Journal of
Sensor and Actuator Networks

MDPI

Editorial

Featured Papers on Network Security and Privacy

Jordi Mongay Batalla

Institute of Telecommunications and Cybersecurity, Warsaw University of Technology, 00-665 Warsaw, Poland; jordi.mongay.batalla@pw.edu.pl

1. Introduction

There is an urgent need to introduce security-by-design in networks. Security-by-design is a way to build a network where security is considered holistically in the whole network from its first concept, through the design, development, installation, configuration and maintenance of the network and to the finalisation of the useful life of the network. Security is placed at a central point of the lifecycle of a network.

This concept is currently used in mobile networks, where the 3GPP (Third-Generation Partnership Project) standards define the whole network, and all the components (called network functions) work together for the common objective of maintaining security and privacy during the operations of the network.

Security and privacy are two different concepts in networks. Security refers to the efforts of the network to improve data confidentiality, data integrity and service availability. It is worth remarking that data confidentiality comprises the protection of a user's data privacy, so nobody can read the data except the authorised individuals.

Privacy in a network refers to the necessity of protecting the identity of the users and services. Identification of users and services is crucial for the maintenance of security, which, in turn, is crucial for the maintenance of user data privacy. The latest effort to increase network privacy protection is the Zero Trust approach, defined by the National Institute of Standards and Technology.

Zero Trust involves the continuous verification of the security position of network elements, thus minimising the impact of breaches caused by outer/insider attackers and automating the context analysis of the customer and the delivery of appropriate responses. It involves the introduction of electronic identities for customers and devices into the authentication and authorisation schemas required before a session can be established; it performs continuous behavioural analyses of subjects and resources typically supported by AI/ML in the industry (e.g., geolocation and correlation with authorised services); it considers multiple factors to determine the trust (not implicit) of the user (subject) to access resources; and it is also about understanding the endpoint applications, their secure access and control, and much more.

Zero Trust security principles should be embedded in the self-organised and self-managed operations of the network, which often rely on machine learning techniques that may have opposite objectives (e.g., reducing signalling overhead vs. increasing per-flow security). Moreover, Zero Trust security should estimate the trustiness of external entities, including roaming scenarios, and use obfuscation and similar techniques in open interfaces when the network is exposed to the activity of external entities.

New security mechanisms are needed at all levels, and since networks are becoming more complex, mechanisms may sometimes have different and antagonistic objectives. This problem needs to be solved through security-by-design and Zero Trust.

To avoid misoperation in end-to-end network security, open (public) and mature security standards are required. Then, a network can not only protect its data and services but it will also be secure. This is the so-called security assurance, i.e., the demonstration that a network is secure. Independent tests of network equipment achieve this, as do tests of

Citation: Mongay Batalla, J. Featured Papers on Network Security and Privacy. *J. Sens. Actuator Netw.* **2024**, *13*, 11. https://doi.org/10.3390/jsan13010011

Received: 20 January 2024
Accepted: 30 January 2024
Published: 1 February 2024

the processes that produce and maintain network equipment, including the whole supply chain. More research is being dedicated to systematising security assurance methodologies and developing open tools for increasing the testing capacity of networking stakeholders, including mobile networks (e.g., EvORAN, Evaluation of Open RAN network equipment including underlying, which is a project funded by the European Commission through Europe Horizon NGIsargasso (Grant No. 101092887)). Security assurance increases the awareness of security principles and, above all, promotes the importance of protecting the information assets (related to network privacy) and the supporting assets (related to network security) in the network.

2. An Overview of Published Articles

The featured topic Network Security and Privacy presents new research on mechanisms for protecting a network from attacks on its security and privacy, including all networking technologies, with special attention to wireless technologies. Most new research deploys AI/ML for security tasks. AI/ML can potentially disrupt the classical principles of network security by introducing fast reactions to anomalies detected in the network and, sometimes, even by preventing the attacks before they impact the network.

In [1], Antony and Bahari conducted an examination of two cryptographic methods: public-key and symmetric cryptography. The former, while more intricate, demands more memory and storage, and is both slower and more energy-consuming. The latter faces a significant drawback—the challenge of key distribution. This implies that the shared single key must be known to the pair of communicating nodes before they can securely encrypt and decrypt data. The authors claim that creating an effective key distribution scheme for a constrained network (e.g., a wireless sensor network, WSN) poses difficulties due to constraints on devices, including energy and processing capability constraints. Failure to distribute keys among sensor nodes in a constrained network through a key distribution scheme may render the entire communication process vulnerable to attacks.

Therefore, the authors of [1] introduce a novel pre-shared key scheme based on elliptic curves over a prime field and demonstrate the applicability of the fixed scheme while exhibiting full connectivity. The scheme supports node mobility in the network, has a high scalability, and uses the elliptic curve group law and scalar multiplication in calculations instead of basic integer addition and multiplication.

Aljabri et al. discussed the adoption of artificial intelligence (AI) techniques, particularly machine learning (ML), in [2]. They argue that AI/ML has proven highly beneficial owing to their capacity to learn from past experiences and proactively thwart cyber-attacks before they escalate. ML, a subset of AI, utilises data and algorithms to mimic human learning processes, progressively improving through experience. The domain of network security, particularly constrained devices' security, presents formidable challenges, and leveraging the capabilities of ML can lead to more resilient solutions, safeguarding the confidentiality, integrity, and availability of network and user data. Paper [2] investigates the impact of different sets of features when constructing ML models for the detection of attacks on various constrained devices' and assessing model performance through feature selection techniques. In addition, the authors compare the results of binary and multiclass experiments on the dataset to identify and categorise the mentioned attacks and achieve superior benchmark results of anomaly identification.

