N. O. Tippenhauer, and A. Peter, "Identifying near-optimal single-shot attacks on icss with limited process knowledge," in *Proceedings of Conference on Applied Cryptography and Network Security (ACNS)*, Springer, 2022, pp. 170–192.

[8] Y. Han, M. Chan, Z. Aref, N. O. Tippenhauer, and S. Zonouz, "Hiding in plain sight? on the efficacy of power side channel-based control flow monitoring," in *Proceedings of the USENIX Security Symposium (USENIX Security)*, Aug. 2022.

[9] D. Antonioli, N. O. Tippenhauer, K. Rasmussen, and M. Payer, "Blurtooth: Exploiting cross-transport key derivation in Bluetooth classic and Bluetooth low energy," in *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022.

[10] A. Alsoliman, G. Rigoni, M. Levorato, C. M. Pinotti, N. O. Tippenhauer, and M. Conti, "COTS drone detection using video streaming characteristics," in *Proceedings of International Conference on Distributed Computing and Networking (ICDCN)*, ACM, 2021, pp. 166–175.

[11] J. Wu, R. Wu, D. Antonioli, M. Payer, N. O. Tippenhauer, D. Xu, D. J. Tian, and A. Bianchi, "LIGHTBLUE: Automatic profile-aware debloating of Bluetooth stacks," in *Proceedings of the USENIX Security Symposium (USENIX Security)*, Aug. 2021.

[12] A. Erba, R. Taormina, S. Galelli, M. Pogliani, M. Carminati, S. Zanero, and N. O. Tippenhauer, "Constrained concealment attacks against reconstruction-based anomaly detectors in industrial control systems," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2020.

[13] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "BIAS: Bluetooth impersonation attacks," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2020.

[14] H. R. Ghaeini, N. O. Tippenhauer, and J. Zhou, "Zero residual attacks on industrial control systems and stateful countermeasures," in *Proceedings of the Conference on Availability, Reliability and Security*, ser. ARES '19, Canterbury, CA, United Kingdom: ACM, 2019, 80:1–80:10.

[15] H. R. Ghaeini, M. Chan, R. Bahmani, F. Brasser and, L. Garcia, J. Zhou, A.-R. Sadeghi, N. O. Tippenhauer, and S. Zonouz, "PAtt: Physics-based attestation of control systems," in *Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019.

[16] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "The KNOB is broken: Exploiting low entropy in the encryption key negotiation of bluetooth BR/EDR," in *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2019.

[17] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, "HADES-IoT: A practical host-based anomaly detection system for IoT devices," in *Proceedings of the Asia Conference on Information, Computer and Communications Security (ASIACCS)*, Jul. 2019.

[18] J. Giraldo, D. Urbina, A. Cárdenas, and N. O. Tippenhauer, "Hide and seek: An architecture for improving attack visibility in industrial control systems," in *Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS)*, Jun. 2019.

[19] A. Tambe, Y. L. Aung, R. Sridharan, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "Detection of threats to iot devices using scalable vpn-forwarded honeypots," in *ACM Conference on Data and Application Security and Privacy (CODASPY)*, Mar. 2019.

[20] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Nearby threats: Reversing, analyzing, and attacking google's 'nearby connections' on android," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, Feb. 2019.

[21] X. Wang, X. Hou, R. Rios, P. Hallgren, N. O. Tippenhauer, and M. Ochoa, "Location proximity attacks against mobile targets: Analytical bounds and attacker strategies," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Sep. 2018.

[22] R. Sridharan, R. R. Maiti, and N. O. Tippenhauer, "WADAC: Privacy-preserving anomaly detection and attack classification on wireless traffic," in *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Jun. 2018.

[23] A. Fakhreddine, N. O. Tippenhauer, and D. Giustiniano, "Design and large-scale evaluation of wifi proximity metrics," in *Proceedings of European Wireless*, May 2018.

[24] H. R. Ghaeini, D. Antonioli, F. Brasser, A.-R. Sadeghi, and N. O. Tippenhauer, "State-aware anomaly detection for industrial control systems," in *Proceedings of Security Track at the ACM Symposium on Applied Computing (SAC)*, Apr. 2018.

[25] R. Ranjan Maiti, S. Siby, R. Sridharan, and N. O. Tippenhauer, "Link-layer device type classification on encrypted wireless traffic with COTS radios," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Sep. 2017.

[26] J. H. Castellanos, D. Antonioli, N. O. Tippenhauer, and M. Ochoa, "Legacy-compliant data authentication for industrial control system traffic," in *Proceedings of the Conference on Applied Cryptography and Network Security (ACNS)*, Jul. 2017.

