

**The 6th International Symposium on
Mobile Internet Security**
MobiSec 2022

December 15 – 17, 2022
Jeju Oriental Hotel,
Jeju Island, South Korea



*Jeju Island,
South Korea*

Organized by

KIISC Research Group on 5G Security

Kookmin University Cryptography & Information Security Institute

Hosted by

Korea Institute of Information Security and Cryptology (KIISC)

In Cooperation With

Kookmin University BK21 Four Institute of Information Security Education for Secure Hyperconnected Society

MobiSec 2022 Symposium Organization

Honorary Chair

Okyeon Yi

Kookmin University, South Korea

Advisory Committee Chairs

Souhwan Jung

Soongsil University, South Korea

Kyung-Hyune Rhee

Pukyong National University, South Korea

Jaecheol Ryou

Chungnam National University, South Korea

General Chair

Ilseun You

Kookmin University, South Korea

Organizing Committee Chair

Kiwook Sohn

SSNC, South Korea

Program Committee Chairs

Hwankuk Kim

Sangmyung University, South Korea

Pelin Angin

Middle East Technical University, Türkiye

Poster Chairs

Haehyun Cho

Soongsil University, South Korea

Taek-Young Youn

Dankook University, South Korea

Local Arrangement Chair

Ji Won Kang

Sejong University, South Korea

Publication Chairs

Yuh-Shyan Chen

National Taipei University, Taiwan

Igor Kotenko

SPIIRAS and ITMO University, Russia

Publicity Chair

Hsing-Chung Chen
Siu Ming Yiu

Asia University, Taiwan
The University of Hong Kong, Hong Kong

Web Chair

Jiyeon Kim
Jungsoo Park

Gyeongsang National University, South Korea
Soongsil University, South Korea

Advisory Committee

Xiaofeng Chen
KwangHee Choi
Ik-Kyun Kim
Kibom Kim
Francesco Palmier
Kouichi Sakurai
Antonio Skarmeta
Willy Susilo
Jianhua Yang
Huachun Zhou

Xidian University, China
KISA, South Korea (Executive Director)
ETRI, South Korea (Executive Director)
NSR, South Korea (Executive Director)
University of Salerno, Italy
Kyushu University, Japan
Universidad de Murcia, Spain
University of Wollongong, Australia
Columbus State University, USA
Beijing Jiaotong University, China

Organizing Committee

Hyo-Beom Ahn
Dong-Guk Han
Ki Hyo Nam
Hee-Un Park
Jong-Geun Park
Jung Taek Seo
Jungsuk Song

Kongju National University, South Korea
Kookmin University, South Korea
UMLogics Ltd., South Korea
KISA, South Korea
ETRI, South Korea
Gachon University, South Korea
KISTI, South Korea

Technical Program Committee

Ramón Alcarria
Hiroaki Anada
Philip Virgil Astillo
Ram Basnet
Yuanlong Cao

Universidad Politécnica de Madrid, Spain
Aomori University, Japan
University of San Carlos, Philippines
Colorado Mesa University, USA
Jiangxi Normal University, China

Jorge Bernal Bernabe	University of Murcia, Spain
Dooho Choi	Korea University, South Korea
Michał Choraś	Bydgoszcz University of Science and Technology, Poland
Gaurav Choudhary	Technical University of Denmark, Denmark
Salvatore D'Antonio	University of Naples "Parthenope", Italy
Jianfeng Guan	BUPT, China
Shoichi Hirose	University of Fukui, Japan
Kihun Hong	Soongsil University, South Korea
Huisu Jang	Soongsil University, South Korea
Jongkil Kim	University of Wollongong, Australia
Youngsoo Kim	ETRI, South Korea
Peter Kieseberg	St. Pölten University of Applied Sciences, Austria
Gokhan Kul	University of Massachusetts Dartmouth, USA
Hyun Kwon	Korea Military Academy, South Korea
Manhee Lee	Hannam University, South Korea
Mun-Kyu Lee	Inha University, South Korea
Sokjoon Lee	Gachon University, South Korea
C. Mala	NIT Trichy, India
Alessio Merlo	DIBRIS- University of Genoa, Italy
Ki-Woong Park	Sejong University, South Korea
Sandi Rahmadika	State University of Padang, Indonesia
Vishal Sharma	Queen's University Belfast, UK
Seog Chung Seo	Kookmin University, South Korea
Sang Uk Shin	Pukyong National University, South Korea
SeongHan Shin	AIST, Japan
Tjoa Simon	St. Pölten University of Applied Sciences, Austria
Kunwar Singh	NIT Trichy, India
Kunlin Tsai	Tunghai University, Taiwan
Noriki Uchida	Fukuoka Institute of Technology, Japan

