UK-Qatar Cyber Security Workshop on Adaptive Information Security

Doha - 24th October 2016

Venue: Room 105, Qatar University Research Complex, Building H10

09:00-10:30: Session 1 - Welcome & Keynote Presentation

- Welcome by Dr. Sumaya Al-Madeed, Head, Department of Computer Science and Engineering, Qatar University
- Opening Remarks by Dr. Abbes Amira, Director, KINDI Research Lab, Qatar University
- Introductions and Context
  - Prof. Bashar Nuseibeh, The Open University (OU), UK
  - Dr. Khaled Khan, Qatar University (QU), Qatar
  - Dr. Munir Tag, QNRF, Qatar

- **Keynote Presentation:**
  - **IoT security: what are we talking about?**

    Dr. Marc Dacier, Research Director, Cyber Security Group, QCRI / HBKU, Qatar

10:30-11:00: Coffee Break

11:00-12:00: Session 2 - Adaptive Information Security Project Presentations

- **Adaptive Security for ownCloud**: Dr. Arosha Bandara (OU) & Dr. Khaled Khan (QU)
- **Requirements and Specifications for Adaptive Information Security:** Dr. Thein Tun (OU)
- **Beyond "access denied"**: Dr. Armstrong Nhlabatsi (QU) & Dr. Yijun Yu (OU)

12:00-13:00: Lunch

Posters & Demo

KINDI Computing Research — جامعة قطر QATAR UNIVERSITY — The Open University — Qatar National Research Fund, Member of Qatar Foundation

13:00-13:45: Session 3 - Keynote Presentation

- **Controlling Data Leakage and Theft in Big Data Applications**
  Prof. Ernesto Damiani, Chair of the Information Security Group and Program, Khalifa University, UAE

13:45-15:00: Session 4 - Research Presentations

- **Blockchain Security and Privacy: Preliminary Data Analytics Perspective**
  Dr. Davor Svetinovic, Masdar Institute, UAE,
- **Practical cryptographic designs for restricted environments**
  Dr. Hoda A.Alkhzaimi, Director of Center for Cyber Security & Research Assistant Professor, Center for Cyber Security, New York University/Abu Dhabi
- **Cyber Medicine: Adaptive Information Security in Healthcare**
  Dr. Ali Al Sanousi, Executive Chief Medical Information Officer, Hamad Medical Corporation, Qatar
- **Adaptive Security Architecture Trends in 2016**
  Dr. Thieyacine Ely Fall, Qatar University
- **Cyber Security Education – the Gulf MOOC Experience**
  Dr. Arosha Bandara, The Open University, UK

15:00-15:15: Coffee Break

15:15-15:55: Session 5 - Panel Discussion

- **"International and commercial dimensions of cyber security research"**
  - John Taylor McEntire, Director of IP Commercialization, QF
  - Dr. Munir Tag, Director - ICT, QNRF
  - Dr. Ali Sanousi, Executive Chief Medical Information Officer, HMC
  - Dr. Khaled Khan, Editor-in-Chief of the International Journal of Secure Software Engineering, QU
  - Dr. Marc Dacier, Research Director, Cyber Security Group, QCRI / HBKU, QCRI
  - Dr. Hoda A.Alkhzaimi, Director of Center for Cyber Security & Research Assistant Professor, Center for Cyber Security, New York University/Abu Dhabi
  - Prof. Ernesto Damiani, Chair of the Information Security Group and Program, Khalifa University, UAE

15:55-16:00: Close

Keynote Talks

IoT security: what are we talking about?

Dr. Marc Dacier, Research Director, Cyber Security Group, QCRI / HBKU, Qatar

IoT security is a very hot buzzword these days when it comes to new research directions. Unfortunately, it is very ill defined and it is not always clear which, if any, new problem needs to be tackled in that area. This talk will offer a brief overview of what IoT is (or not) as well as of IoT security. It will offer a generic framework to think about it and highlight a couple of new interesting research threads.

Controlling Data Leakage and Theft in Big Data Applications

Prof. Ernesto Damiani, Chair of the Information Security Group, Khalifa University, UAE

In Big Data environments, information is made available as huge data sets or streams, collected and analyzed at different locations, asynchronously and under the responsibility of different authorities. It has become common for such data to be de-normalized, replicated and shuffled in other to boost performance of Big Data applications. Intuition suggests that such Big Data techniques may also boost security risks; for example they may: increase leakage risk by increasing the value for the attacker per unit of information leaked; or increase intrusion risk, making injection attacks (i.e. attacks aimed at poisoning data for subverting the outcome of analytics) more effective per unit of poisoned information injected. However, no clear methodology is currently available for quantifying the impact of these boosters. This talk will discuss a (semi-)quantitative technique for computing Big Data leakage risk estimates, in order to meaningfully compare them with the quantifiable benefits of semantic enrichment. Also, it will discuss a model and a toolkit for protecting data streams based on the idea of dynamic filters, incrementally built based on the applicable Access Control policy and on the analytics to be performed.