[27] M. Rocchetto and N. O. Tippenhauer, "Towards formal security analysis of industrial control systems," in *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS)*, Apr. 2017.

[28] Y. Meidan, M. Bohadana, A. Shabtai, J.-D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "ProfilIoT: A machine learning approach for iot device identification based on network traffic analysis (poster)," in *Proceedings of the Security Track at ACM Symposium on Applied Computing (SAC)*, Apr. 2017.

[29] E. Wilhelm, D. MacKenzie, Y. Zhou, L. Cheah, and N. O. Tippenhauer, "Evaluation of transport mode using wearable sensor data from 43,000 students," in *Proceedings of Transportation Research Board Annual Meeting (TRB)*, Jan. 2017.

[30] D. Urbina, J. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Oct. 2016.

[31] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver GPS spoofing detection: Error models and realization," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Dec. 2016.

[32] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Sep. 2016.

[33] M. Rocchetto and N. O. Tippenhauer, "CPDY: Extending the Dolev-Yao attacker with physical-layer interactions," in *Proceedings of the International Conference on Formal Engineering Methods (ICFEM)*, Oct. 2016.

[34] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Assessing the effect of cyber-physical attacks on water distribution systems," in *Proceedings of World Congress on Environmental & Water Resources (EWRI)*, May 2016.

[35] E. Wilhelm, N. O. Tippenhauer, Y. Zhou, and N. Zhang, "SENSg: Large-scale deployment of wearable sensors for trip and transport mode logging," in *Proceedings of Transportation Research Board Annual Meeting (TRB)*, Jan. 2016.

[36] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Simulation of cyber-physical attacks on water distribution systems with EPANET," in *Proceedings of Singapore Cyber Security Conference (SG-CRC)*, Jan. 2016.

[37] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cárdenas, "Attacking fieldbus communications in ICS: Applications to the SWaT testbed," in *Proceedings of Singapore Cyber Security Conference (SG-CRC)*, Jan. 2016.

[38] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "UWB rapid-bit-exchange system for distance bounding," in *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Jun. 2015.

[39] N. O. Tippenhauer, W. G. Temple, A. H. Vu, B. Chen, D. M. Nicol, Z. Kalbarczyk, and W. Sanders, "Automatic generation of security argument graphs," in *Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing (PRDC)*, Nov. 2014.

[40] A. H. Vu, N. O. Tippenhauer, B. Chen, D. M. Nicol, and Z. Kalbarczyk, "CyberSAGE: A tool for automatic security assessment of cyber-physical systems," in *Proceedings of the Conference on Quantitative Evaluation of SysTems (QEST)*, Sep. 2014.

[41] W. G. Temple, B. Chen, and N. O. Tippenhauer, "Delay makes a difference: Smart grid resilience under remote meter disconnect attack," in *Proceedings of the IEEE Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2013.

[42] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2013.

[43] N. O. Tippenhauer, D. Giustiniano, and S. Mangold, "Toys communicating with LEDs: Enabling toy cars interaction," in *Proceedings of Consumer Communications and Networking Conference (CCNC)*, IEEE, 2012, pp. 48–49.

[44] D. Giustiniano, N. O. Tippenhauer, and S. Mangold, "Low-complexity visible light networking with led-to-led communication," in *Proceedings of IFIP Wireless Days*, 2012.

[45] A. Ranganathan, N. O. Tippenhauer, B. Skoric, D. Singelé, and S. Čapkun, "Design and implementation of a terrorist fraud resilient distance bounding system," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, ser. Lecture Notes in Computer Science, Springer, 2012.

[46] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011.

[47] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Čapkun, "Investigation of signal and message manipulations on the wireless channel," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2011.

[48] N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Čapkun, "Attacks on public WLAN-based positioning," in *Proceedings of the ACM Conference on Mobile Systems, Applications and Services (MobiSys)*, 2009.

[49] N. O. Tippenhauer and S. Čapkun, "ID-based secure distance bounding and localization," in *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2009.

## Workshop Proceedings

[1] T. Walita, A. Erba, J. H. Castellanos, and N. O. Tippenhauer, "Blind concealment from reconstruction-based attack detectors for industrial control systems via backdoor attacks," in *Proceedings of the Cyber-Physical System Security Workshop (CPSS), co-located with ASIACCS*, Jul. 2023.

[2] A. Erba, A. Müller, and N. O. Tippenhauer, "Security analysis of vendor implementations of the opc ua protocol for industrial control systems," in *Proceedings of the Workshop on CPS & IoT Security and Privacy (CPSIoTSec), co-located with CCS'22*, 2022, 1–13.

