JEEIT Conference Report

Ahmed Amro

April 2019

1 Introduction

In the period between 9th-11th of April I visited a conference in the Jordanian capital Amman titled "2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)". The conference is concidered the first edition of merging three previous conferences in Jordan focusing on electrical engineering and information technology, which are:

1. The 11th Jordanian Int'l Electrical and Electronic Eng. Conf. (JIEEEC 2019)
2. The 5th IEEE Jordan Conf. on Applied Electrical Eng. and Computing Technologies (AEECT 2019)
3. The 9th Int'l Conf. on Information Technology (ICIT 2019)

The conference received high attention in the Jordanian academic community due to it's diverse tracks (13 tracks). Additionally, the conference was organized and sponsored by prestigious entities in Jordan like the IEEE jordan section, Jordan Engineers Association, Al-Zaytoonah University of Jordan, Cisco, Siemens, and many more. The conference theme was "Technology for solving national problems"

The conference received 357 papers from 49 countries from which only 167 papers were accepted and were presented in 36 sessions. The presented papers were results of collaboration between universities in Asia (Jordan, Malasia, Saudi Arabia, United Arab Emirates, Lebanon, Palestine, Taiwan, Oman, Turkey, Iran, Iraq, and Qatar), Europe (Hungary, United Kingdom,Austria, France, and Denmark), Africa (Egypt, Libya, Mauritius, Morocco, South Africa, and Tunisia), Australia, USA and Canada.

Among the sessions I attended, only some papers were discussing cybersecurity topics in the fields of (Cryptography, Malware, IoT Security, Cloud Security, attack detection, Wireless Sensor Network security). Additionally, two of the 5 keynote speeches discussed challenges in the field of industrial cybersecurity, and IoT security. Also, I attended several sessions related to communication and software development.

2 Top Papers

The chosen papers are discussed below:

2.1 Hiding Malware on Distributed Storage

The paper presents a method for hiding a malware in a blockchain-like distributed storage services called distributed ledger technologies (DLTs). The malware will be divided into chunks and uploaded to DLT. The authors aimed to demonstrate the weak validation measures applied at such distributed storage services mainly the IPFS and swarm technologies and claimed they successfully uploaded a known malware after segregating it to bypass detection.

My questions to the presenter
1. Did you apply encryption on the malware before deployment?
Answer: No, but we are considering it for future work.
2. Do you have a mechanism to reattach the distributed malware chunks at the victim side?
Answer: No, not at the moment, the target was to illustrate the lack of sufficient validation measures at the distributed storage services.

2.2 Survey of Online Social Networks Threats and Solutions

This paper was influenced by the fact that the majority of cyber crimes in Jordan were related to online social network OSN activities, which led to the foundation of the Jordanian cyber crime law in 2015. The authors conducted an analysis for the OSNs' threats and suggested three categories for 13 types of threats the three categories are: account-based, URL-based and content-based threats. The authors also analyzed the existing protection methods and discussed their weaknesses and the possible recommendations to improve them like protection against malicious links.

2.3 Detection of Wangiri Telecommunication Fraud Using Ensemble Learning

The Wangiri fraud is the type of attack when a mobile client is tricked into returning a missed phone call which consequently cost money ending up as a loss for the telecommunication service provider. The authors suggested the implementation of machine learning to classify call logs in order to identify fraudulent calls efficiently. The authors claims that the Extreme Gradient Boosting algorithm demonstrated the best results in term of accuracy and performance.

My questions to the presenter
1. Did you test online or offline detection?
Answer: Online, we evaluated the solution over real calls and the detection

took less than one second.
2. What programming language did you use?
Answer: Python, with XGBoost and scikit-learn libraries.

2.4 Mobility Effect on the Authenticity of Wireless Sensor Networks

This paper discusses the effect of mobility on energy consumption and network delay when applying the Forward first (FF) and the Authentication first (AF) message distribution protocols in wireless sensor network WSN. The paper demonstrates the the trade-off between operational requirements and security requirements in designing a suitable WSN considering the effect of attackers distributing fake messages. Forward first protocol in the applications that require less latency and flexible with power consumption while AF protocol is more suitable in the applications that require less power consumption and flexibile with latency.

2.5 An Efficient Digital Image Encryption Using Pixel Shuffling for Wireless Network Applications

In this paper the authors suggested a symmetric image encryption algorithm suitable for wireless sensor network environment based on Chaotic maps to generated randomness. The encryption algorithm is divided into three phases: key generation, permutation, and transposition. The authors claim that their algorithm satisfies security requirement to resist known attacks and perform better compared to other techniques.