Elena Vlahu-Gjorgievska	University of Wollongong, Australia)
Akihiro Yamamura	Akita University, Japan
Toshihiro Yamauchi	Okayama University, Japan
Naoto Yanai	Osaka University, Japan
Baokang Zhao	National University of Defense Technology, China

Program Overview

Time	Thursday 15th December, 2022	
	Offline Session	Online Session
09:00 ~ 10:15	Session1A: Cloud Security	Session1B: AI Security & Blockchain1
10:15 ~ 10:45	Break	
10:45 ~ 12:00	Session2A: Cryptography and Access Control1	Session2B: AI Security & Blockchain2
12:00 ~ 13:30	Lunch	
13:30 ~ 14:00	Opening Ceremony	
14:00 ~ 15:00	Invited Talk 1: Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation Prof. Kim Kwang Choo (University of Texas at San Antonio, USA)	
15:00 ~ 15:15	Break	
15:15 ~ 16:15	Invited Talk 2: Security Mechanisms for Data Transmission among 5G/6G Networks Prof. Fang-Yie Leu (TungHai University and Ming Chuan University, Taiwan)	
16:15 ~ 16:30	Break	
16:30 ~ 18:00	Session3A: AI Security & Blockchain3	Session3B: Cryptography and Access Control2
Time	Friday, 16th December, 2022	
	Offline Session	Online Session
09:00 ~ 10:15	Session4A: Emerging Mobile Application & Security1	Session4B: IoT Application and Security
10:15 ~ 10:45	Break	
10:45 ~ 12:00	Session5A: Emerging Mobile Application & Security2	Session5B: 5G and 6G Security1
12:00 ~ 13:30	Lunch	
13:30 ~ 14:45	Session6: 5G and 6G Security2	Session6B: Emerging Mobile Application & Security3
14:45 ~ 15:15	Break	
15:15 ~ 16:15	Invited Talk 3: Understanding the cyber exercise Dr. Jungmin Kang (National Security Research Institute, South Korea)	
16:15 ~ 16:30	Break	
16:30 ~ 18:00	Poster Session	
18:30 ~ 20:30	Banquet	
Time	Saturday, 17th December, 2022	
	Offline Session	
09:00 ~ 10:35	Session7: 5G and 6G Security3	
10:35 ~ 11:00	Break	
11:00 ~ 12:35	Session8: AI Security & Blockchain4	
12:35 ~ 12:40	Closing Ceremony	

Session Overview

Day 1: 15th December 2022

Session 1A – Cloud Security

- ❖ **Security requirements and countermeasures in a cloud-native environment**
Youngsoo Kim, Cheolhee Park, Yongyoon Shin, Jonghoon, Lee, and Jong-Geun Park
ETRI, South Korea
- ❖ **KRSIE: An eBPF-based Kubernetes Runtime Security Instrumentation and Enforcement System**
Songi Gwak, Thien-Phuc Doan, and Souhwan Jung
Soongsil University, South Korea
- ❖ **Application Hibernation Framework with Dynamic Throttling of Resource**
Sang-Hoon Choi¹, Seong-Jin Kim¹, Hanjin Park², and Ki-Woong Park¹
¹Sejong University, South Korea
²The Affiliated Institute of ETRI, South Korea
- ❖ **Refining Seccomp Security Profile for Container Hardening**
Linh Nguyen-Thuy, Long Nguyen-Vu, Jungsoo Park, and Souhwan Jung
Soongsil University, South Korea

Session 1B – AI Security & Blockchain1

- ❖ **Multi-objective Deep Reinforcement Learning for Virtual Security Function Placement**
Cong Zhou, Jing Tao, Baokang Zhao, and Baosheng Wang
National University of Defense Technology, China
- ❖ **A Graph Neural Network Detection Scheme for Malicious Behavior Knowledge Base**
Ouyang Liu, Kun Li, Ziwei Yin, and Huachun Zhou
Beijing Jiaotong University, China
- ❖ **Recent Challenges in a New Distributed Learning Paradigm**
Sandi Rahmadika, Bayu Ramadhani Fajri, Geovanne Farell, Ahmaddul Hadi, and Khairi Budayawan
Universitas Negeri Padang, Indonesia