[3] N. O. Tippenhauer, B. Chen, D. Mashima, and D. M. Nicol, "Vbump: Securing ethernet-based industrial control system networks with VLAN-based traffic aggregation," in *Proceedings of the Workshop on CPS&IoT Security and Privacy (CPSIoTSec)*, ACM, 2021, pp. 3–14.

[4] F. Turrin, A. Erba, N. O. Tippenhauer, and M. Conti, "A statistical analysis framework for ics process datasets," in *Proceedings of the Joint Workshop on CPS & IoT Security and Privacy (CPSIOTSEC'20)*, Nov. 2020.

[5] A. Siddiqi, N. O. Tippenhauer, D. Mashima, and B. Chen, "On practical threat scenario testing in an electric power ics testbed," in *Proceedings of the Cyber-Physical System Security Workshop (CPSS), co-located with ASIACCS*, Jun. 2018.

[6] N. Govil, A. Agrawal, and N. O. Tippenhauer, "On ladder logic bombs in industrial control systems," in *Proceedings of the Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS), co-located with ESORICS*, Sep. 2017.

[7] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, and N. O. Tippenhauer, "Gamifying ICS security training and research: Design, implementation, and results of S3," in *Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (SPC-CPS), co-located with CCS*, Nov. 2017.

[8] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "IoTScanner: Detecting privacy threats in IoT neighborhoods," in *Proceedings of the Workshop on IoT Privacy, Trust, and Security (IoTPTS), co-located with ASIACCS*, Apr. 2017.

[9] J. Guarnizo, A. Tambe, S. S. Bunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "SIPHON: Towards scalable high-interaction physical honeypots," in *Proceedings of the Cyber-Physical System Security Workshop (CPSS), co-located with ASIACCS*, Apr. 2017.

[10] H. Ghaeini and N. O. Tippenhauer, "HAMIDS: Hierarchical monitoring intrusion detection system for industrial control systems," in *Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (SPC-CPS), co-located with CCS*, Oct. 2016.

[11] D. Antonioli, A. Agrawal, and N. O. Tippenhauer, "Towards high-interaction virtual ICS honeypots-in-a-box," in *Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (SPC-CPS), co-located with CCS*, Oct. 2016.

[12] A. Mathur and N. O. Tippenhauer, "SWaT: A water treatment testbed for research and training on ICS security," in *Proceedings of Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater)*, Apr. 2016.

[13] N. O. Tippenhauer, M. Ochoa, and A. Mathur, "Water treatment, distribution, and electric power testbeds for research in the design of secure interdependent critical infrastructures," in *Proceedings of Workshop on Security and Resilience of Cyber-Physical Infrastructures (SERECIN)*, Apr. 2016.

[14] X. Dong, S. Jauhar, W. G. Temple, B. Chen, Z. Kalbarczyk, W. H. Sanders, N. O. Tippenhauer, and D. M. Nicol, "The right tool for the job: A case for common input scenarios for security assessment," in *Proceedings of Workshop on Graphical Models for Security (GraMSec)*, Jun. 2016.

[15] D. Antonioli and N. O. Tippenhauer, "MiniCPS: A toolkit for security research on CPS networks," in *Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (SPC-CPS), co-located with CCS*, Oct. 2015.

[16] B. Chen, Z. Kalbarczyk, D. M. Nicol, W. H. Sanders, R. Tan, W. G. Temple, N. O. Tippenhauer, A. H. Vu, and D. K. Yau, "Go with the flow: Toward workflow-oriented security assessment," in *Proceedings of New Security Paradigm Workshop (NSPW)*, 2013.

[17] M. Kuhn, H. Luecken, and N. O. Tippenhauer, "UWB impulse radio based distance bounding," in *Proceedings of the Workshop on Positioning, Navigation and Communication (WPNC)*, 2010.

## Book Chapters

[1] N. O. Tippenhauer, "Design and realization of testbeds for security research in the industrial internet of things," in *Security and Privacy Trends in the Industrial Internet of Things*, Springer, 2019, pp. 287–310.

[2] N. O. Tippenhauer, "Attack detection for CPS," in *Encyclopedia of Cryptography, Security and Privacy*, Springer, 2021.

## Selected Technical Reports

[1] C. Troncoso, M. Payer, J.-P. Hubaux, *et al.*, *Decentralized privacy-preserving proximity tracing*, Technical report on arXiv cs.CR 2005.12273, 2020.

## Patents Granted

[1] D. Giustiniano, S. Mangold, and N. O. Tippenhauer, *Visible light communication with flickering prevention*, US Patent 8,873,965, Oct. 2014.

[2] N. O. Tippenhauer, R. R. Maiti, S. Sandra, and R. Sridharan, *Apparatus and method for monitoring a wireless network*, US Patent 10,567,243, Feb. 2020.

