H. Roßnagel, C.H. Schunck, J. Günther (Hrsg.): Open Identity Summit 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 123

MANTRA: A Graph-based Unified Information Aggregation Foundation for Enhancing Cybersecurity Management in Critical Infrastructures

Philipp Fuxen[1] Rudolf Hackenberg[1] Michael P. Heinl[2] Mirko Ross[3] Heiko Roßnagel[4]
Christian H. Schunck[4] Raphael Yahalom[5]

Abstract: The digitization of almost all sectors of life and the quickly growing complexity of interrelationships between actors in this digital world leads to a dramatically increasing attack surface regarding both direct and also indirect attacks over the supply chain. These supply chain attacks can have different characters, e.g., vulnerabilities and backdoors in hardware and software, illegitimate access by compromised service providers, or trust relationships to suppliers and customers exploited in the course of business email compromise. To address this challenge and create visibility along these supply chains, threat-related data needs to be rapidly exchanged and correlated over organizational borders. The publicly funded project MANTRA is meant to create a secure and resilient framework for real-time exchange of cyberattack patterns and automated, contextualized risk management. The novel graph-based approach provides benefits for automation regarding cybersecurity management, especially when it comes to prioritization of measures for risk reduction and during active defense against cyberattacks. In this paper, we outline MANTRA's scope, objectives, envisioned scientific approach, and challenges.

Keywords: Cybersecurity Management; Graph Theory; Supply Chain Security; Critical Infrastructures; Peer-to-Peer; Mesh

1 Introduction

With the increasing interconnection of public, private, and economic infrastructure, the attack surface will drastically increase during the next decades. With IPv6, the number of directly addressable endpoints will rise to potentially 340 undecillion. Moreover, all connected actors may inherit vulnerabilities over hardware, software and services supply chains and different types of trust relationships to suppliers and customers. Existing cybersecurity measures cannot keep up with this scaling and non-transparent network of interrelations,

[0] The author list is ordered alphabetically.

[1] OTH Regensburg, Faculty Computer Science and Mathematics, Seybothstr. 2, 93053 Regensburg, Germany, philipp.fuxen@oth-regensburg.de, rudolf.hackenberg@oth-regensburg.de

[2] Fraunhofer Institute for Applied and Integrated Security AISEC, Department Product Protection and Industrial Security, Lichtenbergstr. 11, 85748 Garching near Munich, Germany, michael.heinl@aisec.fraunhofer.de

[3] asvin GmbH, Schulze-Delitzsch-Str. 16, 70565 Stuttgart, Germany, m.ross@asvin.io

[4] Fraunhofer Institute for Industrial Engineering IAO, Group Identity Management, Nobelstr. 12, 70569 Stuttgart, Germany, heiko.rossnagel@iao.fraunhofer.de, christian.schunck@iao.fraunhofer.de

[5] Massachusetts Institute of Technology, MIT Sloan School of Management, 100 Main Street, Cambridge, MA 02142, USA, yahalom@mit.edu

doi:10.18420/OID2023_10

resulting in an unacceptable dimension of economical and infrastructural damages through cyberattacks [IB22] caused by: **Insufficiently automated processes** in risk management requiring manual intervention, wasting valuable and highly limited human resources; **A lack of trust** between actors when it comes to information sharing, causing insufficient situational awareness; **Silo mentality** which leads to oversimplification of existing relationships and misses out vulnerabilities and threat actors; **Missing context** of vulnerabilities, attacks paths, and relationships of actors, impeding measure prioritization; **Latency** in information sharing regarding vulnerabilities and attack patterns which extends the possible time frame for successful attacks.

2 Related Work

There is current research covering partial aspects similar to those addressed by MANTRA, such as cyber threat information (CTI) sharing using machine learning but based on a central platform [Gu22] and using federated learning but focusing on network intrusion detection [Sa23]. Other research covers benefits and barriers of CTI sharing [Zi19], challenges of CTI sharing automation [Wa19] and data models to foster it [Br21] as well as the protection of shared CTI using privacy-enhancing technologies (PETs), such as homomorphic encryption [Ba19] or attribute-based encryption [Bk22; Pr21]. However, there is no other holistic approach integrating those and other aspects envisioned by MANTRA.

3 Objectives

The goal has to be the creation of a cybersecurity mesh architecture to overcome the limitations of currently existing silos because the cross-organizational context along the supply chain is a valuable tool for assessing an organization's or individual unit's cybersecurity posture [Hu22]. MANTRA bridges the currently prevalent silos by providing a resilient and secure framework as foundation for this cybersecurity mesh system by: **Information exchange via graph models** representing relations between actors and endpoints as well as allowing contextualization and prioritization of cybersecurity risks and measures; **Increased resilience through peer-to-peer-based information exchange** between actors and along supply chains; **Secure provisioning of semantic information** to enable federated learning between actors and aggregation of data from trustworthy sources; **Leveraging post-quantum cryptography** (PQC), PETs, and hardware trust anchors to build protocols for zero trust authentication fulfilling very high security requirements; **Minimizing latency** by bidirectional, machine-readable peer-to-peer communication; **Developing socio-economic governance models** to enable the sharing of sensitive cybersecurity information along supply chains and across organizational boundaries.

