

Table of Contents

A Note on the Post-Quantum Security of Identity-Based Encryption on Isogenous Pairing Groups <i>Malte Andersch, Cezary Pilaszewicz, and Marian Margraf</i>	1
A Multi Method Framework for GNSS Anomaly Detection in Vehicular Systems Using NMEA Data <i>Mathias Gerstner, Tobias Reichel, Sebastian Fischer, and Rudolf Hackenberg</i>	11
CVEs With a CVSS Score Greater Than or Equal to 9 <i>Lena Sinterhauf, Andreas Assmuth, and Roland Kaltefleiter</i>	17
GNSS Spoofing Simulator <i>Tobias Reichel, Mathias Gerstner, Andreas Attenberger, and Klara Dolos</i>	24
Introducing the Cyber-Physical Data Flow Diagram to Improve Threat Modelling of Internet of Things Devices <i>Simon Liebl, Ian Ferguson, Andreas Assmuth, Natalie Coull, and George R. S. Weir</i>	30
SEPP 4.0 - Evaluation of Hands-On IoT-Security Exercises <i>Louis Ebneht and Sebastian Fischer</i>	40
"The Development of an IoT-Focused Investigative Methodology: The Case of a Pico 4 Headset" <i>Luke Yates, Ian Fergusson, and Karl van der Schyff</i>	43
Performance Analysis of a Container Based Security Approach in 5G Networks <i>Musab Mustafa Wahbi MohamedAli, Roberto Bruschi, Alessandro Carrega, and Ramin Rabbani</i>	49
End-to-End Security of Smart Meter Infrastructure-Based Control Chains: A STRIDE Analysis of Residual Risks Beyond the Smart Meter Gateway <i>Julian Britz, Julian Maximilian Behrensen, Sascha Kaven, Felix Scholl, Kolja Eger, Milena Zachow, and Volker Skwarek</i>	56
From Network Traffic to Data Space: Design, Validation, and Multi-Model Benchmarking <i>Julian Graf, Murad Hachani, Christoph Moser, Sebastian Fischer, and Rudolf Hackenberg</i>	65
An Agentic GraphRAG Architecture for Organization-Aware Cyber Threat Intelligence <i>Philipp Fuxen and Rudolf Hackenberg</i>	71
An Analysis of Attack Vectors Against FIDO2 Authentication <i>Alexander Berladskey and Andreas Assmuth</i>	77
Secure-by-Design Prototyping of an IoT Access-Control System <i>Oliver Vainikko, Ulrich Norbistrath, and Ruben Jubeh</i>	84

Closing the Temporal Gap: A Deterministic Simulation Framework for Physics-Aware Automotive Intrusion Detection <i>Liron Ahmeti, Klara Dolos, Conrad Meyer, Andreas Attenberger, Sebastian Fischer, and Rudolf Hackenberg</i>	90
Agentic AI Systems as a New Class of Cybersecurity Actors: Translating Human Behavioral Concepts to Artificial Intelligence <i>Klaas Ole Kurtz</i>	97
Towards Unsupervised Adversarial Document Detection in Retrieval Augmented Generation Systems <i>Patrick Levi</i>	103
Bridging the Gap: A Linear Algebra Unit for Critical Infrastructure Defense <i>Donna Beers and Clifton P. Morrow</i>	107
An Analysis of Malware Threats Facing the IoT <i>Ross Heenan, Ian Fergurson, and Laith Al-Jobouri</i>	112
A Smart-Contract–Based Validation Framework for Secure and Auditable Federated Learning in Dementia <i>Elif Calik, Ayse Keles, and Malika Bendecheche</i>	128
SoK: Toward Protecting Internet-Accessible Legacy Systems <i>William Yurcik, Gregory Koenig, Gregory Pluta, Gianni Pezzarossi, Stuart Turner, Fabio Roberto de Miranda, and Luciano Pereira Soares</i>	134
A Meta-Analysis of the Effectiveness of Deep Learning Algorithms, Generative AI, and Agentic AI in Forecasting School Cyberattacks <i>Thushan Amarasinghege and Kalpdrum Passi</i>	142