[3] A. Mathur, S. Adepu, S. Shrivastava, M. A. Kaung, N. Tippenhauer, and G. Sabaliauskaite, *Defense system and method against cyber-physical attacks*, US Patent 11,431,733, Aug. 2022.

### Patents pending

1. "Communication Method And Apparatus For An Industrial Control System", Martin Ochoa and Nils Ole Tippenhauer and John Henry Castellanos and Daniele Antonioli, PCT application no: PCT/SG2018/050326

2. "Industrial Control Systems Anomaly Detection by Learning Algorithms with Physical Process Features", Nils Ole Tippenhauer and Hamid Reza Ghaeini, Singapore provisional patent application no: 10201801597P

3. "Method And Apparatus For Determining An Identity Of An Unknown Internet-Of-Things (IoT) Device In A Communication Network", Martin Ochoa and Nils Ole Tippenhauer and Juan Guarnizo and Asaf Shabtai and Yuval Elovici and Yair Meidan and Michael Bohadana, PCT application no: PCT/SG2018/050089

4. "Computer-Implemented Method And Data Processing System For Testing Device Security", Yuval Elovici and Nils Ole Tippenhauer and Shachar Siboni and Asaf Shabtai, US Patent App. 16/347,493

## Invited Talks

1. "Out of control: Attacking and Defending Industrial Control Systems", Keynote at DefMal Workshop, June 2024

2. "Quo Vadis Bluetooth? Security by Transparency", vision talk at Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), May 2024

3. "A Tale of Stale (Data) – Sensor Deprivation Attacks", invited talk at ELLIIT Symposium, April 2024

4. "MTD via Adaptive Control in Cyber-Physical Systems", Workshop on Moving Target Defense (MTD), November 2023

5. "Déjà Vu? Challenges and Opportunities for AM security from an ICS perspective", Workshop on Additive Manufacturing (3D Printing) Security (AMSec), November 2022

6. "Oh What A Tangled Web We Weave – Securing ICS Networks", talk at workshop on Critical Infrastructure and Manufacturing System Security (CIMSS), June 2022

7. "Through the looking glass, and what we found there", talk at Dagstuhl seminar 22171 'Digital Twins for Cyber-Physical Systems Security', April 2022

8. "The Quest for Industrial Host Security", keynote at CSS 2021
9. " Process-aware Attack Detection in Cyber-Physical Systems", talk at University of Queensland, Australia, July 2021
10. "Process-aware Attack Detection in Cyber-Physical Systems – The good, the bad, and the ugly", keynote at DSN Workshop on Data-Centric Dependability and Security (DCDS), June 2021
11. "Trials and Tribulations: Securing Industrial Control Systems", invited talk at GT SSLR (Systems and network security working group of the GDR Sécurité), May 2021
12. "Trust, but verify? Perspectives On Industrial Device Security", keynote at 6th ACM Cyber-Physical System Security Workshop, October 2020
13. "IT+OT=IoT? On Security for Industrial Control Systems", invited keynote at 12th Workshop on RFID and IoT Security (RFIDSec), Hong Kong, November 2016
14. "Challenges and Opportunities in Practical Industrial Control System Security Research", invited talk at SVA group of Prof. Dieter Gollmann, Hamburg University of Technology, August 2015

### CVEs

- CVE-2022-20361 (based on **antonioli22blurtooth**)
- CVE-2020-25235 (based on BSc thesis of Max Bäumler)
- CVE-2020-15802 (based on **antonioli22blurtooth**)
- CVE-2020-10135 (based on **antonioli20bias**)
- CVE-2019-9506 (based on **antonioli19knob**)

## Research Activities

Involved as principle investigator (PI) or co-PI in research projects with total funding of more than 20M SGD. Major contributions to writing grant proposals of ResilIoT, ASPIRE, NSE, and SAFE.

### Research Projects

1. "Proseca: Proactive Security Chain for Automotive", role: PI, 10/2023-9/2026, BMWK
2. "ASRIOT: Automatisierte Sicherheitsanalyse von RTOS und MCU basierter IoT Firmware", role: project coordinator, PI; 04/2023-3/2026, funding BMBF
3. "Konstruktiv adaptive Mobilität bei Leichtfahrzeugen durch dynamische Fahrzeuganpassung mit KI-basierter multisensorischer Umfelderkennung", role: co-PI, 04/2019-04/2022, funding BMBF
4. "Location Privacy in Smart Cities" (collaboration with ZJU), role: PI, 7/2017–7/2018, funding: SUTD/ZJU grant
5. "ReSILIoT: Research and Security Innovation Lab for Internet of Things", role: Co-PI, 9/2015–9/2018, funding: Ministry of Defence
6. "ASPIRE: Advancing Security of Public Infrastructure using Resilience and Economics", role: Co-PI, 1/2015–12/2018, funding: National Research Foundation
7. "National Science Experiment", role: Co-PI, 2/2015–12/2017, funding: National Research Foundation