❖ **Parameters Transfer Framework for Multi-domain Fake News Detection**

*Rafał Kozik, Krzysztof Samp, Michał Choraś, and Marek Pawlicki
Bydgoszcz University of Science and Technology, Poland*

Session 2A – Cryptography and Access Control1

❖ **NTT quantum circuit for CRYSTALS-Kyber**

*Gyeongju Song, Kyungbae Jang, Siwoo Eum, Minjoo Sim, and Hwajeong Seo
Hansung University, South Korea*

❖ **AVX512 Crypto : Parallel Implementation methods of Korean Block Cipher using AVX-512**

*Young Ryeol Choi, Hojin Choi and Seog Chung Seo
Kookmin University, South Korea*

❖ **K-XMSS and K-SPHINCS+: Hash based Signatures with Korean Cryptography Algorithms**

*Minjoo Sim, Siwoo Eum, Gyeongju Song, Yujin Yang, Wonwoong Kim, and Hwajeong Seo
Hansung University, South Korea*

❖ **Simulation of Vehicle-to-Vehicle Communication based on selected PQC-DSA**

*Young Beom Kim and Seog Chung Seo
Kookmin University, South Korea*

Session 2B – AI Security & Blockchain2

❖ **A Practical Detection and Defense Scheme against Smart Contract Attacks based on Transaction Features**

Ruichi Yan¹, Guohua Tian¹, Shichong Tan¹, and Zhengtao Jiang²

¹Xidian University, China

²Communication University of China

❖ **A blockchain-based framework for audio copyright deposition**

*Ridong Huang, Jianmao Xiao, Jing Zhao, Yuhang Zhang, Jiangyu Wang, Siqi Chen, Jianyu Zou, and Yuanlong Cao
Jiangxi Normal University, China*

❖ **Identifier Resolution Mechanism based on Blockchain for Industrial Internet**

*Wang Xiuling, Zhu Shuxing, and Zou Biaofei
Beijing Jiaotong University, China*

❖ **A Trust-based Blockchain System for Secured Migration of BLE Devices in IoT Networks**

*E Suresh Babu and A. Aswani Devi
NIT Warangal, India*

Session 3A – AI Security & Blockchain3

❖ **An Explainable Cyberattack Alert Framework using Knowledge Graph Construction and Reinforcement Learning**

*Kunyoung Kim, Jeongbin Lee, Jongmo Kim, and Mye Sohn
Sungkyunkwan University, South Korea*

❖ **Practical Machine Learning-based Software Vulnerability Discovery for Internet of Things**

*So-Eun Jeon, Sun-Jin Lee and Il-Gu Lee
Sungshin Women's University, South Korea*

❖ **Malicious traffic classification techniques utilizing compressed sensing and learning for secure Internet of Things**

*Yu-Rim Lee, Na-Eun Park, Seo-Yi Kim, and Il-Gu Lee
Sungshin Women's University, South Korea*

❖ **Incremental Learning for Personalized Development of Personalized Activity Recognition Model using Incremental Learning**

*Jeongbin Lee, Jaewoong Kang, and Mye Sohn
Sungkyunkwan University, South Korea*

❖ **Machine Learning-based Endpoint Detection and Response Framework against Intelligent Cyber Attacks**

*Sun-Jin Lee, So-Eun Jeon and Il-Gu Lee
Sungshin Women's University, South Korea*

Session 3B – Cryptography and Access Control2

❖ **Using Machine Learning for Detecting Timing Side-Channel Attacks in Software-Defined Networks**

*Faizan Shoaib, Yang-Wai Chow, Elena Vlahu-Gjorgievska, and Chau Nguyen
University of Wollongong, Australia*

