Editorial: Special Issue on IoT Security and Privacy

Guest Editors:
Matthias Schunter, Intel Labs, Germany
Andreas Wespi, IBM Research - Zurich

Recent years have witnessed a fast evolution of the Internet of Things (IoT). There is a steadily increasing number of devices that are connected to the Internet. Reports forecast an increase from 23 Billion IoT devices, already today, to 75 Billions by 2025 [1]. From a security and privacy point of view, IoT can be seen as the technology area where we experience the highest number of new attacks. On the one hand it is fascinating to see the wide variety of new attacks criminals but also researchers come up with. On the other hand this situation is very frightening because IoT devices sit at the border of the logical and physical domains. Hacked IoT devices are not only used for, e.g., leaking data but they can also be misused to negatively impact the physical world. This means that IoT is not only an IT security and privacy problem but it is also a safety problem with many implications in various domains.

The drive towards injecting intelligence into all objects drives innovation in many different areas. The Industrial Sector created IoT environments such as Industry 4.0 and Industrial Control Systems. The Internet of Medical Things (IoMT) aims at provide better service to patients. Researchers also tend to define IoT domains that best reflect their research area. An example is the Internet of the Body (IoB) [2]. All these domains share a common architecture. There are end devices or sensors, a backend that manages the devices and the collected data, and finally there are communication links between IoT devices as well as to the backend. Edge devices can serve as intermediaries between the IoT devices and the backend. Over time we have seen attacks against all these domains and components.

The most prominent IoT attack, besides Stuxnet [3], is the Mirai DDoS attack [4]. The Mirai botnet successfully attacked IoT devices whose factory set password was never changed. Mirai demonstrated how easily a large number of IoT devices could not only be penetrated but also be used to attack IT infrastructures. There are other types of IoT attacks that are more difficult of execute. For example, a Belgium research team demonstrated how a car's key fob can be cloned by exploiting an outdated and vulnerable cryptographic cipher. The cloned fob would allow an attacker to enter the car and start it.

The motivation behind this special issue on IoT security and privacy is to bring together state- of-the-art work that addresses the manifold IoT security and privacy challenges. In our call for papers we did not want to limit the scope to specific domains or IoT challenges. We were wondering what specific problems researchers tackle today, and therefore we kept the scope very wide.

We were not disappointed. There was a large variety of topics covered in the submissions we received. We are convinced that the papers that eventually made it into our journal will stimulate new ideas, all of them helping us to improve overall IoT security and privacy.

We received 52 submissions. Unlike other special issues of this Journal, we created a small and dedicated Editorial Board.

All papers have received at least three reviews from experts in the different areas. Several reviewers offered to engage in a close collaboration with the authors helping them to further improve the quality of the papers and address the reviewer comments. The papers published in our special issue of IoT security and privacy cover the following areas: (I) IoT security and privacy surveys, (II) IoT attacks, (III) IoT device security, (IV) IoT communication security, and (V) privacy enhancing technologies for IoT. The papers were selected based on their quality. Nevertheless it is surprising that the subsequent set of accepted papers covers such a wide variety of domains. This is yet another proof that IoT security and privacy is a large field that offers many challenges to be tackled:

There are two overview papers that look at IoT security and privacy research but from different angles. *"Current Research of Internet of Things (IoT) Security: A Survey"* by M. Noor and W. Hassan analyzes the IoT security publications between 2016 and 2018. Their analysis focuses on selected IoT security areas such as authentication, encryption, and routing. The investigation shows that authentication has been the topic of highest interest in the past two years. The authors also gave special consideration to the IoT simulation and modelling tools that have been used in the different IoT security and privacy research projects. Given the wide variety of tools deployed, we can conclude that the availability of good and common simulation and modelling tools will foster progress in IoT security and privacy research. The sharing, comparison, and revalidation of results are supported and will help to improve the state of the art.

"A Survey on Internet of Things Security from the Data Perspectives" analyzes the protection of IoT data along three dimensions. J. Houa and W. Shia survey security and privacy research on the management of IoT data, from the IoT device up to the backend. First, they analyze the techniques available to secure the data at the device level which includes both sensor and control data. Second, they look at the various communication security solutions, and third they review the work on application security. The survey highlights the need to have a holistic view on IoT security and privacy. One of the main practical challenges is to secure IoT solutions from the device up to the backend.

"IREXF: Data Exfiltration from Air-gapped Networks via Infrared Remote Control Signals" by Z. Zhou et al. shows an interesting attack that leaks information from air-gapped networks. We hear about new types of IoT security attacks on a regular basis. On the one hand we are amazed by the creativity of the attackers. On the other hand we are concerned about the many security holes that exist in today's IoT solutions. It is important also that IoT security and privacy researchers think about possible new attacks in order to eliminate the deficiencies in current IoT components. The authors implemented a side-channel attack and leak information via infrared remote control signals. The attack is based on a dedicated hardware device that is implanted in a keyboard and is used to exfiltrate keystroke data. The communication rate is limited to about 3 bits/s. However, this is still fast enough to leak sensitive data.

"Towards Automatic Fingerprinting of IoT Devices in the Cyberspace" by K. Yang et al. addresses the important challenge of keeping track of the many IoT devices that large organizations deploy. Manually created inventories are known to not always be accurate. Automatically detecting and classifying IoT devices would cure the problem. They collect device information at the network, transport, and application network protocol layers. For the classification of the data they apply deep learning technology. The results obtained are impressive and show that fingerprinting of IoT devices is possible at a large scale.

