The 2018 International Workshop on the Internet of Things Cybersecurity and Safety (ITCS 2018)

Dong Seong Kim, Huy Kang Kim

Outline

- Workshop organizers introduction
- Health and Safety briefing
- Participants introduction
  - Name, affiliation and research interests
- MBIE/NRF research project introduction
  - **Advanced Security Technologies for the Internet of Things**
- Discussions

Advanced Security Technologies for the Internet of Things

Lead PIs: Huy Kang Kim (Korea University),

Dong Seong Kim (University of Canterbury)

Co-PIs: HyoungShick Kim (SKKU),

JiWon Yoon (Korea University),

Julian Jang-Jaccard (Massey University),

Ian Welch (Victoria University of Wellington),

William Liu (Auckland University of Technology)

Sponsor:

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

NRF 한국연구재단 National Research Foundation of Korea

Advanced Security Technologies for the Internet of Things

- Funded by
  - The Ministry of Business, Innovation and Employment (MBIE) of New Zealand, September 2017 Catalyst: Strategic Investment Round
    - $515,002.02 NZD total (GST incl.)
  - The National Research Foundation of Republic of Korea

- Project duration: three years (19/Feb/2018 to 18/Feb/2021)

Advanced Security Technologies for the Internet of Things

- Motivation:
  - The IoT is being used in numerous applications including Agribusiness, Smart home/cities, connected/autonomous vehicles, Digital health.
  - Many researchers expect to see about 20 billion IoT devices by 2020.
  - According to the New Zealand (NZ) IoT alliance, about 14 percent of NZ enterprises have deployed an IoT solution and the IoT could bring up to $2.2 billion economic benefits to New Zealand over the next 10 years through smart cities, agribusiness, health.
  - The biggest concern is that every 'thing' can be hacked.
    - e.g., Mirai malicious software identifies vulnerable IoT devices and launch distributed denial of service attacks on Internet service providers
  - Korea is one of the international leaders in IoT deployment and testbeds which will benefit NZ research team.
  - The IoT embedded with advanced cybersecurity technologies will promote proliferation of the safe use of IoT and will bring a social and economic benefit to NZ and Korea.

Advanced Security Technologies for the Internet of Things

- Main goal: design and test a novel suite of advanced cybersecurity technologies for the Internet of Things (IoT)
- Sub-goals:
  - an automated security risk assessment framework,
  - intrusion detection and response,
  - security incident prediction, and
  - usable security and privacy technologies for the IoT

Sub-goals and focuses.

1. Automated Security Assessment framework:
   - The focus will be on developing a novel framework which integrates security models, measurement, metrics and evaluation methods.
2. Intrusion Detection and Response:
   - The focus will be on developing a novel intrusion detection using machine learning and deep learning technologies and automated response methods.
3. Security Incidents Prediction:
   - The early prediction of cyber attacks incident will be done using electrical signal processing and advanced statistical inference of IoT devices.
4. Usable Security:
   - Usability of the developed security technologies for the IoT will be evaluated via rigorous usability evaluation framework.

Relationships between the sub-goals

- The 'self-learning' intrusion detection and security incident prediction results will be used as an input for the automated security assessment.
- The automated security assessment results will be used to find out optimal intrusion response and prevention.
- The framework, intrusion detection, and security incident prediction will be tested and evaluated by usable security evaluation.

Project deliverables

Sequence	Short title	Type	Start date	End date	Realisation date
1	Secure and Safe Internet of Things	Impact statement	15/01/2018	14/01/2021	
1.1	Cybersecurity Assessment Framework for the IoT	Research aim	15/01/2018	14/01/2021	
1.1.1	Graphical Security Models Development	Critical step	15/01/2018	14/07/2018	
1.1.2	Efficient Evaluation Methods	Critical step	15/07/2018	14/01/2019	
1.1.3	Develop Security metrics for the IoT	Critical step	15/01/2018	14/07/2018	
1.1.4	Develop Performance and Economic metrics for the IoT	Critical step	15/07/2018	14/01/2019	
1.1.5	Develop an integrated tool and Testing	Critical step	15/01/2020	14/01/2021	

Project deliverables (cont.)