8. "SAFE: Security Assessment and Forensic Examination", role: PI, 8/2014–7/2017, funding: SUTD startup grant

9. "CYPRO: Cyber-Physical Protection", role: co-PI, 10/2014–9/2016, funding: Ministry of Defence

### Events Organized

1. Program Co-Chair: 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), 2023

2. Program Co-Chair: 19th International Conference on Applied Cryptography and Network Security (ACNS), 2021

3. Co-Chair: 7th ACM Cyber-Physical System Security Workshop (CPSS 2021), co-located with AsiaCCS, 2021

4. Chair: ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC), co-located with CCS, 2018-2019

5. Chair: SCy-Phy Systems week'17: Think-In event and Singapore Security Showdown event, SUTD, 2017

6. Co-Chair: SCy-Phy Systems week'16: Think-In event and Singapore Security Showdown event, SUTD, 2016

7. Co-Chair: SCy-Phy Systems week'15: Think-In event and ICS security hands-on, SUTD, 2015

8. Publicity Committee: Conference on Quantitative Evaluation of SysTems (QEST), 2014

9. Publicity Co-Chair: Automation Protocols Security in Cyber-Physical Systems (APS-CPS), 2016

## Research Outcomes

- Co-designer of *MiniCPS*, MiniCPS is a lightweight simulator for accurate network traffic in an industrial control system, with basic support for physical layer interaction
- Co-author of *APE: Attacker Profile Examiner* tool for attacker models
- Design and implementation of first working UWB-based radio distance bounding system
- Co-inventor of COTS-GPS receiver-based GPS spoofing detection
- Co-developer of Cyber Security Argument Graph Evaluation tool (CyberSAGE), now licensed to third parties by ADSC

## Service

### Journal Reviewer

1. IEEE/ACM Transactions on Networking (ToN)

2. ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)

3. IEEE Security & Privacy

4. Elsevier Computer Networks

5. IEEE Sensors

6. IEEE Transactions on Information Forensics & Security
7. IEEE Communications Letters
8. IEEE Transactions on Dependable and Secure Computing
9. IEEE Transactions on Industrial Informatics
10. IEEE Transactions on Wireless Communications
11. Wireless Networks (WINE), Springer
12. ACM Transactions on Internet Technology
13. Elsevier Computers & Security
14. ACM Transactions on Privacy and Security (former TISSEC)
15. Elsevier Future Generation Computer Systems
16. ACM Computing Surveys
17. IEEE Transactions on Mobile Computing
18. IEEE/ACM Transactions on Networking
19. Transactions on Emerging Telecommunications Technologies
20. Journal of Field Robotics
21. KSII Transactions on Internet and Information Systems
22. Journal of Computer Security
23. MILCOM

### Technical Program Committee Member

1. USENIX Security Symposium, 2020-24
2. ACM Conference on Computer and Communications Security (CCS), 2018-2019, 2022
3. ACM AsiaCCS, 2021-22
4. International Conference on Applied Cryptography and Network Security (ACNS), 2019-2021, 2024
5. European Symposium on Research in Computer Security (ESORICS), 2017-2021, 2023
6. International Conference on Critical Information Infrastructures (CRITIS), 2019-22
7. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2017-2022
8. GI Sicherheit, 2022
9. Conference on Cryptology and Network Security (CANS), 2017
10. ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC), 2016-2022 (co-located with CCS, renamed to CPSIoTsec in'20)
11. Cyber-Physical System Security Workshop (CPSS), 2015-2023 (co-located with ASIA-CCS)

12. IEEE Workshop on the Internet of Safe Things (SafeThings), 2020-2023 (co-located with S&P)
13. Workshop on Cyber-Physical Systems Security (CPS-Sec) co-located with CNS, 2016-2017, 2019, 2022-2023
14. Workshop on Cyber Security for Intelligent Transportation Systems (CSITS), 2018-2019 (co-located with Esorics)
15. Workshop on Security and Privacy in the Internet of Things (SePrIoT), 2018
16. Workshop on Industrial Internet of Things Security (WIIoTS), 2018
17. Workshop on Security for Embedded and Mobile Systems (SEMS), 2017
18. Singapore-Cyber Security R&D Conference (SG-CRC) 2016 + 2017
19. International Symposium on High Assurance Systems Engineering (HASE), 2017
20. Workshop on RFID Security and Privacy (RFIDsec), 2016
21. IFIP International Information Security and Privacy Conference (IFIP SEC), 2015 + 2016
22. International Conference on Network and System Security (NSS), 2014 +2016
23. International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA) 2016
24. International Workshop on Authentication Techniques (AuthTech), 2016
25. Smart City Security and Privacy Workshop (SCSP-W), co-located with CPS week, 2016