3.1 Architecture

MANTRA's architecture follows a layered approach presented in Fig. 1. A peer-to-peer protocol layer serves as the technological basis and enables the secure exchange of semantic

information (P1). In order to understand its context, this semantic information from various peers is then aggregated and processed into a graph model (G1). Different applications in the application layer (A1-4) leverage these graph models for cross-organizational analysis and highly contextualized prioritization of security measures.

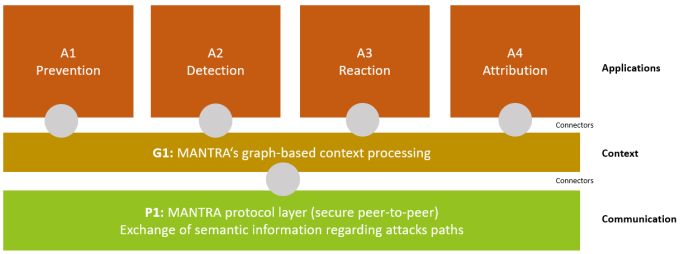


Fig. 1: MANTRA's layered architecture.

3.2 Protocol Layer

The protocol layer allows to securely exchange threat-related information based on the social graph of an organization and its individual units as described in Fig. 2. It serves as the foundation for the decentralized applications which also work offline in the worst-case scenario. Since there is no central server representing a single point of failure, the protocol increases the resilience of the participating organizations' security program. A granular governance structure strengthens the sovereignty of each participating organization which can freely decide with whom to share information. In order to serve high security demands, the protocol layer is planned to be secured by post-quantum cryptography and hardware trust anchors to be used at least at organizational borders. Furthermore, specific semantic data can be secured making use of privacy-enhancing technologies.

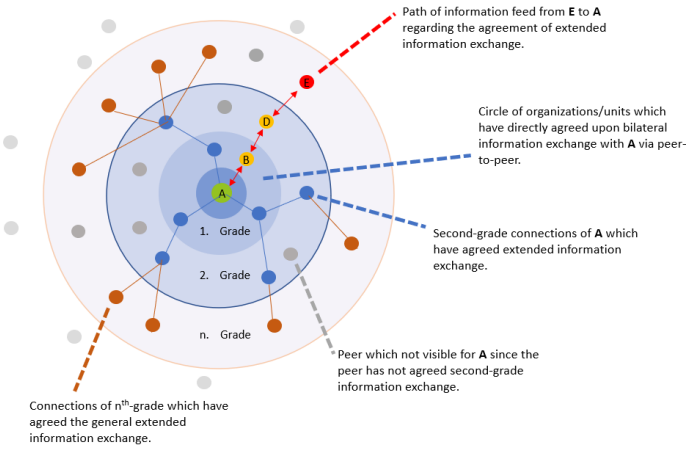


Fig. 2: MANTRA's Peer-to-Peer Protocol Layer.

3.3 Graph Layer

As shown in Fig. 3, data retrieved via the peer-to-peer protocol is going to be processed and aggregated into a graph model. Making use of federated learning allows us to further protect an individual organization's or unit's information by not sharing the information itself but rather only the learned context.

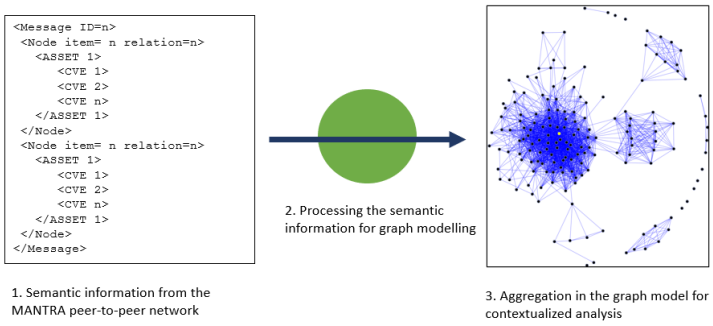


Fig. 3: MANTRA's Graph Layer.

3.4 Application Layer

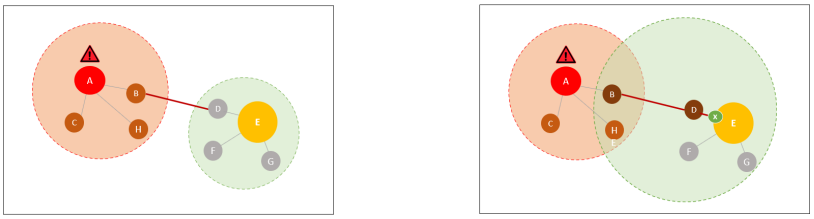
On this foundation, MANTRA will foster the establishment of new services and applications, which are going to be implemented as a prototype and evaluated in three different pilots. The services will be based on the four pillars prevention, detection, reaction, and attribution.

