ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

Scientific Report

First name / Family name	Manoranjan Mohanty
Nationality	Indian
Name of the *Host Organisation*	SICS Swedish ICT
First Name / family name of the *Scientific Coordinator*	Christian Gehrmann
Period of the fellowship	01/04/2014 to 01/04/2015

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

Fellow's research activities in his host institute SICS Swedish ICT falls under ERCIM's *Security and Trust Management* area of research. During his fellowship, the fellow worked on two main projects: Media Data Protection during Execution on Mobile Devices (MEDPRO) and Avoiding Weak Parameters in Secret Image Sharing.

The MEDPRO project focuses on using hypervisor and ARM TrustZone isolation to protect media rendering pipeline when DRM (Digital Rights Management) protected media is being rendered in a mobile device. The goals here are to obtain a more generalized and secure DRM system that can prevent a malicious user from misusing premium media content, which is obtained through a license from a content provider. In this project, the fellow worked in a team to prepare the pre-study, analyse the problem, and design the solution. The pre-study and initial analysis has been published as a SICS report [1]. Currently, the fellow is involved in implementation that involves ARM v8 architecture. From this project, the fellow has been exposed to embedded security research and embedded system development.

The second project, Avoiding Weak Parameters in Secret Image Sharing, falls under secret image sharing research area. This project was analysed, designed, and implemented by the fellow as the lead researcher. In this project, the fellow showed that color information can be lost from typical (3, 3, n) multi-secret sharing based secret image sharing techniques when share numbers have not been selected carefully. To counter this information loss, fellow proposed a share selection scheme. This work has been presented in IEEE VCIP 2014 conference [2].

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

[1] **Media Protection During Execution on Mobile Platforms – A Review**; Manoranjan Mohanty, Viktor Do, and Christian Gehrmann; SICS Report, July 2014; http://soda.swedishict.se/5685/

ABSTRACT

Multimedia content streaming has become an essential part of digital life. The media-on-demand (e.g., video on demand) service of certain enterprises, such as Netflix, Hulu, and Amazon etc. is changing the equations in which media content were accessed. The days, when one has to buy a bulk of media storage devices, or has to wait for the public broadcasting (e.g., television), to enjoy her preferred media has gone. Such change in the way of entertainment, however, has created new issues of piracy and unauthorized media access. To counter these concerns, the digital rights management (DRM) protection schemes have been adopted. In this report, we investigate one of the most important aspects of the DRM technology: the problem of protecting the clear text media content when playing licensing protected content on a mobile device. To this end, we first investigate how this problem has been addressed on different platforms and CPU architectures so far, and then discuss how virtualization technologies can be potentially used to protect the media pipe on mobile platforms. Our study will consider both industry-level and academic-level works, and will discuss the hardware-based and software-based approaches.

[2] **Avoiding Weak Parameters in Secret Image Sharing**; Manoranjan Mohanty, Christian Gehrmann, and Pradeep K Atrey In Proceedings of the 2014 IEEE VCIP Conference, Malta; 7th December 2014 to 10th December 2014.

ABSTRACT

Secret image sharing is a popular image hiding scheme that typically uses (3, 3, n) multi-secret sharing to hide the colors of a secret image. The use of (3, 3, n) multi-secret sharing, however, can lead to information loss. In this paper, we study this loss of information from an image perspective, and show that one-third of the color values of the secret image can be leaked when the sum of any two selected share numbers is equal to the considered prime number in the secret sharing. Furthermore, we show that if the selected share numbers do not satisfy this condition (for example, when the value of each of the selected share number is less than the half of the value of the prime number), then the colors of the secret image are not leaked. In this case, a noise-like image is reconstructed from the knowledge of less than three shares.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

IEEE VCIP Conference, Malta; 7th December 2014 to 10th December 2014.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

The fellow attended REP in Department of Computer Science, Salzburg University, Austria from 11th June 2014 to 18th June 2014. During this period, the fellow attended ACM IH&MMSec 2014 workshop, delivered a talk in Department of Computer Science, Salzburg University, and interacted with Prof. Andreas Uhl’s (fellow’s host in Salzburg University) research team.