## Committee Work and other Service

### SUTD

At SUTD, I was member of the following committees

- Graduate Studies Committee, 2017–current
- Faculty Search Committee, 2016–2017
  Responsible for review of applications, recommendations to Department Head. Reviewed over 390 applications.
- Master of Science in Secure Design committee member, 2016-current
  Co-designer of the first Masters' programme in the department (curriculum, administrative process). Review and selection of applications.
- Representative of ISTD in the Learning Research Governance Sub-Committee
- ISTD Labs committee member, 2015-2016.
  Design and procurement of LEETlab, used for teaching 50.012 Networks and 50.020 Security.

In addition, I supported SUTD as follows:

- Leading and coordinating efforts to maintain and modernize the department's website (2014-now)
- Organizer of an inter-department end-of-term social event for faculty members, with 3 events each year since December 2014.
- Evaluation committee member for procurement efforts for more than 6.7M SGD since 2014.

# Teaching

## CISPA/UdS

- WS 2024: Core lecture "Security"
- SS 2023 Advanced lecture "Physical-Layer Security"
- SS 2023 Proseminar "Physical-Layer Security"
- WS 2022: Seminar "Industrial Control System Security"
- SS 2022: Advanced lecture "Physical-Layer Security"
- WS 2021: Core lecture "Security"
- WS 2020: Core lecture "Security"
- SS 2020: Advanced lecture "Physical-Layer Security"
- WS 2019: Core lecture "Security"
- SS 2019: Advanced lecture "Physical-Layer Security"
- SS 2019: Proseminar "Hacking"
- WS 2018: Proseminar "Physical-Layer Security"

## SUTD

Designed and implemented two undergraduate classes at SUTD, 50.012 Networks (Term 6), and 50.020 Security (Term 7). Both classes are electives, and form the "Security and Communications" track. Per week: 2x1.5h interactive lectures and one 2h exercise in the lab. Total term duration: 14 weeks (including recess week).

- 50.012 Networks: taught Spring and Fall 2015, Fall 2016, and Fall 2017.
  Average course rating in evaluation: 4.3/5. Average instructor rating 4.6/5.
- 50.020 Security: taught Fall 2014, Spring 2016, Spring 2017, Spring 2018.
  Average course rating in evaluation: 4.38/5. Average instructor rating 4.55/5. The security class contains a capture-the-flag competition, with student-made challenges to apply security concepts

Co-designer of overall curriculum for the Master's in Security by Design (MSSD) program at SUTD.

## ETH Zurich

- 4 years as Teaching Assistant of the Systems Security graduate class
- 1 year as Teaching Assistant of the Security of Wireless Networks graduate class

## Other classes

Other short courses developed and delivered:

- "Security Attacks", 4 hours, developed for Swiss high school students
- "Cybersecurity Foundations Class", 8 hours, developed for Defence Science and Technology Agency, Singapore
- "Cyber-Security for Industrial Control Systems", 4 hours, developed for Keppel Offshore Marine, Singapore

## Supervised Students and Researchers

### Postdoctoral Researchers

- John H. Castellanos, Oct 2021 to Mar 2024
- Hamid Ghaeini, Oct 2020 to Dec 2022
- Wang Xueou, Nov 2017 to July 2018
- Yan Lin Aung, Nov 2017 to July 2018
- Rajib Ranjan Maiti, July 2016 to July 2018
- Marco Roccetto, Sept. 2015–Sept. 2016, next Research Scientist at University of Luxembourg
- Liang He, Sept 2014–Nov 2014, next Research Fellow at University of Michigan, USA

### PhD Students

- Simeon Hoffmann, from Sept 2022 to date
- Yu-De Ling, from January 2022 to date
- Till Schlüter, from June 2020 to date
- Alessandro Erba, from May 2019 to April 2024, now PostDoc at KIT with Christian Wressnegger
- Daniele Antonioli, from September 2015, successfully defended in July 2019, next: postdoc with Mathias Payer. now: Faculty at EURECOM
- Hamid Ghaeini, from January 2015, successfully defended in July 2019, next postdoc with Michael Backes