1.2	Intrusion Detection and Response for the IoT	Research aim	15/01/2018	14/01/2021	
1.2.1	Threat modeling for autonomous vehicles	Critical step	15/01/2018	14/07/2018	
1.2.2	Designing Infrastructure for the detected attack pattern sharing	Critical step	15/07/2018	14/01/2019	
1.2.3	Implementing signature based intrusion detection system for in-vehicle network	Critical step	15/01/2019	14/07/2019	
1.2.4	Implementing anomaly based intrusion detection system for in-vehicle network	Critical step	15/07/2019	14/01/2020	
1.2.5	Machine learning based self-learning intrusion detection	Critical step	15/01/2020	14/07/2020	
1.2.6	Developing countermeasure by using intrusion prevention system	Critical step	15/07/2020	14/01/2021	

Project deliverables (cont.)

1.3	Malicious Security Event Prediction of IoT networks	Research aim	15/01/2018	14/01/2021	
1.3.1	Exploring efficient acquisition of electrical power signals from IoT devices	Critical step	15/01/2018	14/01/2019	
1.3.2	Intelligent detection and extraction of electrical power signals in a noise multimedia	Critical step	15/07/2018	14/01/2019	
1.3.3	Extracting and combining multiple ENF signals with harmonic characteristics	Critical step	15/01/2019	14/07/2019	
1.3.4	Signal alignment with partially overlapping signals	Critical step	15/07/2019	14/01/2020	
1.3.5	Evaluation of the possibility and applicability to detect and predict security incidents using ENF signal	Critical step	15/01/2020	14/07/2020	
1.3.6	Applying to security incident prediction system with the ENF signal from IoT networks	Critical step	15/07/2020	14/01/2021	

Project deliverables (cont.)

1.4	Usable Security for the IoT	Research aim	15/01/2018	14/01/2021	
1.4.1	Developing IoT threat models for casual users	Critical step	15/01/2018	14/07/2018	
1.4.2	Developing usable and secure IoT applications	Critical step	15/07/2018	14/01/2019	
1.4.3	Developing cybersecurity threat detection systems for IoT applications	Critical step	15/07/2019	14/01/2020	
1.4.4	Developing cybersecurity warning systems for IoT applications	Critical step	15/07/2019	14/01/2020	
1.4.5	Translating users' security requirements into security rules for IoT applications	Critical step	15/01/2020	14/07/2020	
1.4.6	Developing formal security and usability evaluation metrics	Critical step	15/07/2020	14/01/2021	

Workshop program

09:00 – 09:30	Opening and Introduction (Dr DongSeong Kim and Dr Huy Kang Kim)
09:30 – 10:30	Keynote 1 (Chair: Dr Dong Seong Kim) Speaker: Dr Surya Nepal, Data61/CSIRO, Australia Title: IoT security
10:30 – 11:00	Coffee/Tea Break
11:00 – 11:30	Talk 1 (Chair: Dr Ian Welch) Speaker: Dr Dong Seong Kim, University of Canterbury, New Zealand Title: IoT security modelling and analysis
11:30 – 12:00	Talk 2 (Chair: Dr William Liu) Speaker: Dr Huy Kang Kim, Korea University, South Korea Title: IoT security: Intrusion Detection for Autonomous Vehicles
12:00 – 13:00	Lunch (in Engineering Core, Room 120)

Workshop program (cont.)

13:00 – 13:30	Talk 3 (Chair: Dr Julian Jang-Jaccard) Speaker: Hwang, Tae Yoon, (A student from Dr Ji Won Yoon's group, Korea University, South Korea) Title: Recent trends of malware and their analysis in IoT
13:30 – 14:00	Talk 4 (Chair: Dr Dong Seong Kim) Speaker: Dr Dong Joo Kang Title: IoT security – Autonomous Operation and Anomaly Detection Scheme in Home IoT based Energy Management System
14:00 – 14:30	Talk 5 (Chair: Dr Dong Seong Kim) Speaker: Dr Ian Welch, Victoria University of Wellington, New Zealand Title: Towards Secure Smart Home IoT: Manufacturer and User Network Access Control Framework
14:30 – 15:00	Coffee/Tea Break
15:00 – 15:30	Talk 6 (Chair: Dr Huy Kang Kim) Speaker: Dr Julian Jang-Jaccard, Massey University, New Zealand Title: Benchmarking the Performance of CP-ABE Schemes for Lightweight Internet-of-Things (IOT) Devices
15:30 – 16:00	Talk 7 (Chair: Dr Dong Joo Kang) Speaker: Dr William Liu Title: Building the Resilient and Energy-efficient Internet of Things (IoT) Networks.
16:00 – 17:00	Discussions and Wrap-up.
17:30 – 20:00	Dinner (at Shilling Club) and Social Networking