

The 22nd World Conference on Information Security Applications

WISA 2021

August 11-August 13, 2021

MAISON GLAD, Jeju Island, Korea
hybrid (on-off mix) conference

Hosted by



Sponsored by



Co-Sponsored by





KEY CONTACTS

General Information

Prof. Kyungho Son

Kangwon National University, Korea

E-mail :khson@kangwon.ac.kr

Technical Program

Prof. Hyounghick Kim

Sungkyunkwan University, Korea

E-mail : hyoung@skku.edu

Registration: KIISC (Korea Institute of Information Security and Cryptology)

Korea Institute of Information Security and Cryptology Seongji Heights 3-Cha Bldg.,
Room 909 507 Nonhyeon-ro(Yeoksam-dong), Gangnam gu, Seoul 06132, Korea

Tel: +82-2-564-9333~4

Fax: +82-2-564-9226

E-mail: kiisc@kiisc.or.kr



The 22nd World Conference on Information Security Applications

WISA 2021

CONTENTS

Committee	2
Keynotes	4
Invited talks	6
Tutorials	9
Conference Program	11
Registration	17

▶ Committee

▶ General Chair

Jaecheol Ryou

Chungnam National University, Korea

▶ Program Committee Chair

Hyounghick Kim

Sungkyunkwan University, Korea

▶ Program Committee

Ki-Woong Park

Sejong University, Korea

Yonghwi Kwon

University of Virginia, USA

Junghwan Rhee

University of Central Oklahoma, USA

Sang Uk Shin

Pukyong National University, Korea

Qiong Huang

South China Agricultural University, China

Seonghan Shin

AIST, Japan

Muhammad Ejaz Ahmed

CSIRO Data61, USA

Simon Woo

Sungkyunkwan University, Korea

Sang Kil Cha

KAIST, Korea

Siqi Ma

The University of Queensland, Australia

Yansong Gao

NJUST, China and CSIRO Data61, Australia

Min Suk Kang

KAIST, Korea

Kyu Hyung Lee

University of Georgia, USA

Dongseong Kim

The University of Queensland, Australia

Joonsang Baek

University of Wollongong, Australia

Kouichi Sakurai

Kyushu University, Japan

Kazumasa Omote

University of Tsukuba, Japan

Younghee Park

San Jose State University, USA

Hsu-Chun Hsiao

National Taiwan University, Taiwan

Ulrich Rührmair

Ruhr University Bochum, Germany

Naoto Yanai

Osaka University, Japan

Toshihiro Yamauchi

Okayama University, Japan

Kangkook Jee

University of Texas at Dallas, USA

Dongwan Shin

New Mexico Tech, USA

Marcus Peinado

Microsoft, USA

Byoungyoung Lee

Seoul National University, Korea

Taejoong Chung

Virginia Tech, USA

Committee ◀

Dooho Choi	Korea University, Korea
Kirill Morozov	University of North Texas, USA
Jin Hong	University of Western Australia, Australia
Eul Gyu Im	Hanyang University, Korea
Ji Won Yoon	Korea University, Korea
Masakatsu Nishigaki	Shizuoka University, Japan
David Mohaisen	University of Central Florida, USA
Hoon Lee	Sungkyunkwan University, Korea
Kevin Koo	Sungkyunkwan University, Korea
Chung Hwan Kim	University of Texas at Dallas, USA
Byung-Chul Choi	ETRI, Korea
Heeseok Kim	Korea University, Korea

► Organizing Committee Chair

Kyungho Son	Kangwon National University, Korea
-------------	------------------------------------

► Organizing Committee

Hyojin Jo	Soongsil University, Korea
Taejin Lee	Hoseo University, Korea
Hwanguk Kim	Sangmyung University, Korea
Changhun Lee	Seoul National University of Science and Technology, Korea
Jin Kwak	Ajou University, Korea
Dongguk Han	Kookmin University, Korea
Jung Taek SEO	Gachon University, Korea
Donghwan Oh	KISA, Korea
Seongjae Lee	KISA, Korea
Byungchul Choi	ETRI, Korea
Yousung Kang	ETRI, Korea
Hyeongcheon Kim	NSR, Korea
Woonyon Kim	NSR, Korea