❖ **Theoretical and Deep Learning Based Analysis of Biases in Salsa 128 bits**

*SK Karthika and Kunwar Singh
NIT Tiruchirappalli, India*

- ❖ **A Blockchain-Assisted Searchable Lightweight CP-ABE for IoT**
Peng Liu, Qian He, Siyuan Liu, Jianing Li, and Zhongyi Zhai
Guilin University of Electronic Technology, China
- ❖ **Blockchain-based Terminal Access Control in Software Defined Network**
Bingcheng Jiang, Qian He, Qi Pan, and Mingliu He
Guilin University of electronic and technology, China
- ❖ **A Token-Based Access Control Mechanism for the Internet of Things Using Blockchain**
Yuzheng Yang, Zhe Tu, Haoxiang Song, and Huachun Zhou
Beijing Jiaotong University, China

Day 2: 16th December 2022

Session 4A – Emerging Mobile Application & Security1

- ❖ **Single-Frame-Based Data Compression for CAN Data Authentication**
Shiyi Jin¹, Dong-Hyun Seo², Yeon-Jin Kim³, Youn-Eun Kim³, Samuel Woo⁴, and Jin-Gyun Chung¹
¹Jeonbuk National University, South Korea
²Jeonbuk Institute of Automotive Convergence Technology, South Korea
³Korea Automotive Technology Institute, South Korea
⁴Dankook University, South Korea
- ❖ **ReplayFuzzer: IoT attack replay analysis platform based on IoT virtualization**
Hye Lim Jung and Ki-Woong Park
Sejong University, South Korea
- ❖ **Low Power High Performance Security Mechanism for Internet of Things**
Sun-Woo Yun, Na-Eun Park, and Il-Gu Lee
Sungshin Women's University, South Korea
- ❖ **A practical method for identifying ECUs using differential voltage**
Jungho Lee¹, Samuel Woo¹, and Yousik Lee²
¹Dankook University, South Korea
²ETAS Korea Co. Ltd, South Korea

Session 4B – IoT Application and Security

❖ **Hybrid Deep Learning Approaches for Gait-based Continuous Authentication using Wearable Sensors**

Sakorn Mekruksavanich¹, Ponnipa Jantawong¹, and Anuchit Jitpattanakul²

¹University of Phayao, Thailand

²King Mongkut's University of Technology North Bangkok, Thailand

❖ **Web API Verifier for IoTtalk and Its Applications**

Wen-Yu Lin, Min-Zheng Shieh, and Yi-Bing Lin

National Yang Ming Chiao Tung University, Taiwan

❖ **Proposal of Early Landslide Warning System considering Scalability and Reliability with Emergent IoT Data Priority**

Noriki Uchida¹, Shigeyuki Endo¹, Tomoyuki Ishida¹, Hiroaki Yuze², and Yoshitaka Shibata³

¹Fukuoka Institute of Technology, Japan

²University of Shizuoka, Japan

³Iwate Prefectural University, Japan

❖ **WebThingsTalk: An IoTtalk adapter for WebThings devices**

Yu-Ching Chen and Min-Zheng Shieh

National Yang Ming Chiao Tung University, Taiwan

Session 5A – Emerging Mobile Application & Security2

❖ **Automated Dynamic Analysis Scheme for Unpacking Malware**

Minho Kim, Gwangyeol Lee, Haehyun Cho, and Jeong Hyun Yi

Soongsil University, South Korea

❖ **Deriving IoT Botnet Defense Technique Using MITRE ATT&CK-D3FEND**

Donghyun Kim, Jiho Shin, and Jung Taek Seo

¹Gachon University, South Korea

²Korean National Police University, South Korea

❖ **Framework for Analyzing Abnormal Behavior of Drones through Simulation Parallelization**

Sung-Kyu Ahn, Hyelim Jung, and Ki-Woong Park

Sejong University, South Korea

❖ **A Framework for Security Attack Detection and Root Cause Analysis based on Elastic Stack**

Hyojoung Shin and Moohong Min

Sungkyunkwan University, South Korea

Session 5B – 5G and 6G Security1

- ❖ **Security SFC Path Selection Using Deep Reinforcement Learning**
Shuangxing Deng, Man Li, Qi Guo, and Huachun Zhou
Beijing Jiaotong University, China
- ❖ **Attacks Against Security Context in 5G Network**
Zhiwei Cui¹, Baojiang Cui¹, Li Su², Haitao Du², Hongxin Wang¹, and Junsong Fu¹
¹Beijing University of Posts and Telecommunications, China
²China Mobile Research Institute
- ❖ **Deployment approach for securing NetApp onboarding in 5G**
Ana Hermosilla¹, Jorge Gallego-Madrid¹, Antonio Skarmeta¹, Pedro Martinez-Julia², and Ved Kafle²
¹Odin Solutions, S.L, Spain
²National Institute of Information and Communications, Japan
- ❖ **Spatial multiplexing techniques and multifrequency cells for massive-type communications in future 6G networks**
Borja Bordel Sánchez^{1,3}, Ramón Alcarria^{1,3}, Joaquin Chung¹, and Ivan Armuelles Voinov²
¹Argonne National Laboratory, USA
²Universidad de Panamá, Panamá
³Universidad Politécnica de Madrid, Spain

