SHORT TERM SCIENTIFIC MISSION (STSM)
SCIENTIFIC REPORT

This report is submitted for approval by the STSM applicant to the STSM coordinator

Action number: CA15127 - Resilient communication services protecting end-user applications from disaster-based failures (RECODIS)
STSM title: "Secure Connectivity of Future Cyber-Physical Systems"
STSM start and end date: 2019-03-08 to 2019-03-19
Grantee name: Dr. Madhusanka Liyanage

PURPOSE OF THE STSM:

The purpose of this visit is to establish a research collaboration between Department of Computer Science, Swansea University and CWC (Centre for Wireless Communications), University of Oulu focusing on network security domain and finalize the book chapter 1.9 in RECODIS book together with Dr. Pradeep Kumar.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

I was invited to visit Department of Computer Science, Swansea University, UK by Dr. Pardeep Kumar. On arrival, I had a meeting with Dr. Kumar and he explained his research on blockchain and security domains. Moreover, he explained briefly about ongoing projects in his research group. He also gave a tour around the university and department. Moreover, he introduced few colleagues at the department od computer science.

Public Seminar

I conducted a public seminar on my current research work on "Software Defined VPLS Architectures: Opportunities and Challenges" for researchers at Department of Computer Science, Swansea University. Virtual Private LAN Services (VPLS) is an Ethernet based VPN (Virtual Private Network) service which provides protocol independent and high speed multipoint-to-multipoint connectivity. In the talk, I will discuss the possibility to use emerging networks concepts such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) to improve the performance, flexibility and adaptability of VPLS networks. SDN and NFV based VPLS (SoftVPLS) architectures offer new features such as centralized control, network programmability and abstraction to improve the performance, flexibility and automation of traffic, security and network management functions for future VPLS networks.

The public seminar was interested to many researchers and it opened up many collaborative research areas.

Collaborative Research and Main research Findings

Then, I discussed the research work with Prof. Matt Jones who is the Head of College at collage of science at Swansea University. He was very fond of University of Oulu's research activities on toward 6G. Specially, we discuss about possible collaborations under the umbrella of 6Genesis (the 6G-Enabled Wireless Smart Society & Ecosystem) project at University of Oulu, Finland. Then, I have discussed with Prof. Arnold Beckmann who is the Head of the Department at Department of Computer Science, Swansea University. We discuss the possible collaborations under blockchain domain. In addition, I have talked with Dr Anton Setzer about the usecase of Blockchain for IoT applications.

With Dr. Pardeep, I have discussed about the research related to "5G authentication" as well. We found the security vulnerability in current 5G Authentication scheme and proposed a modified version to tackle these issues. Dr. Pardeep will finalize the formal verification of proposed security scheme. Moreover, we discuss the possibility to apply EPSRC-SFI Project. We discuss few project ideas however we need to work further on this task to finalize the proposal.

We also finalized and submitted joint publication on "A Survey of 5G Security" to IEEE Communications Surveys and Tutorials.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

- **Joint Publications**

1. Finalize the joint publication on "A Survey of 5G Security" which will be submitted to IEEE Communications Surveys and Tutorials.

Abstract: Security has become the primary concern in any telecommunications system in the world today as risk measures can be rather perilous. Security and privacy concerns are become forefront, especially, with 5G networks as confidential information will move in all layers in the future wireless systems. The hazard exposed by the infected wireless network not only affects the security and privacy concerns, but also impends the complete dynamic communications ecosystem. The complexity and strength of security attacks have increased in the recent past by making the detection or prevention a global challenge.

In this survey, we present a comprehensive detail on the 5G security model, network softwarization security, PHY (Physical) layer security and 5G privacy concerns. Moreover, we investigate security monitoring and management of 5G networks. In this paper, we also evaluate the 5G security standards from different standardization bodies and provide a brief overview of 5G standardization security forces. Furthermore, we list out the main projects with an international significance in line with the security concerns of 5G and beyond. Finally, we offer interesting future directions and open challenges to encourage future research.

2. Working on Joint Publication on “Novel 5G Authentication Protocol to Improve the Resistant against Active Attacks and Malicious Serving Networks”

   Abstract: The security of mobile communication largely depends on the strength of the authentication key exchange protocol. The 3GPP (3rd Generation Partnership Project) group has standardized the 5G AKA (Authentication and Key Agreement) protocol for the next generation of mobile communications. It has been recently shown that the current version of this protocol still contains several weaknesses regarding user localization, leakage of activity, active attackers and in the presence of malicious serving networks, leading to potentially major security leaks.

   We propose a new version of the 5G AKA protocol to overcome all the currently identified weaknesses in the protocol. In the new protocol, we replace the sequence numbers with random numbers, making it possible to drastically reduce the number of required communication phases and steps in the protocol. The usage of random numbers for 5G AKA protocol is possible since the current Universal Subscriber Identity Modules (USIMs) are now capable of performing randomized asymmetric encryption operations. Moreover, the proposed protocol provides two additional security features, i.e. post-compromise security and forward security, not present in the current 5G AKA protocol. Finally, we evaluate the performance, both computation and communication efficiency, of the proposed AKA protocol and show its improvements compared to the current 5G AKA protocol.

- **Book Chapter**

  Together, with Dr. Pradeep we will finalize chapter 1.9 in RECODIS book.

FUTURE COLLABORATIONS (if applicable)

To strengthen our collaborations, Dr. Kumar and I have discussed two possible collaborative activities.

1. Dual-degree Program: We initiated the discussion about starting a Dual-degree PhD program between University of Oulu and Swansea University.

2. Research Visit: We have agreed to conduct a research visit from Swansea University to University of Oulu during Summer 2019.

3. Workshop on 5G and Security: With Dr. Pardeep We agreed to conduct a workshop on “5G and Security” at Lovely Professional University, Punjab, India.

4. Joint Project: Prepare a project proposal for EPSRC-SFI Project | UK-Ireland call: http://www.sfi.ie/funding/funding-calls/epsrc-sfi-partnership/index.xml