▶ Keynotes

▶ Keynotes 1



Keynote 1: Ross Anderson (Univ. of Cambridge)

Title: Security Engineering and Machine Learning

Date : August 11, 16:00 PM (UTC+09:00)

Abstract

Statistical machine-learning techniques have been used in security applications for over 20 years, starting with spam filtering, fraud engines and intrusion detection. In the process we have become familiar with attacks from poisoning to polymorphism, and issues from redlining to snake oil. The neural network revolution has recently brought many people into ML research who are unfamiliar with this history, so it should surprise nobody that many new products are insecure. In this talk I will describe some recent research projects where we examine whether we should try to make machine-vision systems robust against adversarial samples, or fragile enough to detect them when they appear; whether adversarial samples have constructive uses; how we can do service-denial attacks on neural-network models; on the need to sanity-check outputs; and on the need to sanitise inputs. We need to shift the emphasis from the design of "secure" ML classifiers, to the design of secure systems that use ML classifiers as components.

Biography

Ross Anderson is Professor of Security Engineering at Cambridge University. He is one of the founders of a vigorously-growing new academic discipline, the economics of information security. Ross was also a seminal contributor to the idea of peer-to-peer systems and an inventor of the AES finalist encryption algorithm "Serpent". He also has well-known publications on many other technical security topics including hardware tamper-resistance, emission security, copy-right marking, and the robustness of application programming interfaces (APIs). He is a Fellow of the Royal Society, the Royal Academy of Engineering, the IET and the IMA. He also wrote the standard textbook "Security Engineering-a Guide to Building Dependable Distributed Systems".

▶ Keynotes 2



Keynote 2: Surya Nepal (CSIRO Data61)

Title: Building Trustworthy Deep Neural Networks

Date : August 12, 13:30 PM (UTC+09:00)

Abstract

Backdoor attacks insert hidden associations or triggers to the deep learning models to override correct inference such as classification and make the system perform maliciously according to the attacker-chosen target while behaving normally in the absence of the trigger. As a new and rapidly evolving realistic attack, it could result in dire consequences, especially considering that the backdoor attack surfaces are broad. This talk first provides a brief overview of backdoor attacks, and then present countermeasures towards building trustworthy deep neural networks.

Biography

Dr Surya Nepal is a Senior Principal Research Scientist at CSIRO Data61. He currently leads the distributed systems security group comprising 30+ research staff and 50+ postgraduate students. His main research focus is on the development and implementation of technologies in the area of cybersecurity and privacy, and AI and Cybersecurity. He has more than 250 peer-reviewed publications to his credit. He is a member of the editorial boards of IEEE Transactions on Service Computing, ACM Transactions on Internet Technology, IEEE Transactions on Dependable and Secure Computing, and Frontiers of Big Data- Security Privacy, and Trust. He is currently a deputy research director of Cybersecurity Cooperative Research Centre (CRC), a national initiative in Australia.

▶ Invited talks

▶ Invited talks 1



Invited Talk 1: Yonghwi Kwon (Virginia Univ.)

Title: Program Analysis for Security

Date : August 12, 11:00AM (UTC+09:00)

Abstract

Program analysis is the automated process of analyzing the behavior of computer programs both statically and dynamically. Over the years, we have seen various applications of program analysis, including malware analysis, vulnerability analysis, software testing, etc. As we virtually live with computer systems, the importance of secure and correct programs and program analysis techniques improve those properties. In this talk, I will present two recent projects of program analysis solving security problems: malware analysis and swarm security. First, I will present the difficulties in web-server-based malware analysis techniques and our solution to effectively expose malicious behaviors. We propose a novel concept of cooperative counter-factual executions. Second, we will discuss how the concept of counter-factual causality can be used in the context of robotics. We introduce a testing technique that can effectively and efficiently test swarm robotics, finding and fixing configuration bugs in swarm algorithms.