Session 6A – 5G and 6G Security2

- ❖ **A Method to Train DDoS Detection Models for Insufficient 5G Traffic with GAN and SMOTE**
YeaSul Kim and Hwankuk Kim
SangMyung University, South Korea
- ❖ **A study on machine learning-based false base station detection method in 5G**
Hoonyong Park¹, Daehyeon Son², Gunwoo Kim², and Ilsun You²
¹Soonchunhyang University, South Korea
²Kookmin University, South Korea
- ❖ **Procedure Collision Testing for 5G SA Network**
Yeongbin Hwang, Mincheol Son, and Yongdae Kim
KAIST, South Korea
- ❖ **Building and utilizing small-scale testbed for research on 5G SA network-related security vulnerabilities**
Dowon Kim^{1,2}, Ilsun You², Seongmin Park^{1,2}, and Sungmoon Kwon¹
¹KISA, South Korea
²Kookmin University, South Korea

Session 6B – Emerging Mobile Application & Security3

- ❖ **DyBAnd: Dynamic Behavior-Based Android Malware Detection**
Shashank Jaiswal¹, Vikas Sihag¹, Gaurav Choudhary², and Nicola Dragoni²
¹Sardar Patel University of Police, Security and Criminal Justice, India
²Technical University of Denmark (DTU), Denmark
- ❖ **Detecting Account Level Disinformation Based on Facebook Platform by Social Robot**
Huan-Chieh Tseng, Min-Yuan Ho, Tzer-Shyong Chen, Yu-Fang Chung, Chun-Ming Lai and Bo-Wei
TungHai University, Taiwan
- ❖ **A Novel Co-operative Traffic Congestion Level Estimation Scheme for Diverse Regions in VANET**
Manipriya Sankaranarayana¹ and Mala. C²
¹IIT Sri City, China
²NIT Tiruchirappalli
- ❖ **The Enhancement of FlexE Network Performance Based On Network Calculus Theory**
Gao Kaiqiang¹, Wang Zhihui¹, Pan Juan¹, Pang Yuhang¹, Wei Lei², and Jiang Song²
¹China Electric Power Research Institute Co. Ltd, China
²State Grid Jiangsu Electric Power Co. Ltd, China

Day 3: 17th December 2022

Session 7 – 5G and 6G Security3

- ❖ **A Systematic Approach to Security Management in the MonB5G Architecture**
Slawomir Kuklinski^{1,2} and Jacek Wytrowski¹
¹Warsaw University of Technology, Poland
²Orange Polska, Poland
- ❖ **A Study on 5G Security Activities in Japan**
SeongHan Shin
National Institute of Advanced Industrial Science and Technology (AIST), Japan

- ❖ **A Secure Data Encryption Method for Mobile Edge Computing**
Kun-Lin Tsai, Tzu-Chen Liu, Shao-tang Lin, Fang-Yie Leu, Yu-Chia Lin, and Ming-Wun Chiang*
Tunghai University, Taichung, Taiwan
- ❖ **A Study on Botnet Attack Formulation Technique for 5G Massive IoT Targets**
Hojun Jin¹, Jiho Shin², and Jung Taek Seo¹
¹Gachon University, South Korea
²Korean National Police University, South Korea
- ❖ **Shannon Entropy Mixing Cumulative Sum Algorithm for DoS/DDoS Detection and Defense**
Shih-Ting Chiu¹, Heru Susanto², and Fang-Yie Leu¹
¹ThungHai University, Taiwan
²Universiti Teknologi Brunei, Indonesia

