future internet

MDPI

Editorial

Information and Future Internet Security, Trust and Privacy

Weizhi Meng [1,*], Thanassis Giannetsos [2] and Christian D. Jensen [1]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
[2] Secure Systems & Trusted Computing Group, UBITECH, 11632 Athens, Greece
* Correspondence: weme@dtu.dk

Abstract: The Internet has rapidly grown into a distributed and collaborative network with over one billion users, e.g., the Internet of Things (IoT). The future Internet will become the core of the next information infrastructure in regard to computation and communication, being capable of extensibility, survivability, mobility, and adaptability. However, with the increasing complexity of the future Internet and boost in information sharing, there is a threat to such infrastructure in the aspects of security, trust, and privacy. This editorial discusses the state-of-the-art advancements in information and the future internet.

Keywords: future internet; information security; trust management; data privacy; cyber security

check for updates

Citation: Meng, W.; Giannetsos, T.; Jensen, C.D. Information and Future Internet Security, Trust and Privacy. *Future Internet* **2022**, *14*, 372. https://doi.org/10.3390/fi14120372

Received: 5 December 2022
Accepted: 9 December 2022
Published: 12 December 2022

1. Introduction

According to the ITU-T Technology Watch Reports [1], the internet is evolving steadily and rapidly in order to meet the requirements of new applications, services, and users. The future internet will be an important part of international and national infrastructure. The evolutionary trend has enabled the internet to address challenges and problems over the past decade. Currently, the internet of things (IoT) enables billions of internet-connected devices, e.g., smart sensors, to communicate and interact with each other over the network/internet worldwide. It offers the capacity for remote monitoring and control and continues to be adopted in many domains. For example, it is the basis of smart cities, helping to achieve a better quality of life and lower consumption of resources [2]. In addition, smartphones are the most commonly used IoT devices, which can help to control washing machines, refrigerators, or cars.

However, the IoT also faces many challenges with respect to information and internet security. For example, attackers can impersonate a relay node to compromise the information integrity during communications. When they control or infect several internal nodes in an IoT network, the security of the whole distributed environment will be greatly threatened. There are many internal threats in such distributed environments, e.g., passive message fingerprint attacks [3], a kind of collusion attack in which malicious nodes can work together to exchange the required messages and send false information to degrade the alarm aggregation process. Hence, there is a need to safeguard information and the internet environment against the plethora of modern external and internal threats.

This Special Issue focuses on information and internet security with the aim of soliciting the latest technologies, solutions, case studies, and prototypes on this topic.

2. Contributions

The first paper [4] introduces a phishing detection engine based on machine learning algorithms and URL features. Specifically, the authors used the Levenshtein distance as a similarity index feature to train a range of machine learning algorithms. The evaluation of a dataset with 305,737 benign URLs and 74,436 phishing URLs indicated that an averaged accuracy of 94% could be achieved.

The second paper [5] introduces IoTSRM2, an IoT security risk management strategy reference model with the purpose of supporting practitioners in formulating the relevant IoT security risk management strategies. The authors started with the key cybersecurity drivers and then introduced a taxonomic hierarchy that can classify IoT security best practices based on the group and type of target audience.

The third paper [6] discusses the challenges in APSIA (automated privacy and security impact assessment) and introduced a systematic approach for assessing the privacy impact levels of organizations according to the demanded security status and threat vectors. They then detailed the prototype implementation of APSIA and demonstrated its applicability through a case study in the healthcare domain. The authors believe that their approach could complement existing security-based risk assessment tools by enhancing the privacy aspect of all the involved partners.

The fourth paper [7] reviews the existing standardization advancements in relation to blockchain and digital ledger techniques and introduces a set of criteria for comparing these standards and recommendations for blockchain systems/networks, which can be useful in the design of future networks. The authors also discussed the value of these techniques and criteria by analyzing the dependencies of the selected publications in relation to other standardization work.

The fifth paper [8] focuses on IndexedDB, which is a NoSQL (not only SQL) transactional database system that enables swift access to persistent data through JSON (JavaScript object notation) objects, and explores whether it can be used as a source of digital evidence, i.e., providing hints to the traditional investigation methods. The authors took WhatsApp Messenger and Web Application as a case study in order to populate and investigate artifacts in the IndexedDB storage of Google Chrome. They found that the WhatsApp Web IndexedDB storage could be used for timeline analysis.

The sixth paper [9] focuses on name data networking (NDN), a subtype of information centric networking (ICN), and proposed a strategy (PEKS-based NDN strategy) for protecting the names in NDN based on the best route strategy and multicast strategy. The proposed strategy can achieve higher privacy preservation without the need for a master secret key, which can be used to derive private keys. The authors also attempted to reduce the number of PEKS operations by loading several components at one time.

Acknowledgments: The guest editors would like to thank all the contributing authors, the professional reviewers, and the excellent editorial support from the Future Internet editorial office during the publication process of this Special Issue.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. The Future Internet, ITU-T Technology Watch Report 10. Available online: https://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000A0001PDFE.pdf (accessed on 1 December 2022).
2. Li, W.; Meng, W.; Furnell, S. Exploring Touch-based Behavioral Authentication on Smartphone Email Applications in IoT-enabled Smart Cities. *Pattern Recognit. Lett.* **2021**, *144*, 35–41. [CrossRef]
3. Li, W.; Meng, W.; Kwok, L.F.; Ip, H.H.S. PMFA: Toward Passive Message Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks. In Proceedings of the 10th International Conference on Network and System Security (NSS 2016), Taipei, Taiwan, 28–30 September 2016; pp. 433–449.
4. Butnaru, A.; Mylonas, A.; Pitropakis, N. Towards Lightweight URL-Based Phishing Detection. *Future Internet* **2021**, *13*, 154. [CrossRef]
5. Popescu, T.M.; Popescu, A.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet* **2021**, *13*, 148. [CrossRef]
6. Papamartzivanos, D.; Menesidou, S.-A.; Gouvas, P.; Giannetsos, T. A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly. *Future Internet* **2021**, *13*, 30. [CrossRef]
7. König, L.; Korobeinikova, Y.; Tjoa, S.; Kieseberg, P. Comparing Blockchain Standards and Recommendations. *Future Internet* **2020**, *12*, 222. [CrossRef]
8. Paligu, F.; Varol, C. Browser Forensic Investigations of WhatsApp Web Utilizing IndexedDB Persistent Storage. *Future Internet* **2020**, *12*, 184. [CrossRef]
9. Ko, K.T.; Hlaing, H.H.; Mambo, M. A PEKS-Based NDN Strategy for Name Privacy. *Future Internet* **2020**, *12*, 130. [CrossRef]