Biography

Yonghwi Kwon is an assistant professor of computer science at the University of Virginia. He is broadly interested in solving system security problems via program analysis. He is a recipient of the two ACM Distinguished Paper Award in 2019 and 2013, NSF CRII Award in 2018, Maurice H. Halstead Memorial Award in 2017, IEEE/ACM Automated Software Engineering (ASE) Best Paper Award in 2013.

▶ Invited talks 2



Invited Talk 2: Yang Zhang (CISPA)

Title: Quantifying Privacy Risks of Machine Learning Models

Date : August 13, 09:00 AM (UTC+09:00)

Abstract

Machine learning has made tremendous progress during the past decade. While continuing to improve our daily lives, recent research shows that machine learning models are vulnerable to various privacy attacks. In this talk, I'll cover our two recent works on quantifying the privacy risks of machine learning models. First, I will talk about some recent development of membership inference, including membership inference with only labels and attacks against machine unlearning. Second, I will present our work on the first link stealing attacks against graph neural networks.

Biography

Yang Zhang is a faculty member at CISPA Helmholtz Center for Information Security, Germany. Previously, he was a group leader at CISPA. He obtained his Ph.D. degree from University of Luxembourg in November 2016. Yang's research interests lie at the intersection of privacy and machine learning. Over the years, he has published multiple papers at top venues in computer science, including WWW, CCS, NDSS, and USENIX Security. His work has received NDSS 2019 distinguished paper award. Yang has served in the technical program committee of USENIX Security 2022 2021, ACM CCS 2021 2020 2019, WWW 2021 2020, and PETS 2022 2021 2020.

▶ Invited talks

▶ Invited talks 3



Invited Talk 3: Eun Jung Kim (Texas A&M Univ.)

Title: Preventing Cache Leakage from Spectre and Meltdown Attacks

Date : August 13, 10:00 AM (UTC+09:00)

Abstract

Recently the Spectre and Meltdown vulnerabilities have shaken the computing industry to its core, showing that security is not only a software problem, but that the vulnerabilities exist in the design of modern processors and allow for sensitive information such as passwords and e-mail contents to be read from memory. These attacks take advantage of high performance hardware design features known as Speculative Execution and Branch Prediction. In this talk, I will first introduce these attack examples and I will then discuss an idea to build next generation CPUs to enable secure speculation without sacrificing performance.

Biography

Eun Jung Kim is an associate professor in the Department of Computer Science & Engineering, Texas A&M University, where she has been since 2003. Her research interests include computer architecture, parallel/distributed systems, low-power design, secure computing, performance evaluation, and fault tolerant computing. She is serving as associated editors for IEEE transactions on Computer and IEEE Computer Architecture Letter. She has served as program committee chairs/members for top-tier conferences in the Computer Architecture area. She has published more than 70 scientific papers in leading refereed journals, conferences and book chapters. She has graduated 11 Ph.D. students and 17 M.S. since joining Texas A&M. Dr. Kim received the NSF CAREER Award in 2009. She is a member of the IEEE Computer Society and the ACM.

▶ Tutorials 1



Tutorial 1: Daehee Jang (Sungshin W. Univ.)

Title: OS Command Injection Exercise

Date : August 11, 10:00 AM (UTC+09:00)

Abstract

IoT devices and web applications often provide services by utilizing its underlying OS commands instead of implementing the whole service from scratch. For example, the majority of modern Wi-Fi routers provide network ping service for users to check if their network setup is correct; and its implementation is built on top of existing Linux `ping` command instead of re-implementing the entire ICMP protocol. Re-using OS commands has the benefit of providing fast/accurate service development with minimal engineering effort. However, improper data sanitization exposes such service to OS command injection which is a serious yet easy-to-overlook security flaw. Exploiting OS command injection is way too easy compared to other system exploitation techniques; however, its security impact is high. In this tutorial, I will demonstrate advanced OS command injection techniques against common bash shells and explain how we can bypass various filters/restrictions. Also I will provide a docker-based platform as a small series of CTF/Wargame challenges to practice such exploitation techniques as a lab exercise.

