The 2019 International Workshop on the Internet of Things Cybersecurity and Safety (ITCS 2019)

Local organizer: Julian Jang-Jaccard

Co-organizers: Dongseong 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), Fabian Gilson (University of Canterbury)

Co-PIs:

Dong Seong Kim (University of Queensland/University of Canterbury)

HyoungShick Kim (SungKunKwan University),

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 and progress

Sequence	Short title	Type	Start date	End date	Progress
1	Secure and Safe Internet of Things	Impact statement	15/1/2018	14/01/2021	
1.1	Cybersecurity Assessment Framework for the IoT	Research aim	15/1/2018	14/01/2021	
1.1.1	Graphical Security Models Development	Critical step	15/1/2018	14/07/2018	100%
1.1.2	Efficient Evaluation Methods	Critical step	15/7/2018	14/01/2019	100%
1.1.3	Develop Security metrics for the IoT	Critical step	15/1/2019*	14/07/2019*	15%
1.1.4	Develop Performance and Economic metrics for the IoT	Critical step	15/7/2019*	14/01/2020*	
1.1.5	Develop an integrated tool and Testing	Critical step	15/1/2020	14/01/2021	

*The dates have been incorrected recorded in the proposal. The current table shows the correct dates.

Project deliverables and progress (cont.)

Sequence	Short title	Type	Start date	End date	Progress
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	100%
1.2.2	Designing Infrastructure for the detected attack pattern sharing	Critical step	15/07/2018	14/01/2019	100%
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 and progress (cont.)

Sequence	Short title	Type	Start date	End date	Progress
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	100%
1.3.2	Intelligent detection and extraction of electrical power signals in a noise multimedia	Critical step	15/07/2018	14/01/2019	100%
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 and progress (cont.)

Sequence	Short title	Type	Start date	End date	Progress
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	100%
1.4.2	Developing usable and secure IoT applications	Critical step	15/07/2018	14/01/2019	100%
1.4.3	Developing cybersecurity threat detection systems for IoT applications	Critical step	15/07/2019	14/07/2020	
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

Aug 9th (Friday) : Round Room, Atrium Building	
8:45 – 9:20 am	Greeting & catch up (light breakfast available)
9:20 - 9:30 am	Opening and Introduction (either Julian, or DS/HKK)
9:30-10:00am	Talk 1 (Chair: Julian Jang-Jaccard) Speaker: Ian Welch (University of Victoria Wellington, NZ) Title: Automatic generation of IoT policies
10:00-10:30am	Talk 2 (Chair: Julian Jang-Jaccard) Speaker: Dong Joo Kang (Korea University, Korea) Title: Anomaly Detection System based on Cross-sectional Data from Renewable Energy Farm in the framework of CPS (Cyber-Physical System)
10:30-11:00am	Coffee/tea break
11:00-11:30am	Talk 3 (Chair: Huy Kang Kim) Speaker: Hooman Alavizadeh (Massey University, NZ) Title: An Automated Security Analysis Framework and Implementation for Cloud
11:30-12:00pm	Talk 4 (Chair: William Yu) Speaker: Ke He (University of Canterbury, NZ) Title: IoT devices Malware Detection using Deep Learning Techniques
12:00 – 1:00pm	Lunch

Workshop program (cont.)

	Afternoon session
1:00 – 1:30pm	Talk 5 (Chair: Ian Welsh) Speaker: Taeyong Hwang (Korea University, Korea) Title:
1:30 – 2:00pm	Talk 6 (Chair: Dong Joo Kang) Speaker: Yuanyuan Wei (Massey University, NZ) Title: MSD-Kmeans: A Novel Algorithm for Efficient Detection of Global and Local Outliers for IoT Applications
2:00 – 2:30pm	Talk 7 (Chair: William Yu) Speaker: Bilal Ishfaq (University of Canterbury, NZ) Title: Network Level Defenses for Internet of Things (IoT).
2:30 – 3:00pm	Coffee/tea break
3:00 – 3:30pm	Talk 8 (Chair: Ian Welch) Speaker: Dilli P. Sharma (University of Canterbury, NZ) Title: Moving Target Defenses and Their Applications in the Internet of Things
3:30 – 4:00pm	Talk 9 (Chair: Dongseong Kim) Speaker: William Yu (AUT,NZ) Title: A Resilient and Sustainable IoT Network Architecture
4:00 – 4:30pm	Talk 10 (Chair: Dongseong Kim) Speaker: Hyoungshick Kim (Sungkyunkwan University, Korea) Title: Robustness of Lightning Network in Bitcoin
4:30 – 5:30pm	Discussion and Wrap Up

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

Acknowledgement statement for this project

- This work was made possible by the support of a grant (UOCX1720) from The Ministry of Business, Innovation and Employment (MBIE) of New Zealand, September 2017 Catalyst: Strategic Investment Round.

Collaboration and published co-authored research papers

- Collaboration and co-publications
- Research collaboration between participating the universities
- Inviting other participants from Korea, NZ, other countries in IoT security

The next IoT security workshops (in 2020-2020)

- Probably somewhere else? Wellington or another city (e.g., Sydney or Brisbane)?
  - Who would to volunteer organize this?
  - When is good period of time?

- Who would like to visit South Korea to attend a meeting in South Korea (sometime this December)?

- Any suggestions/comments?

2nd Year Progress Report

- Due date: 22 December 2019
  - Start writing sometime in late November 2019
- Content
  - Plan vs. progress
  - Research outputs
    - Research papers (workshop, conference, journals) and short summary related to the project steps
    - Technical reports
  - Workshop(s) information
  - Students (on-going, completion)
  - International collaborations
    - Visiting from other universities
    - Seminars
    - Etc.
  - Future plan