Session 8 – AI & Blockchain Application4

- ❖ **A Blockchain-based Secure and Fair Decentralized Data Trading System**
Youngho Park, Mi Hyeon Jeon, and Sang Uk Shin
Pukyong National University, South Korea
- ❖ **A Study on PLC Data Integrity Verification Using Private Blockchain**
ChangHyun Roh¹, Ilhwan Ji¹, Jiho Shin², and Jung Taek Seo¹
¹Gachon University, South Korea
²Korean National Police University, South Korea
- ❖ **Privacy Protection Data Delivery Scheme**
Akihiro Yamamura
Akita University, Japan
- ❖ **A Secure Dataset Distribution Protocol for An Accountable AI Collaboration System**
Siwan Noh and Kyung-Hyune Rhee
Pukyong National University, South Korea
- ❖ **Trends in Personalized Federated Learning: Concept, Methods, and Challenges**
Muhammad Firdaus and Kyung-Hyune Rhee
Pukyong National University, South Korea

Poster Session

Poster Session – Poster Papers

- ❖ **POSTER: Threshold Implementation of Lightweight Block Cipher PIPO**
Yeon-Jae Kim and Dong-Guk Han
Kookmin University, South Korea
- ❖ **POSTER: Deep-Learning-based Key Generation Mechanism using Sensor Data collected from IoT Devices**
Yong Woo Lee, Jejin Jo, Jun Seob Kim, Mee Lan Han and Dooho Choi
Korea University, Sejong, South Korea
- ❖ **POSTER: Renewable Electricity Certificates using Smartmeter and BlockChain**
Yuki Satou, Szilard Zsolt Fazekas and Akihiro Yamamura
Akita University, Japan
- ❖ **POSTER: Metaverse-based Counseling System to Protect the Identity of Clients**
Jun Lee, Hanna Lee, Seongchan Lee and Hyun Kwon
Hoseo University, South Korea
- ❖ **POSTER: Packet Sequence-based Intrusion Detection System for In-Vehicle CAN Bus Network**
Seungmin Lee, Hyunghoon Kim, Haehyun Cho and Hyo Jin Jo
Soongsil University, South Korea
- ❖ **POSTER: Blockchain Applied 5G Authentication and Key Agreement Evaluation**
Hoseok Kwon, Gunwoo Kim, Ajung Im, Bonam Kim and Ilsun You
Kookmin University, South Korea
- ❖ **POSTER: Delegatable Searchable Encryption with Proof-of-work**
Jongkil Kim
Ewha Womans University, South Korea
- ❖ **POSTER: Merging Method to Prevent Identification of Pseudonym Information: Elliptical Curve Diffie-Hellman Key Exchange**
Myeong-Hyeon Kim and Taek-Young Youn
Dankook University, South Korea

- ❖ **POSTER: Formal Security Analysis for TLS 1.3 using AVISPA tool**
Jongmin Oh, Daehyeon Son, Jiyeon Kim and Ilsun You
Kookmin University, South Korea

- ❖ **POSTER: A Study on the Deep-Learning-Based Video Surveillance and Management System in Security and Dangerous Facilities**
Jeong Jaehyeok, Choi Yourak and Park Taejin
Sangmyung University, South Korea

- ❖ **POSTER: A Study on Analyzing Build Properties for Android Emulator Detection**
Il-kyu Kim, Jae-do Lim, Namsu Kim, Boojoong Kang and Seong-je Cho
Dankook University, South Korea

- ❖ **POSTER: Development of Security Evaluation Tools for Key Sensors in Autonomous Vehicles**
Jungho Ju, Dongchan Ham and Samuel Woo
Dankook University, South Korea

- ❖ **POSTER: Improving facial expression recognition using contactless sensing data**
Youngeun An, Jimin Lee, EunSang Bak and Sungbum Pan
Chosun University, South Korea

- ❖ **POSTER: Dynamic Monitoring and Surveillance of Anomaly Detection for Advanced Security Facility using Unsupervised Learning**
Yonghoon Choi, Hwanhee Jung and Minsuk Kim
Sangmyung University, South Korea

- ❖ **POSTER: Unified framework for the cybersecurity management system and software update management system**
Yunkeun Song and Samuel Woo
Dankook University, South Korea

- ❖ **POSTER: Cyber Security Management System (CSMS) Requirements: Requirements Analysis**
Junhee Oh and Samuel Woo
Dankook University, South Korea

- ❖ **POSTER: Application Vulnerability Analysis of AI Security using Fully Homomorphic Encryption**
Inpyo Hong, Gyuho Choi and Chang Choi
Gachon University, South Korea