Prerequisites for this tutorial

Tutorial exercises require a web browser such as Chrome. Please prepare an Internet-available laptop if you want to try out the tutorial tasks.

▶ Tutorials

▶ Tutorials 2



Tutorial 2: Hojoon Lee (Sungkyunkwan Univ.)

Title: Isolating and Protecting Sensitive Program Components with Intel SGX

Date : August 12, 16:00 PM (UTC+09:00)

Abstract

Ensuring confidentiality and integrity of sensitive workloads is becoming increasingly more difficult with today's computing systems. Modern software is growing more and more complex and inevitably contains bugs. The presence of vulnerabilities in user programs and even operating system kernels render the protection of secrets a daunting challenge. Trusted Execution Environments (TEEs) ensures confidentiality and integrity of sensitive program code and data by constructing a safe and isolated execution compartment within the system by leveraging hardware support for isolation in modern architectures.

Intel has introduced Software Guard eXtension (SGX) in its processor architecture to provide secure enclaves for protecting program secrets. This tutorial will discuss the security model, design patterns, and applications of SGX. Then, we will write a simple SGX-protected program together to provide a hands-on experience with trusted execution environments.

Prerequisites for this tutorial

This tutorial will require a Linux-based system that can run docker containers. We will provide docker images that have SGX SDK preinstalled. Note that an SGX-capable Intel system is not required since our example will use the simulation mode provided by the SDK. So bring your laptop and make sure you have access to a Linux machine via SSH or a local virtual machine if your laptop is not running Linux already.

Conference Program ◀

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 1 August 11 (Wednesday), 2021

10:00 ~ 12:00	Tutorial 1: OS Command Injection Exercise Daehee Jang (Sungshin W. Univ.) Session Chair: Howon Kim (Pusan National University)
12:00 ~ 13:30	Lunch Break
13:30 ~ 14:30	Session 1 (Crystal Hall I) Session Chair: Haehyun Cho (Soongsil University) LOM: Lightweight classifier for obfuscation methods Jeong-Woo Kim (Chungnam National University), Seoyeon Kang (Chungnam National University), Eun-Sun Cho (Chungnam National University) and Joon-Young Paik (Tiangong University) A Method for Collecting Vehicular Network Data for Enhanced Anomaly Detection Samuel De La Motte (University of Western Australia) and Jin Hong (University of Western Australia) Unsupervised Driver Behavior Profiling leveraging Recurrent Neural Networks Young Ah Choi (Korea University), Kyung Ho Park (SOCAR), Eunji Park (Korea University) and Huy Kang Kim (Korea University)
	Session 2 (Convention Hall) Session Chair: Hyojin Jo (Soongsil University) Quantum Cryptanalysis Landscape of Shor's Algorithm for Elliptic Curve Discrete Logarithm Problem Harashta Tatimma Larasati (Pusan National University) and Howon Kim (Pusan National University) Anonymous IBE from PEKS : A Generic Construction Hyun Sook Rhee (Samsung Electronics) and Dong Hoon Lee (Korea University) Secure Computation of Shared Secrets and Its Applications Xin Liu (University of Wollongong), Willy Susilo (University of Wollongong) and Joonsang Baek (University of Wollongong)

▶ Conference Program

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 1 August 11 (Wednesday), 2021

Poster Session (Online)

A Study on Author Profiling based on Text Mining for Effective Forensic Investigation

Minho Kim (Catholic University of Pusan), Pyo-Gil Hong (Catholic University of Pusan) and Dohyun Kim (Catholic University of Pusan)

High-Speed Software of Karatsuba Multiplication for SABER Round 3 on ARMv8-A Series

Jingyo Song (Kookmin University), Youngbeom Kim (Kookmin University) and Seog Chung Seo (Kookmin University)

Countermeasure to Detecting Memory Forensics Tools and Evading Data Acquisition

Inyeung Kim (Seoul National University of Science and Technology), Seunghee Seo (Seoul National University of Science and Technology), Yeog Kim (Seoul National University of Science and Technology) and Changhoon Lee (Seoul National University of Science and Technology)

