ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Mudassar Aslam / Jadoon
Nationality	Pakistani
Name of the Host Organisation	RISE SICS
First Name / family name of the Scientific Coordinator	Shahid Raza
Period of the fellowship	01/12/2018 to 01/12/2019

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

The main scientific activity planned for the fellowship period was to explore the automated auditing and certification mechanism for edge and IoT nodes. This research was mainly motivated by the envisioned EU Cybersecurity Certification framework therefore the EU activity around this domain remained a topic of interest. The main research activity, to realize the required automated audit and certification of edge/IoT nodes, was focused on using hardware based Trusted Execution Environment, that is, Trusted Platform Module. Hence, TPM 2.0 specifications were read thoroughly and used in the proposed solutions. The principles designed during the fellowship were written to produce a research publication (FoNAC - An Automated Fog Node Audit and Certification Scheme) which was submitted to a reputed security journal with good impact factor.

In addition to the main research activity, other related research articles were also written and submitted simultaneously. A list of those submissions is presented in the next section.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Following papers were focused during the fellowship period:

Paper 1: FoNAC - An Automated Fog Node Audit and Certification Scheme
Authors: Mudassar Aslam, Bushra Mohsin, Abdul Nasir, Shahid Raza
Abstract: *“Meeting the security and privacy needs for IoT data becomes equally important in the newly introduced intermediary Fog Computing layer, as it was in its former technological layer - Cloud; but the accomplishment of such security is critical and challenging. While security assurance of the fog layer devices is imperative due to their exposure to the public Internet, it becomes even more complex, than the cloud layer, as it involves a large number of heterogeneous devices deployed hierarchically. Manual audit and certification schemes are unsuitable for large number of fog nodes thereby inhibiting the involved stakeholders to use manual security assurance schemes altogether. However, scalable and feasible security assurance can be provided by introducing automated and continuous monitoring and auditing of fog nodes to ensure a trusted, updated and vulnerability free fog layer. This paper presents such a solution in the form of an automated Fog Node Audit and Certification scheme (FoNAC) which guarantees a secure fog layer through the proposed fog layer assurance mechanism. FoNAC leverages Trusted Platform Module (TPM 2.0) capabilities to evaluate/audit the platform integrity of the operating fog nodes and grants certificate to the individual node after a successful security audit. FoNAC security is also validated through its formal security analysis performed using AVISPA under Dolev-Yao intruder model. The security analysis of FoNAC shows its resistance against cyber-attacks like impersonation, replay attack, forgery, Denial of Service (DoS) and MITM attack.“*
Publisher: Computers and Security Journal (Elsevier)
Current status: Submitted revision with minor changes. Decision awaited

Paper 2: Security and Trust Preserving Inter- and Intra-Cloud VM Migrations
Authors: Mudassar Aslam, Simon Bouget, Shahid Raza
Abstract: *“This paper focus on providing a secure and trustworthy solution for virtual machine (VM) migration within an existing cloud provider domain, and/or to the other federating cloud providers. The Infrastructure-as-a-Service (IaaS) cloud service model is mainly addressed to extend and complement the previous Trusted Computing techniques for secure VM launch and VM migration case. The VM migration solution proposed in this paper uses a Trust_Token based to guarantee that the user VMs can only be migrated and hosted on a trustworthy and/or compliant cloud platforms. The possibility to also check the compliance of the cloud platforms with the predefined baseline configurations makes our solution compatible with an existing widely accepted standards-based, security focused cloud frameworks like FedRAMP. Our proposed solution can be used for both, inter- and intra-cloud VM migrations. Different from previous schemes, our solution is not dependent on an active (on-line) trusted third party, that is, the trusted third party only performs the platform certification and is not involved in the actual VM migration process. We use the Tamarin solver to realize a formal security analysis of the proposed migration protocol and show that our protocol is safe under Dolev-Yao intruder model. Finally, we show how our proposed mechanisms fulfil major security and trust requirements for secure VM migration in cloud environments.“*
Publisher: International Journal of Network Management (Elsevier)
Current status: Accepted

Paper 3: ShieLD: Shielding Cross-zone Communication within Limited-resourced IoT Devices running Vulnerable Software Stack

Authors: Anum Khurshid, Sileshi Demesie, **Mudassar Aslam**, Shahid Raza

Abstract: *"Arm TrustZone partitions a CPU and system into a secure and non-secure world, where secure services are placed in the protected zone and traditional applications are placed in the non-secure world. A common design pattern might be to allow non-secure applications the ability to use secure services, however, this is problematic because it might be that the rich (insecure) OS is compromised and can corrupt or eavesdrop on communications, motivating the need to provide a trusted channel between the non-secure world app and the secure services. Prior work used encryption and runtime memory isolation to establish the channel, however, encryption can be costly. This paper presents ShieLD, which takes advantage of a new hardware feature in MPU based trustzone chips, where a non-secure world app can directly call into a secure service. ShieLD uses this along with memory isolation to ensure that only the permitted non-secure application has access to a new cross-domain shared page where communications occur. ShieLD must ensure that it properly associated each of these page vaults with their associated non-secure world app, and to ensure that whenever the given task is switched out of context, so to is the shared vault. This requires controlling interrupts. The vault is provided by means of control over the devices MPU. The MPU is isolated using MMIO protections. So the untrusted OS has no ability to modify the protection bits. A prototype is provided along with a minimal microbenchmark evaluation."*

Current status: Submitted to a tier-1 security conference. Decision awaited

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

Conference: Speaker at Paranoia Conference – 22nd May 2019, Oslo, Norway

Seminar: RISE SICS and Ericsson Security Day – 28th November 2018, Stockholm, Sweden
Seminar: EU Cybersecurity Certification Seminar – 24th April, 2019, Stockholm, Sweden
Seminar: 19th Seminar within the Framework of a Swedish IT Security Network for PhD students (SWITS) – on 3,4 June 2019, Karlstad, Sweden

IV – RESEARCH EXCHANGE PROGRAMME (REP)

Organization visited: NTNU
Department: Systems Security Group
Country: Norway
Local Scientific Coordinator: Prof. Stewart James Kowalski (stewart.kowalski@ntnu.edu
Duration: November 24, 2019 to November 29, 2019

Reflections from REP Visit

It was a very interesting and useful visit because of the relevance of my research areas and the activities at the Systems Security department in NTNU, Gjøvik. The first day was mainly spent on introduction, getting access to labs and sitting place, etc. During the visit, the local scientific coordinator helped in setting up several meetings and discussions with different research groups' heads which gave me interesting insights into the broad spectrum of security domains. In addition to such one-to-one meetings, two main meetings were also arranged with a group of researchers from different domains with an objective to share the research activities at RISE and NTNU for possible future collaborations. Special presentation on the Norwegian Cyber Range was also arranged to see potential for future collaborations with RISE Cyber Range. On the final day, I got chance to attend a research seminar on “Deep Learning based Malware Detection and Classification” which highlighted interesting techniques of malware detection; the visit was finally concluded with a tasty pizza (served during the seminar) before my departure from NTNU, Gjøvik.