Prevention: The graph-based approach includes the relationships between vulnerabilities of different actors and allows to model potential attacks paths in case of a security incident both within an organization and beyond its borders. This enables new approaches to risk management by taking into account risk propagation along supply chains. It further allows to prioritize decision making regarding security measures based on a more complete picture of their predicted impact. The semantic model supports continuous learning and adaption of defense strategies on the foundation of most current data.

Detection: The graph-based analysis of attack paths provides contextual information to improve detection of anomalies and false-positive rates. Detected anomalies can be related to endpoints and organizations using the MANTRA graph model in order to foster early detection and even prediction of attacks.

Reaction The direct cross-organizational exchange and the semantics-based automation possibilities provided by MANTRA can reduce latency and therefore improve reaction times in case of security incidents. Fig. 4 shows the difference between today's isolated visibility and the extended visibility when leveraging MANTRA's graph-based approach. Organization **A** detects an attack and informs connected nodes. **E** detects no direct connections. The critical connection would require an information flow along the chain **A-B-D-E**. Via MANTRA, **E**

directly receives information about the critical exposition of **B** via the attack path graph **B-D-E**. Node E can directly react at the interface of **D** and **E** in order to minimize the risk.



(a) Context insufficient for rapid reaction (b) MANTRA context for rapid reaction

Fig. 4: Comparison of isolated visibility today (a) and visibility enhanced by MANTRA (b).

Attribution: Using the collective perspectives of the graph-based model allows for better attribution. Furthermore, comparing the attack paths and patterns with those already mapped to specific threat actors allows an cross-organizational analysis on the basis of graph-relationships. Moreover, the attribution can even be used to predict further steps of the attacker.

4 Challenges

The project's risks lie especially in the interplay between information sharing and extracting actionable intelligence: The benefits of the latter can only be achieved if information is shared and the data quality is sufficient [Sc21]. The willingness to share sensitive information by ecosystem participants in turn will be based on the promised benefits and their confidence that the measures to reduce the associated risks are sufficient. This challenge turns MANTRA into a high-risk, high-reward project. MANTRA addresses this risk by working right from the start closely with ecosystem players across industries and the public domain to ensure that what will be developed will meet their needs. This will be accompanied by an ethics by design approach as well as technological and social impact assessments to ensure benefits will outweigh risk also at a societal level.

5 Conclusion

As supply chains continue to gain economic importance and become more and more interconnected both physically and digitally, they are an increasingly attractive target for attackers. In the future, it will therefore not be sufficient to secure individual organizations against attacks, but the resilience of entire supply networks and economic ecosystems must be improved. This leap can only be achieved if new, sustainable models for information sharing between ecosystem actors and novel, more efficient models for extracting actionable intelligence from the aggregated data are put in place. The MANTRA project addresses both issues: By increasing technical capabilities in form of federated learning, PQC, zero trust

mechanisms, and peer-to-peer-based information exchange, it aims at reducing the risk in information sharing while increasing the value of the shared data. This will be accompanied by a sustainable governance framework to ensure that for all ecosystem participants benefits outweigh potential risks. Secondly, the graph-based approach to data analysis enables a far more comprehensive view on damage scenarios and business impacts as well as cybersecurity risk propagation along supply chains. This broadened view allows to enhance *prevention* by prioritizing the most effective countermeasures and establishing early warning systems across supply chains, enhance *detection* by contextualizing information across company boundaries, enhance *reaction* by coordinating responses supply-chain wide, and enhancing *attribution* by cross-organizational analysis of attacker-specific patterns.

6 Acknowledgment

This work is funded by the Agentur für Innovation in der Cybersicherheit GmbH "Innovation for Cybersecurity".

References

[Ba19] Badsha, S. et al.: Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense. In: CCWC'19. 2019.

[Bk22] Bkakria, A. et al.: Secure and Robust Cyber Security Threat Information Sharing. In: Foundations and Practice of Security. Pp. 3–18, 2022.

[Br21] Bromander, S. et al.: Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange. Digital Threats 3/1, 2021.

[Gu22] Guarascio, M. et al.: Boosting Cyber-Threat Intelligence via Collaborative Intrusion Detection. Future Generation Computer Systems 135/, pp. 30–43, 2022.

[Hu22] Hu, K. et al.: Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment, 2022.

[IB22] IBM Security: Cost of a Data Breach Report, 2022.

[Pr21] Preuveneers, D. et al.: Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. J. of Cybersec. and Priv. 1/1, 2021.

[Sa23] Sarhan, M. et al.: Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection. J. Netw. Syst. Manag. 31/1, p. 3, 2023.

[Sc21] Schlette, D. et al.: Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Sec. 20/1, pp. 21–38, 2021.

[Wa19] Wagner, T.D. et al.: Cyber threat intelligence sharing: Survey and research directions. Comp. & Sec. 87/C, 2019.

[Zi19] Zibak, A. et al.: Cyber Threat Information Sharing: Perceived Benefits and Barriers. In: ARES '19. Canterbury, United Kingdom, 2019.