ASTFuzz: Generic/Generative Language Fuzzer

Gyeongjin Son (Sungshin W. University), Eunyeong Ahn (Sungshin W. University) and Daehee Jang (Sungshin W. University)

Towards Securing 5G Core Network Functions Using SGX

14:30 ~ 15:30

Heekyung Shin (Sungshin W. University), Jiwoo Kang (Sungshin W. University), Hyeon No (Sungshin W. University) and Seongmin Kim (Sungshin W. University)

Design of Exploit-Helper for Penetrating into a Black-Box System

Jaegyong Ju (Sejong University) and Ki-Woong Park (Sejong University)

XTS-AES Parallel Optimization Implementation Technique for Fast FDE

Sang Woo An (Kookmin University) and Seog Chung Seo (Kookmin University)

PyRos: A State Channel-Based Access Control System for a Public Blockchain Network

Siwan Noh (Pukyong National University) and Kyung-Hyune Rhee (Pukyong National University)

Inference of Compiler Provenance from Malware

Hohyeon Jang (Sungkyunkwan University) and Hyungjoon Koo (Sungkyunkwan University)

A Study on the Analysis of Illegal Content Propagation Path Based on Heavy Uploader

Jingang Kim (Hoseo university), Chanwoong Hwang (Hoseo university) and Taejin Lee (Hoseo university)

A study on the Interpretability of Malware Detection based on Artificial Intelligence

Ahyeon Jeong (Hoseo University), Eunyu Lee (Hoseo University), Hongbi Kim (Hoseo University), Doyeon Kim (Hoseo University) and Taejin Lee (Hoseo University)

Conference Program ◀

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 1 August 11 (Wednesday), 2021

	<p>Poster Session (Online)</p> <p>Fast and Reversible Region-of-interest Hiding Scheme based on Chaotic Map Sung-Won Kang (Pukyong National University), Cho Nwe Zin Latt (Pukyong National University), Zhuohao Qian (Pukyong National University), Seolah Jang (Pukyong National University) and Kyung-Hyune Rhee (Pukyong National University)</p> <p>A Flooding Mitigator for Controller Area Networks Jiwoo Shin (Seoul Women's University), Dongwoo Kang (Soongsil University), Jaewoong Heo (Soongsil University) and Hyo Jin Jo (Soongsil University)</p> <p>Blockchain-Enabled 5G Edge Networks and Beyond: An Intelligent Cross-Silo Federated Learning Approach Sandi Rahmadika (Pukyong National University), Muhammad Firdaus (Pukyong National University), Seolah Jang (Pukyong National University) and Kyung-Hyune Rhee (Pukyong National University)</p>
14:30 ~ 15:30	<p>Consideration for the Construction of the Wireless Covert Timing Channels Hayoung Seong (University of Science and Technology), Yongsung Jeon (Electronics and Telecommunications Research Institute), Lee Sang-Woo (Electronics and Telecommunications Research Institute) and Ikkyun Kim (Electronics and Telecommunications Research Institute)</p> <p>Security Analysis for Eavesdropping with Vo5G Mobile Youngkwon Park (Korea Internet & Security Agency), Seongmin Park (Korea Internet & Security Agency) and Dowon Kim (Korea Internet & Security Agency)</p> <p>Proposal of ZeroNet Content Search Technique Hyunpyo Choi (Gachon University) and Jungtaek Seo (Gachon University)</p> <p>F2FS-Based IoT Filesystem Forensics for Cyber-Physical Systems Sungbum Kim (Ajou University), Wooyeon Jo (Ajou University), Minju Kim (Ajou University) and Taeshik Shon (Ajou University)</p>
15:30 ~ 16:00	Break Time
16:00 ~ 17:00	<p>Keynote 1: Security Engineering and Machine Learning Ross Anderson (Cambridge Univ.) Session Chair: Yongdae Kim (KAIST)</p>

▶ Conference Program

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 2 August 12 (Thursday), 2021

