Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

A Session Hijacking Attack on Physical Layer Key Generation Agreement

SPEAKER **Mr Qiao HU**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 21 April 2017 (Friday)
TIME 11:30 am - 12:00 noon
VENUE CS Seminar Room, Y6405, 6th Floor
Yellow Zone, Academic 1
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Physical layer key agreement is a new kind of schemes used to generate a shared key between pervasive and resource constrained devices. These schemes utilize the characteristics of the wireless channel to generate the shared key. As all characteristics are time-depend and location-depend, it is hard for eavesdroppers to get the key. But it lacks research on active attacks which aim at manipulating the key. PHY-UIR (PHYsical layer key agreement with User Introduced Randomness) is the only paper which proposes a solution in detail to against such kind of active attacks. In this paper, we propose a new kind of key manipulating attack which PHY-UIR cannot prevent. We call it session hijacking attack as the attacker hijacking the key agreement by injecting high power signals and force legitimate devices running PHY-UIR protocol with the attacker. In such way, the attacker and device generate the same key. Our simulation result validates our attack and shows the high performance of our attack on manipulating the generated key.

This paper was presented at International Conference on Industrial Technology (ICIT), March 22-25, 2017, Toronto, Canada.

Supervisor: Dr Gerhard Petrus HANCKE
Research Interests: Wireless Security, RFID, Smart Cards and IoT, Embedded and Mobile Systems

All are welcome!

In case of questions, please contact Dr HANCKE Gerhard Petrus at Tel: 3442 9341, E-mail: gp.hancke@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.