- ❖ **POSTER: Side Channel Analysis of Hardware Implementation CRYSTALS-KYBER Ciphertext Comparison**
Soo-Jin Kim and Dong-Guk Han
Kookmin University, South Korea

- ❖ **POSTER: A Study on Personal Recognition based on Multi-Stream Siamese Network**
Jin Su Kim, Cheol Ho Song and Sungbum Pan
Chosun University, South Korea

- ❖ **POSTER: Electromagnetic and Thermal Information Utilization System to Improve The Success Rate of Laser Fault Injection Attack**
Hye-Won Mun, Jaedeok Ji, and Dong-Guk Han
Kookmin University, South Korea

- ❖ **POSTER: Formal Analysis of Trusted Execution Environment API**
Seunghyun Chae, Geunyeol Yu and Kyungmin Bae
Pohang University of Science and Technology, South Korea

- ❖ **POSTER: A Study on the VMI-based Kernel Runtime Protection System for Virtual Machine in Cloud Environment**
Yeo Reum Jo and Ki-Woong Park
Sejong University, South Korea

- ❖ **POSTER: Security Testing via User Credential-based Attacks against Online Services and Applications**
Jaehyeok Han, Byung Il Kwak, Sangjin Lee and Mee Lan Han
Korea University, Sejong, South Korea

- ❖ **POSTER: Development of attack response and intelligent RSU technology for vehicle security threat prevention**
Sangmin Lee, Keon Yun, Jinhyeok Oh, Sunwoo Yun and Myongcheol Lim
Penta Security, South Korea

- ❖ **POSTER: CNN-based Malware Detection using Opcode Frequency Image**
Ko Seok Min, Jaehyeok Yang, Wonjun Choi and Taeguen Kim
Soonchunhyang University, South Korea

- ❖ **POSTER: Detection and identification of bus-off attacks on In-Vehicle CAN**
Dayoung Kim, Seungmin Lee, Jiwoo Shin, Hyunghoon Kim and Hyo Jin
Soongsil University, South Korea

Invited Talk

Invited Talk1

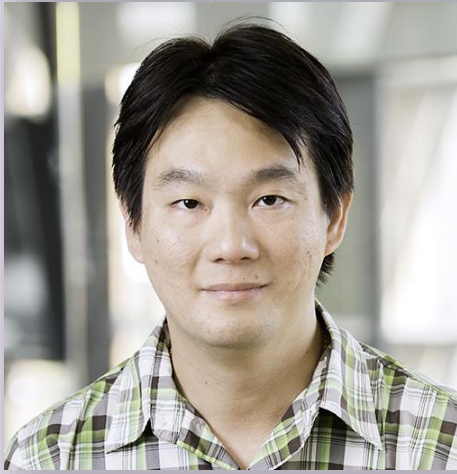
- Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation
Prof. Kim Kwang Choo

Invited Talk2

- Security Mechanisms for Data Transmission among B5G/6G Networks
Prof. Fang-Yie Leu

Invited Talk3

- Understanding the cyber exercise
Dr. Jungmin Kang



Prof. Kim Kwang Raymond Choo

University of San Antonio (UTSA), USA

Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation

The need for cyber resilience is increasingly important in our technology-dependent society, where computing systems, devices and data have been, and will continue to be, the target of cyber attackers, particularly advanced persistent threat (APT) and nation-state / sponsored actors. There are, however, a number of challenges we need to address in the design of a system to facilitate automated vulnerability and risk detection, investigation, and mitigation. In this presentation, we will briefly discuss the role of automation tools (e.g., using artificial intelligence - AI) and human analysts and the design of our Human-in-the-Loop Explainable-AI-Enabled Vulnerability Detection, Investigation, and Mitigation (HXAI-VDIM) system. In our approach, rather than resolving complex scenario of security vulnerabilities as an output of an AI model, we integrate the security analyst or forensic investigator into the man-machine loop and leverage explainable AI (XAI) to combine both AI and intelligence assistant to amplify human intelligence in both proactive and reactive processes. Our goal is that HXAI-VDIM integrates human and machine in an interactive and iterative loop with security visualization that utilizes human intelligence to guide the XAI-enabled system and generate refined solutions.