09:30 ~ 10:30	Session 3 (Crystal Hall I) Session Chair: Jong-Hyoun Lee (Sejong University) Adaptive Network Security Service Orchestration based on SDN/NFV Priyatham Ganta (San Jose State University), Kicho Yu (Northeastern University), Dharma Dheeraj Chintala (San Jose State University) and Younghee Park (San Jose State University) A General Framework for Matching Pattern Hiding in Deep Packet Inspection Jinghang Wen (Jinan University), Jianan Liu (Jinan University), Jian Weng (Jinan University), Jiasi Weng (Jinan University) and Axin Wu (Jinan University) A Privacy-Preserving Payment Model for EV Charging Jane Kim (Hanyang University), Soojin Lee (Hanyang University) and Seung-Hyun Seo (Hanyang University)
	Session 4 (Convention Hall) Session Chair: Dowon Kim (KISA) Measuring Healthcare Data Breaches Mohammed Alkinoon (University of Central Florida), Sung Choi Yoo (University of Central Florida) and David Mohaisen (University of Central Florida) BadASLR: Exceptional cases of ASLR aiding Exploitation Daehee Jang (Sungshin W. University) Quantitative Analysis on Attack Capacity in Meltdown-type Attacks Seokmin Lee (Kwangwoon University), Taehun Kim (Korea University) and Youngjoo Shin (Korea University)
	10:30 ~ 11:00 Break Time
	Invited Talk 1: Program Analysis for Security Yonghwi Kwon (Virginia Univ.) Session Chair: Wonsuk Choi (Hansung University)
	12:00 ~ 13:30 Lunch Break

Conference Program ◀

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 2 August 12 (Thursday), 2021

13:30 ~ 14:30	<p>Keynote 2: Building Trustworthy Deep Neural Networks Surya Nepal (CSIRO Data61) Session Chair: Yeonjoon Lee (Hanyang University)</p>
14:30 ~ 15:30	<p>Session 5 (Crystal Hall I) Session Chair: Hyungjoon Koo (Sungkyunkwan University)</p> <p>On the robustness of intrusion detection systems for vehicles against adversarial attacks Jeongseok Choi (Sungkyunkwan University) and Hyoungshick Kim (Sungkyunkwan University)</p> <p>A Framework for Generating Evasion Attacks for Machine Learning based Network Intrusion Detection Systems Raymond Mogg (The University of Queensland), Simon Yusuf Enoch (The University of Queensland) and Dan Kim (The University of Queensland)</p> <p>HAT: Hybrid Adversarial Training for Simultaneous Training of Deep Learning Model and Denoising Network Gwonsang Ryu (Soongsil University) and Daeseon Choi (Soongsil University)</p> <p>Session 6 (Convention Hall) Session Chair: Seung-Hyun Seo (Hanyang University)</p> <p>Pattern Matching over Encrypted Data with a Short Ciphertext Jongkil Kim (University of Wollongong), Willy Susilo (University of Wollongong), Joonsang Baek (University of Wollongong), Intae Kim (University of Wollongong) and Yang-Wai Chow (University of Wollongong)</p> <p>Efficient adaptation of TFHE for high end-to-end throughput Kang Hoon Lee (Korea University) and Ji Won Yoon (Korea University)</p> <p>AnyTRNG: Generic, High-throughput, Low-area True Random Number Generator based on Synchronous Edge Sampling Asep Muhamad Awaludin (Pusan National University), Derry Pratama (Pusan National University) and Howon Kim (Pusan National University)</p>
15:30 ~ 16:00	Break Time
16:00 ~ 18:00	<p>Tutorial 2: Isolating and Protecting Sensitive Program Components with Intel SGX Hojoon Lee (Sungkyunkwan Univ.) Session Chair: Wan Yi (KISA)</p>
18:00 ~ 19:30	Banquet *cancelled due to Covid-19
19:30 ~ 20:00	Best Paper Award *cancelled due to Covid-19