Securing IoT network protocols is an important area of research. IoT network protocols have to consider the limited footprint of IoT devices. Furthermore, the heterogeneity of IoT devices combined with special communication requirements often demand dedicated IoT network protocols. Given that certain IoT devices have a long lifetime and cannot be changed, protocols cannot be easily updated and can bear security issues for quite some time. Obviously this is a situation that has to improve over time.

"Formal Security Analysis of LoRaWAN" by M. Eldefrawy et al. follows a systematic approach for the analysis of the V1.0 and V1.1 LoRaWAN protocols. LoraWAN is a widely used long range, low power wireless platform for IoT. There are various studies that have identified security issues in this protocol. They use the Scyther formal security analysis tool to evaluate the key exchange component of the LoRaWAN protocol. They found a synchronization issue in V1.0 which makes the protocol vulnerable to replay attacks. However, the issue does not exist in V1.1 any more which indicates the importance of upgrading to the latest protocol version. As the authors indicate, LoRaWAN V1.0 is still widely used which again is an indication that upgrading IoT protocols seems to be a difficult task.

"Denial-of-Sleep Defenses for 99IEEE 802.15.4 Coordinated Sampled Listening (CSL)" by K.-F. Krentz and C. Meinel identifies an important deficiency in the IEEE 802.15.4 protocol. This radio standard has become a main protocol choice for implementing energy-efficient IoT applications. The protocol does not have protection against denial-of-sleep attacks which has implications in terms of draining battery charge. By incorporating the denial-of-sleep feature of an older protocol, the issues can be fixed. Here we are faced with the situation of how quickly new features can be incorporated in an existing protocol. Ideally researchers do not only publish such issues but also play an important role in getting their solution integrated in a next version of the protocol. It remains to be seen what impact this piece of work will have.

"Privacy-preserving raw data collection without a trusted authority for IoT" by Y. Liu et al. proposes a protocol for anonymous collection of data from multiple sources while hiding which source generated what data. Processing IoT data in a privacy-preserving manner remains a challenge. Despite the manifold opportunities of drawing value out of the collected data, many organizations are concerned about sharing data for privacy reasons. Given the importance of this problem, we witness a lot of work in the area of privacy-preserving IoT technology. There is always a tradeoff between data anonymization and utility. The more the data is anonymized, the less useful it becomes for the data consumer. The authors have developed a novel protocol that supports the collection of raw data from multiple sources while guaranteeing unlinkability, i.e., no one knows from which device the data originates except the original contributor. A special property of this approach is that no Trusted Authority is needed.

"RTPT: A Framework for Real-Time Privacy-Preserving Truth Discovery on Crowdsensed Data Streams" by Y. Liu at al. demonstrates that improving privacy-preserving technology not always means a

reduction of processing performance. Mobile Crowdsensig (MCS) is a new technology for IoT that has evolved because of the large number of mobile devices and the valuable information they can provide. Privacy-Preserving Truth Discovery (PPTD) is a technology that has been proposed recently and can be applied to MCS. It allows gaining insight from the the collected data in a privacy preserving way. However, PPTD shows limitations in terms of accuracy and efficiency. These are the challenges the authors successfully tackle. Furthermore, they show that their solution increases the privacy level.

"Privacy Aware IOTA Ledger: Decentralized Mixing and Unlinkable IOTA Transactions" by Sarfraz et al. is similar to the previous mentioned paper with respect to improving the privacy-preserving properties of an existing solution. The IOTA distributed ledger is used for instant micro-transactions of IoT devices. A shortcoming of IOTA is that the used pseudonyms are linkable and hence raise privacy concerns. Due to the fact that IOTA uses a hash-based signature scheme, other approaches such as those used by Bitcoin cannot be applied to IOTA. Therefore, the authors have developed a novel technique that increases the anonymity level of IOTA transactions but still is compatible with the underlying IOTA protocol.

The Guest Editors would like to thank Harry Rudin, Co-Editor in Chief for Special Issues, for initiating this Special Issue on IoT Security and Privacy and for supporting us throughout all phases of the journal creation. Our thanks also go to the Journal Manager, Sami Comohammed, and especially the members of our Editorial Board. They invested substantial time and efforts to produce high-quality and detailed reviews of all 52 papers. Their work with the authors to address the detailed comments and suggestions has allowed us to significantly improve the technical and scientific level, as well as the presentation quality of the accepted papers.

References:

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

[2] https://www.ibm.com/blogs/research/2017/02/of-big-brains-and-tiny-devices-here-comes-the-internet-of-the-body

[3] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[4] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[5] L. Wouters, E. Marin, T. Ashur, B. Gierlichs, and B. Preneel, "Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars," ESCAR EU 2018, Brussels, BE, 2018.

Guest Editors

Matthias Schunter (Intel Labs, Germany)

Andreas Wespi (IBM Research – Zurich, Switzerland)Matthias Schunter (Dr.-Ing, MBA) is the Chief Technologist of the Intel Research Institute for Collaborative Autonomous and Resilience Systems (www.icri-cars.org) and a Principal Engineer at Intel Labs. His current research focuses on security and resilience of collaborative autonomous systems. He has conducted research in diverse areas such as IoT security, virtual systems security, trusted computing, enterprise privacy management, security protocols, and cryptography. He holds an MBA from Warwick University and a Doctorate from Saarland University. He published more than sixty technical papers and 20 patent filings.

Dr. Andreas Wespi is a Research Staff Member at IBM Research - Zurich where he has been leading projects in the areas of intrusion detection, security analytics, data security and privacy, cloud security, and compliance. His current research focuses on multi-cloud security as well as IoT security. Besides his scientific work he has also been on assignment to IBM business organizations where he consulted customers in their cyber security strategy and also worked as security architect in large outsourcing projects.. He holds a Doctorate in Computer Science from the University of Basel, Switzerland.