ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	PALLAVI KALIYAR
Nationality	INDIAN
Name of the *Host Organisation*	NTNU
First Name / family name of the *Scientific Coordinator*	Prof. SOKRATIS KATSIKAS
Period of the fellowship	01/10/2021 to 30/09/2022

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

1. Worked on the deliverables of Norwegian Research Council Project Called CybWIN.
2. Regular meeting with the scientific coordinator to discuss and update work progress.
3. Partially co-taught the Critical Infrastructure Security Course (IMT 4203) to the students of Master of Computer Science. In particular, I delivered the lecture related to “Selected aspects of collaborative manufacturing infrastructure security and resilience”.
4. Explored few other areas related to the Internet of Things Security.
5. I was part of Prof. Sokratis’s group where I improve my research management and collaboration.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

During my ERCIM fellowship I have worked on 4 publications, out of which 2 are already accepted and 2 are still in submission.

1. Laszlo Erdodi, Pallavi Kaliyar, Siv Hilde Houmb, Aida Akbarzadeh, and André Jung Waltoft-Olsen. 2022. Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104. In The 17th

International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria. ACM, New York, NY, USA, 10 pages.

Smart grid brings various advantages such as increased automation in decision making, tighter coupling between production and consumption, and increased digitalization. Because of the many changes that the smart grid inflicts on the power grid as critical infrastructure, cyber security and robust resilience against cyberattacks are essential to handle. With an increased number of attack interfaces and more use of IP-enabled communication, digital stations or IEC 61850 substations need to operate according to a zero-trust security model. Cyber resilience needs to be an integrated part of the substation and its components. This paper presents an experiment utilizing a Hardware-In-the-Loop (HIL) Digital Station environment (enclave), where the focus is on attacking the SCADA protocol IEC 60870-5-104. We implemented 14 attacks, the attacks are described in detail, including the result of each attack action. Furthermore, the paper discusses the implications of the findings in the experiment and what power grid asset owners can do to protect their substations as part of their digitizing efforts.

2. Pallavi Kaliyar, Laszlo Erdodi, Sokratis Katsikas “LIST: Lightweight Solutions for Securing IoT Devices against Mirai Malware Attack". In Proceedings of the Sixteenth International Conference on Emerging Security Information, Systems and Technologies, 2022 (SECURWARE 2022).

   Recently, the number of Internet of Things (IoT) devices has increased significantly, as they have become affordable to most people. This spread has highlighted a critical security threat, namely the increasing number of Distributed Denial of Service (DDoS) attacks. As these resource constrained IoT devices are built to be cost-efficient, their security measures are limited. Moreover, most users are not aware of the security measures that they must apply. Nowadays, almost every IoT device (e.g., fridge, air conditioner, thermostat, toaster) is able to connect to the internet, and this allows the user to access and control it with its own smartphone application. The lack of security measures in these devices was highlighted in September 2016, when a large-scale DDoS attack was launched using a botnet of compromised IoT devices. This type of attack has been since used in different forms and has been classified as Mirai DDoS Botnet Attack. This paper presents a detailed analysis of the Mirai attack and of the source code of the Mirai malware, reports on the implementation of the attack in a controlled environment and proposes possible solutions that could help in mitigating the attack.

3. Pallavi Kaliyar, Vasileios Gkioulos, Sokratis Katsikas “ARMS: A Generic Inter-dependent Risk Assessment Markov Model for Critical Infrastructures". In Proceedings of the Fifteenth International Conference on Norwegian Information Security, 2022 (NISK 2022). (In submission)

   In recent years, Critical Infrastructure Systems (CIS) have become essential to nations’ economies. These CIS are vulnerable to un- intended and intended cyber and physical attacks. The well-being and performance of these critical

infrastructures are analyzed through different attributes, namely Reliability, Availability, Maintainability, Safety, and Security (RAMSS). In this paper we propose a risk analysis framework called ARMS. We design ARMS using the properties of the hidden Markov Model. The transition diagram representation and the formulation of the Markov process properties are done using Markov process definitions. To analyze the performance of ARMS we use the Hardware-In-Loop (HIL) digital substation laboratory setup. We implement five different cyber attacks from which we gather the RAMSS parameter values. With the help of ARMS, we show how all RAMSS five attributes are interdependent, and how a negative impact on one of these attributes can lead to quantifiable impact on the other attributes. This is important to identify the critical attributes among these five, as more resources could be attributed to the critical ones during failures, to ensure the overall impact can be minimized.

4. Mohamed A. El-Zawawy, Pallavi Kaliyar, Mauro Conti, Sokratis Katsikas “Honey-List Based Authentication Protocol for Industrial IoT Swarms". In (Elsevier) Journal of Network and Computer Communication, 2022 (COMCOM 2022). (In submission)

   Industrial Internet of Things (IIoT) systems are advanced IoT systems composed of sensor devices supported with dynamic objects such as smart vehicles and drones. The collaboration among static and heterogeneous mobile objects makes the topologies of IIoT systems dynamic and complex. This dynamic topology is also partially due to that fact that the static devices are typically partitioned into categories of collaborating sensors (called swarms) managed by side servers. However, existing authentication techniques for IIoT systems do not consider realistic system models simultaneously hosting different types of dynamics objects. For such scenarios, there is a need for protocols that guarantees a secure Entity-to-Entity (E2E) communication, thus ensuring a smooth and safe production process.

   In this paper, we present HASFAV, a lightweight and locality-aware key agreement and authentication protocol for IIoT systems, to enable efficient and secure E2E communication between devices in the same or different partitions. HASFAV fills the gap of considering a realistic system model simultaneously hosting different types of dynamics objects. We employ Honey lists (lists with algorithms used to prevent guessing passwords) and mutual authentication technologies in HASFAV to guarantee its security against different attacks, even in public-channel communication scenarios. Using the well-established Real-Or-Random (ROR) model, we proved the security of HASFAV in detail. We also provide a prototype implementation of HASFAV in the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. This tool confirms the results of our theoretical proofs, thus verifying the security of HASFAV. We also carried out a detailed comparative study of HASFAV against existing related authentication techniques. Compared to these techniques, HASFAV offers more functionality (serving more types of dynamic objects) and superior security (via proving backup plans for session keys establishment). Finally, we prove that HASFAV is practical by implementing it in a well-known network simulator, called Omnet++.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

1. Attended Kristian Kanneløning seminar on the results of his research on “how cybersecurity compliant behavior is measured” at NTNU.
2. Attended Håvard Ofte seminar on the results of his research on “Situation Awareness in SOCs, Decoding the Greatest Enigma of Cybersecurity - The Human Operator” at NTNU.
3. Presented a seminar on “Secure data communication techniques for Internet of Things Networks” during my REP visit at RISE, Sweden.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

1. For my Research Exchange Program (REP) I visited Joakim Eriksson head of a unit at RISE, Sweden from 30th of May to the 3rd of June 2022.
2. During this period, Joakim Eriksson introduces me to the other members of his team and their research work.
3. I provided an introduction about my current and previous works, and delivered a talk on my PhD thesis topic, which was “Secure data communication techniques for Internet of Things Networks”
4. We also agreed to expand the discussion into a possible collaboration with Thiemo Voigt at RISE in the field of IoT security.
5. Visiting RISE at Sweden was a very nice experience for me, the host as well as the institute peoples were very welcoming.