Speaker bio

Prof. Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA), and is the founding co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research & Practice, and the founding Chair of IEEE Technology and Engineering Management Society (TEMS)'s Technical Committee on Blockchain and Distributed Ledger Technologies. His research has been supported by U.S. funding agencies (NASA, National Security Agency, National Science Foundation, U.S. Department of Defense, U.S. Office of Juvenile Justice and Delinquency, CPS Energy, LGS Innovations, MITRE, Texas National Security Network Excellence Fund) and Australian funding agencies (Australian Government National Drug Law Enforcement Research Fund, Australian Government Cooperative Research Centre for Data to Decision, Lockheed Martin Australia, auDA Foundation, Government of South Australia, BAE Systems stratsec, Australasian Institute of Judicial Administration Incorporated, Australian Research Council), etc



Prof. Fang-Yie Leu

*TungHai University and Ming Chuan University,
Taiwan*

Security Mechanisms for Data Transmission among B5G/6G Networks

Recently, 5G networks have gradually surrounded our living environments to color our everyday lives and make our daily activities more convenient than before. However, in 5G networks (including 5G/B5G/6G), packet P transmitted from local UPF_A of a 5G network, e.g., 5G-A, to UPF_B in P 's destination 5G network, e.g., 5G-B, is not secure, even not encrypted, particularly via the Internet, $A \neq B$. This conducts a risk of data leakage along the connection established between UPF_A and UPF_B . To solve this problem, we propose an architecture that encrypts/decrypts P to prevent it from being attacked. P is encrypted by an edge computer, e.g., EC_A in 5G-A before it is sent to its destination, and decrypted by another edge computer, e.g., EC_B in 5G-B. In this talk, the scenario includes data transmission between two users or among n -party users, $n > 2$. For the former, the cryptography systems used are symmetric and asymmetric encryption/decryption approaches. For the n -party scheme, we adopt Initial Key Agreement (IKA) mechanism which employs Upflow and Downflow processes to establish a secret key for all participating ECs. Besides, message authentication code, and time stamp are also utilized to enhance the security level of data transmission. Moreover, DoS/DDoS and other security issues (for example, 5G AKA, network-slice security) will be also presented in this talk.

Speaker bio

Prof. Fang-Yie Leu received his bachelor, master and Ph.D. degrees all from National Taiwan University of Science and Technology, Taiwan, in 1983, 1986 and 1991, respectively. His research interests include wireless communication, network security, 5G/6G network and Internet of things. He is currently a professor of TungHai University and Ming Chuan University, Taiwan. He also serves as one of the editorial board members of at least 3 international journals and TPC member of at least 10 international conferences. Prof. Leu now organizes MCNCS, CWECS, Future ICT international conferences/workshops. He was also a visiting scholar of Pittsburg University. Prof Leu has published more than 120 high quality journal papers (most of them are indexed by SCI) and at least 200 conference papers (most of them are indexed by EI). Currently, his 5G/6G research focuses on network slicing, DoS/DDoS, and edge computing.



Dr. Jungmin Kang

National Security Research Institute, South Korea

Understanding the cyber exercise

This talk starts with how important cyber exercise is from a national security point of view. Also, the composition of cyber range, how we can build the cyber range, and the generation of ranges in terms of technology are dealt with. Furthermore, the real cyber range being operated in the wild is going to be introduced as well as future work expanding range domain ICS, 5G, Space and so on. Lastly the global cyber competitions and exercises like CCE (Cyber Conflict Exercise), LS (Locked Shields) are being explained.

Speaker bio

Dr. Jungmin Kang has been working for the National Security Research Institute since 2003 in the field of cybersecurity monitoring, ICS security, education and training, international policy and so on. He is General Manager of Cyber Security Training and Exercise Center, NSR. He played a role as a South Korea Delegation to Meridan Conference in 2018, 2017, 2008 dealing with ICS security, delegation to KANZ(Korea, Australia, New Zealand) Technology Summit in 2014, delegation to NATO Emerging Security Challenges Conference in 2011, and delegation to UN GGE(Group of Governmental Experts) Conference in 2011, 2010, 2005 contributing in writing resolution in the context of international security. He received the Ph. D. degree in Cyber security from the Korea University in 2014. He was also an visiting scholar at UC San Diego QI(Qualcomm Institute) visiting scholar in 2015. He worked for Samsung SDS from 2002 and 2003.