Almuhaideb et al. argue that homoglyph replacement is an easy and often used technique in spoofing attacks in networks [3]. This method allows attackers to manipulate characters, creating a visual resemblance between two words while assigning distinct values in the underlying Unicode. This redirects the URL (uniform resource locator) request to a malicious server that may infect the client. Unicode characters closely resemble or mimic ASCII characters visually. Almuhaideb et al. studied how to precisely and efficiently detect DNS (domain name system) look-alike attacks and homoglyph domains. A detection model utilising hash functions and ML for heightened accuracy was proposed and explored. This was achieved by leveraging historical data to predict new output values. Conversely, a

hash function transforms datasets of varying sizes into fixed-size values. The authors proved that 99.8% homoglyph replacement detection could be achieved by using random forest algorithms.

A network's privacy is intricately connected to information related to a specific individual resource, be that a device, personally identifiable information (PII), a service, etc. [4]. Nevertheless, there are instances where meticulous collection of personal data is necessary for specific use cases or compliance with legal obligations. It is worth noting that a singular datum might not pose a significant threat to privacy. However, the amalgamation of data from various sources could potentially grant unauthorised access to additional information, thereby compromising an individual's privacy.

These privacy concerns are accentuated in the context of blockchain technology, where identifiers are publicly stored and verified by all network nodes. Additionally, transaction data within a blockchain can be leveraged to initiate privacy-related linkage attacks by associating them with other publicly available data. Various data-mining methods and algorithms can exploit the raw data to carry out such attacks. In light of these challenges, the authors of [4] advocate for the implementation of an elliptic curve Qu–Vanstone (ECQV)-based system. This system requires a certificate for mutual authentication, key establishment, and key exchange among network nodes and devices. The authors have demonstrated that the proposed ECQV system offers enhanced security for mutual authentication and efficient privacy preservation.

The paper by Mannix, Gorey, O'Shea and Newe [5] details the important impact of trust models on network security. They discuss Zero Trust and different models that may be applied to estimate trustworthiness in network nodes and end devices. The authors argue that conventional "hard security" measures cannot mitigate all the current threats posed by constrained devices (mainly used in the Internet of Things). For this reason, there is a shift towards adopting a "soft security" approach alongside traditional security measures. Trust models present an effective strategy for addressing the threats posed by malicious entities in networks that conventional security methods may struggle to counteract. The author explored the fundamental framework of a trust model, delving into the contexts in which they are employed and the types of attacks they aim to safeguard against, including the suitability of each parameter and a calculation method for specific environments and network types.

The final paper in this feature topic addresses application security, specifically focusing on click fraud. Alzahrani and Aljabri [6] explore click fraud, which involves creating the illusion that a substantial number of potential customers have clicked on an advertiser's link through automated scripts, computer programs, or human intervention. Despite this, advertisers are unlikely to benefit from these clicks. Fraudulent clicks may be employed to inflate the revenues of an ad hosting site or deplete an advertiser's budget. Numerous efforts have been made to detect and prevent this type of fraud. The authors comprehensively analyse and elucidate all AI/ML solutions proposed to detect and prevent click fraud, encompassing pay-per-click identification and collaborative model training to classify clicks [6].

3. Conclusions

The featured papers on Network Security and Privacy have proven that new technologies, especially ML/AI, may improve the protection of network assets, increasing the network's capacity to show that it is secure. Moreover, the authors of several papers outline the role of ML/AI in the Zero Trust architecture by providing behavioural analyses and anomaly detection for the threats not mitigated by security-by-design, e.g., device or component hijacking through a phishing attack.

In addition, the authors of the papers have shown that the protection of the network should include the protection of the end devices. Otherwise, malware infiltration and malicious insider attacks are difficult to avoid. For this, end devices need higher processing capacities, which is not always possible, especially in the case of constrained devices. Once

again, ML/AI may assist in protecting the network against availability threats, and some new algorithms have been proposed for this purpose.

Funding: This research was funded by the NGIsargasso project (Europe Horizon Grant No. 101092887) under the umbrella of 'Evaluation of Open RAN network equipment including underlying' experiment.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Antony, S.N.F.M.A.; Bahari, M.F.A. Implementation of Elliptic Curves in the Polynomial Blom Key Pre-Distribution Scheme for Wireless Sensor Networks and Distributed Ledger Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 15. [CrossRef]
2. Aljabri, M.; Alahmadi, A.A.; Mohammad, R.M.A.; Alhaidari, F.; Aboulnour, M.; Alomari, D.M.; Mirza, S. Machine Learning-Based Detection for Unauthorized Access to IoT Devices. *J. Sens. Actuator Netw.* **2023**, *12*, 27. [CrossRef]
3. Almuhaideb, A.M.; Aslam, N.; Alabdullatif, A.; Altamimi, S.; Alothman, S.; Alhussain, A.; Aldosari, W.; Alsunaidi, S.J.; Alissa, K.A. Homoglyph Attack Detection Model Using Machine Learning and Hash Function. *J. Sens. Actuator Netw.* **2022**, *11*, 54. [CrossRef]
4. Almuhaideb, A.M.; Algothami, S.S. Efficient Privacy-Preserving and Secure Authentication for Electric-Vehicle-to-Electric-Vehicle-Charging System Based on ECQV. *J. Sens. Actuator Netw.* **2022**, *11*, 28. [CrossRef]
5. Mannix, K.; Gorey, A.; O'Shea, D.; Newe, T. Sensor Network Environments: A Review of the Attacks and Trust Management Models for Securing Them. *J. Sens. Actuator Netw.* **2022**, *11*, 43. [CrossRef]
6. Alzahrani, R.A.; Aljabri, M. AI-Based Techniques for Ad Click Fraud Detection and Prevention: Review and Research Directions. *J. Sens. Actuator Netw.* **2023**, *12*, 4. [CrossRef]