My questions to the presenter
1. The key generation is performed at the encryption stage, how is it handled at the decryption stage?
Answer: We assume the existence of a secure key management algorithm to handle key distribution.
2. I noticed that part of the key is generated from the image itself, why did you choose this approach knowing that a known-plain text attack will take advantage of this feature to recalculate the key?
Answer: We intended for this feature to increase the randomness of the encrypted images.

2.6 Using Machine Learning to Detect DoS Attacks in Wireless Sensor Networks

The authors suggested a DoS attack detection technique that applies machine learning. The authors compared two machine learning algorithms, namely Support vector machine (SVM), and decision tree (DT). They evaluated their technique against a data set from the literature that includes four types of DoS attacks. The results show a slightly better performs of DT compared to SVM.

Critical view: From audience questions, it appeared that the authors haven't considered a real life implementation of their technique since it requires high data transfer and computation which is not suitable for Wireless sensor network.

2.7 An Efficient and Secure Key Exchange Protocol Based on Elliptic Curve and Security Models

The authors in this paper suggested a new Authenticated Key Agreement (AKA) protocol that aims on generating multiple sessions key. The suggested AKA protocol is based on the hash variant of the Menezes–Qu–Vanstone HMQV key agreement protocol and the public key authentication YAK protocol. The proposed protocol depend on static and ephemeral keys for generating multiple sessions keys. The authors claims that the protocol overcomes attacks affecting both the HMQV and YAK protocols.

3 Keynote Speeches

3.1 Internet of Things: Business Transformation and Security Challenges

The speaker Ammar Rayes (Distinguished Engineer at Cisco's Advanced Services Technology Office) discussed his published book on the IoT security challenges, the book titled "Internet of Things From Hype to Reality: The Road to Digitization". The speaker discussed the IoT typical reference architecture which consists of 1. IoT Devices 2. IoT Network 3. IoT Management Service platform 4. IoT Application. Then the authors gave examples of IoT driving factors and use cases such as the convergence between information technology IT and Operational Technology OT which include hardware components like sensors and internet-based services like the self driving cars from UBER and others.

The author also discussed the IoT service platform functions such as discovery and registration which help industries assess their equipment in easy manner. Furthermore, the speaker demonstrated a registration function example using the COAP protocol to discover information related to surrounding IoT devices and their locations. Additionally, the speaker discussed the benefits if the FCAPS network management framework in IoT service platform.

Finally, the speaker discussed the top IoT security challenges and requirements. Security challenges such as, interoperability, mobility, scalability, big data and others. Security requirements such as confidentiality, freshness, forward and backward secrecy. Furthermore, the speaker discussed some attack scenarios targeting the sensing domain in IoT like jamming and vampire attacks.

3.2 Holistic Security Concept for IT Operational Technology Systems

The speaker Fuad Al Attar (Siemens LLC, Executive Vice President, Industry Services, Middle East) discussed the challenges faced by the industry in achieving operational quality while satisfying security requirements. The speaker mentioned the value of IoT to manufacturer like Siemens for their role in reducing the need to send experts to far locations, a goal now can be achieved by an installed device.

The speaker discussed the difference between IT security vs OT industrial security (Concepts and impact). He stressed on the fact that it is impossible to blindly apply IT security into OT security. This is related to different security goals, installment requirements and variant attack vectors. For instance, in OT availability ranks higher than confidentiality, a different case than typical IT systems. Also, the protocols, are mostly different. Additionally, in OT insider attackers have more risk weight.

The speaker discussed two case studies where IT security solutions affected industrial operation goals. The first one discussed the South Pars Integrated Fiber Optic Network (SPIFON), a firewall installment increased latency dramatically to non acceptable operational requirements. Another case study where an increased Zigbee installment initially intended to achieve security with acceptable operational requirements, yielded an increased power consumption making equipment life cycle unacceptable. Later, the speaker discussed the concepts of industrial Security, like physical security, network security and system integrity.

I had the chance to ask the speaker about the challenges facing increased collaboration between academia and industry. He answered that they do collaborate carefully with specific universities in certain roles but to be objective the industry will always be business driven and research doesn't acclaim as a clear revenue source.

4 Links

1. Conference link: https://jeeit.net/
2. Accepted Papers and abstract: https://jeeit.net/accepted-papers/