### Bachelor's Thesis (Co-)Supervision

- Gleb Rostanin, "Embedded Intrusion Detection for Automotive Ethernet", UdS, 2024
- Christian Schumacher, "'Security Analysis of IoT Devices and Vulnerable User Notification", UdS, 2022
- Ole Heydt, "Systematic Evaluation of Stealthy Attacks against Quadcopter Drones", UdS, 2022
- Tim Walita, "Backdoor Attacks on Autoencoder-based Attack Detectors for ICS", UdS, 2022
- Konstantin Holz, "Security Assessment of IPv6 Implementations of Home Routers", UdS, 2021
- Amir Heinisch, "Leverage Trusted Execution Environments to implement trustworthy motor controls", UdS, 2021
- Max Bäumler, "Security Analysis of the Siemens LOGO! 8 Ecosystem", UdS, 2020
- Nils Glörfeld, "Design and Implementation of a Control Logic Manipulation Attack on a Linux-based PLC", UdS, 2020
- Christian Geldermann, "Real-time Manipulation of Industrial Traffic with Constrained Embedded Devices", UdS, 2019

### Bachelor's Thesis Co-Reviewer

- Jorim Bechtle, "New Hardware – Old Vulnerabilities: Software-based Side-channel Attacks on RISC-V Architecture", UdS, 2022
- Joshua Sonnet, "Towards Decentralised Access Control in Thread-based Home IoT", UdS, 2022
- Robin Gärtner, "Implementing Private Set Intersections", UdS, 2021
- Robin Jacobi, "Researching possible reasons for differences in response time in the German ID Card", UdS, 2021
- Mara Schulze, "Identifying Cryptojacking Malware in the Sandnet Analysis Platform", Uds, 2021

### Masters' Thesis (Co-)Supervision

- Leon Barth, "Feasibility of IDS in Automotive Systems using the NXP S32G Platform", UdS, 2024
- Sahil Sihag, "ArduFuzzer", In Situ Fuzzing of Remote Firmware with Coverage Feedback, UdS, 2024
- Marco Schichtel, TBD, UdS, 2024
- Omar Mansour, "Securing SCADA Communication Systems", UdS, 2024
- Farah ElShenawy, "Industrial Control System Network Anomaly Detection", UdS, 2023
- Trupti Ravikumar Koushik, "Key Management for Secu-Box", UdS, 2023
- Sukanya Sengupta, "Threat Modeling of Industrial Control Systems for Secu-Box", UdS 2023
- Shayari Bhattacharjee, "Adversarial Robustness of Camera-Lidar based Multi-Sensor Fusion Architectures in Autonomous Driving", UdS, 2023
- Rutuja Bane, "Industrial Control System Anomaly Detection by Embedded Devices", UdS, 2023
- Daniel Berresheim, "Protecting Motor Control Firmware against Manipulation", UdS, 2023
- Anirudh Upadhya, "Safety and Security Critical Function Identification and Monitoring for Motor Controllers", UdS, 2022
- Lorenzo Rinieri, "Secure provisioning of OPC-UA devices with a certificate manager", Politecnico di Milano, 2022
- Yu-De Lin, "Extracting DNN models from Embedded Devices via Power and Timing Side-Channels", UdS, 2021
- Alessandro Erba, "Evading Anomaly Detectors through Concealment Attacks: A Study on Industrial Control Systems", Politecnico di Milano, 2019
- Francesco Scandola (University of Trento), "Application of MQTT in an Industrial Control System", Advisor: Mariolino De Cecco, 2017
- Yeaz Elias Jaddoo, "AI-enabled detection of anomalous behavior in network traffic and hosts", SUTD, 2018
- Benjamin Mary Priscilla, "Practical security assessment of industrial devices", SUTD, 2018

- Edwin Franco Myloth Josephlal, "Vulnerability analysis of an automotive telematics box", SUTD, 2018
- Ng Pock Chee Paul, "Over-the-air software security for automobile", SUTD, 2018
- Luca Cometta, "Implementation and Evaluation of a GPS Spoofing Countermeasure", ETH Zurich, 2013
- Sami Kerim Galal, "Physical layer attacks on sensor nodes", ETH Zurich 2009
- Bojan Oliver Konic, "Security issues in Microsoft SharePoint 2007", ETH Zurich, 2008
- Ada Lezama Lugo, "Implementation and evaluation of a realistic VANET simulator", EPF Lausanne, 2007
- Dominik Langenegger, "Trusted computing based opportunities for financial services", ETH Zurich, 2007

### Co-Examiner on Masters' Thesis

- Abhilash Gupta (UdS), "Grammar Fuzzing Command-line utilities in Linux", Advisor: Andreas Zeller, 2022
- Joshua Michael Sonnet (UdS), "Towards Decentralised Access Control in Thread-based Home IoT". Advisor: Sven Bugiel, 2021
- Munshi Arif Rashid (UdS), "The effect of privacy enhancing technologies on different electricity load forecasting models", Advisor: Christoph Sorge, UdS, 2019
- Hunter Callum Douglas (SUTD), "Pressure-Driven Hydraulic Modelling of Cyber-Physical Attacks on Water Distribution Systems". Advisor: Stefano Galleli, 2017
- Giulio Lovisotto (U of Padova), "We're not on the same Wavelength: Automatic Deauthentication using Wireless Signal". Advisors: M. Conti (Padova), I. Martinovic (Oxford), 2016

### Co-Examiner on PhD Thesis

- Moshe Kravchik, " Attacks and Defenses of Cyber Physical Systems ", Ben-Gurion University of the Negev, Israel, 2023
- Herson Esquivel Vargas, "Towards Automated Identification and Assessment of Security Weaknesses in Smart Buildings", UT Twente, 2022
- Juan David Guarnizo Hernandez, "Enhancing Software System Transparency via Blockchain-based Approaches", Singapore University of Technology and Design, 2022
- Davide Beradi, "Security Enhancements and Flaws of Emerging Communication Technologies", University of Bologna, 2022
- Yi Han, "AI for Trustworthy Security, Security for Trustworthy AI", advisor Saman Zonouz, Rutgers University, 2021
- Wissam Aoudi, "Process-Aware Defenses for Cyber-Physical Systems", advisor Magnus Almgren, Chalmers University of Technology (Sweden), 2021
- Ron Bitton, "AI-based Methods for Cybersecurity Risk Assessment", advisor: Asaf Shabtai and Rami Puzis, BGU (Israel), 2021

- Silvia Ceccato, "Security in Global Navigation Satellite Systems: authentication, integrity protection and access control", advisor: Nicola Laurenti, University of Padova (Italy), 2019
- Amit Kleinmann, "Network Intrusion Detection for Supervisory Control And Data Acquisition (SCADA) Systems", advisor: Avishai Wool, Tel Aviv University (Israel), 2017

### Research Assistants and Students

- Gleb Rostanin, 2023-2024
- Sahil Sihag, 2023-2024
- Lavanya Govindaraju, 2023
- Anirudh Upadhya, 2021-2022
- Daniel Erceg, 2020-2024
- Nils Glörfeld, 2019
- Amit Tambe, Research Assistant, November 2017 to July 2018
- Dominik Breitenbacher, Research Assistant, November 2017 to July 2018
- Ragav Sridharan, Research Assistant, January 2017 to July 2018
- Francesco Scandola, Research Assistant, October 2016 to July 2018
- Ahnaf Siddiqi, Research Assistant, November 2016-October 2017
- Sandra Siby, Research Assistant, June 2015 to August 2017
- Jinghui Toh, January 2016 to December 2016
- Anand Agrawal, Research Assistant, February 2016 to September 2016
- Mohannad Alhanahnah, January 2016 to June 2016

### Visiting Researchers

- Aymen Fakhreddine, PhD student at IMDEA, Spain, 2017
- Giuseppe Bernieri, PhD student at Roma Tre University, 2017
- Naman Govil, undergrad student at IIIT Hyderabad, in 2016
- Nicolas Iooss, graduate student at Corps des mines, Paris, in 2015
- Pierre Gaulon, graduate student at ENSEIRB, Bordeaux, in 2015
- David Urbina, PhD student of UT at Dallas, in 2015

### Qualifying and Preliminary Examinations

- QE: Daniel Frassinelli
- QE: John Henry Castellanos Alvarado
- QE, PE: Vu Dinh Quyen (as Chair of Committe)
- QE: Sibo Sung
- QE: Dima Dafer S Rabadi (as Chair of Committe)
- QE, PE: Mujeeb Chuadhry (as Chair of QE Committe)
- QE: Jay Prakash (as Chair of Committe)
- QE, PE: Hamid Ghaeini
- QE: Daniele Antonioli
- PE: Hans Anderson (as Chair of Committe)
- PE: Dinh Quang Thinh
- PE: Eyasu Getahun Chekole

## Professional Awards

- Best paper award at CPSS, 2017
- Short-listed for SUTD service award, 2016
- SG Design Mark Award for NSE project, 2016
- Runner-Up Smart Energy Hackathon, UP Singapore, September 2013
- Best Paper Award, IFIP Wireless Days 2012, November 2012
- K.-H. Ditze Award for TUHH's best diploma thesis 2007/2008, April 2008
- Three terms scholarship for University of Waterloo exchange studies (DAAD), April 2004

## References

References available on request.