Conference Program

The Main Place: The Crystal hall (2F), Maison Glad Jeju

DAY 3 August 13 (Friday), 2021

09:00 ~ 10:00	Invited Talk 2: Quantifying Privacy Risks of Machine Learning Models Yang Zhang (CISPA) Session Chair: Ki-Woong Park (Sejong University)
10:00 ~ 11:00	Invited Talk 3: Preventing Cache Leakage from Spectre and Meltdown Attacks Eun Jung Kim (Texas A&M Univ.) Session Chair: Joobeom Yun (Sejong University)
11:00 ~ 12:00	Session 7 (Crystal Hall I) Session Chair: Dooho Choi (Korea University) Echo-Guard : Acoustic-based Anomaly Detection System for Smart Manufacturing Environments Chang-Bae Seo (Hanyang University), Gyuseop Lee (Hanyang University), Yeonjoon Lee (Hanyang University) and Seung-Hyeon Seo (Hanyang University) Research on improvement of anomaly detection performance in industrial control systems Sungho Bae (Hoseo University), Chanwoong Hwang (Hoseo University) and Taejin Lee (Hoseo University) ARMed Frodo: FrodoKEM on 64-bit ARMv8 Processors Hyeokdong Kwon (Hansung University), Kyoungbae Jang (Hansung University), Hyunjun Kim (Hansung University), Hyunji Kim (Hansung University), Minjoo Sim (Hansung University), Siwoo Eum (Hansung University), Wai-Kong Lee (Gachon University) and Hwajeong Seo (Hansung University) Session 8 (Convention Hall) Session Chair: Jae Hoon Nah (ETRI) Masked Implementation of PIPO Block Cipher on 8-bit AVR Microcontrollers Hyunjun Kim (Hansung University), Minjoo Sim (Hansung University), Eum Si Woo (Hansung University), Kyoungbae Jang (Hansung University), Gyeong Ju Song (Hansung University), Hyunji Kim (Hansung University), Hyeokdong Kwon (Hansung University), Wai-Kong Lee (Gachon University) and Hwajeong Seo (Hansung University) Parallel Implementation of PIPO Block Cipher on 32-bit RISC-V Processor Yujin Kwak (Kookmin University), Youngbeom Kim (Kookmin University) and Seog Chung Seo (Kookmin University) No Silver Bullet: Optimized Montgomery Multiplication on Various 64-bit ARM Platforms Hwajeong Seo (Hansung University), Pakize Sanal (Florida Atlantic University), Wai-Kong Lee (Gachon University) and Reza Azarderakhsh (Florida Atlantic University)

▶ International Participants Payment Method

We use online registration to complete the registration for participants.

At least one author of each paper/poster must register until August 2, 2021 (UTC+09:00).

Click on the registration page link: <https://kiisc.or.kr/payment/pay/64>

There is no author registration option. Authors are required to register via Online Attendance (Student) or Online Attendance (General Participant).

The online registration fee will cover (a) the access to the online conference and (b) the access to the online proceedings. Please contact kiisc@kiisc.or.kr regarding any issues related to registration and payment

Credit Card

-Use a credit card payment system (EXIMBAY)

Wire Transfer

- beneficiary' name : KIISC
- beneficiary's account number : 754-01-0008-146
- beneficiary's bank : Kookmin Bank
- the branch name : Yeoksamyeok Branch
- SWIFT code : CZNBKRSE
- beneficiary' address : Room 909, Seongji Heights 3-Cha Bldg., 507, Nonhyeon-ro, Gangnam-gu, Seoul, Korea 06132

*This payment method is provided by Eximbay and is billed as www.eximbay.com.

* Note: Please note that the billing descriptor will be listed as EXIMBAY.COM.

▶ Korean Participants 사전등록: 2021년 8월 2일(월)까지

▷ 학회 홈페이지(www.kiisc.or.kr)접속 → 학회행사 → 사전등록바로가기 → WISA 2021 (KOREAN PARTICIPANTS) 클릭 (신용카드/계좌이체 결제 가능)

▷ 사전등록 송금처

- 예금주 : 한국정보보호학회

- 계좌번호 : (국민은행) 754-01-0008-146

* 입금명은 필히 [행사명 첫 글자+ 등록자 성함]으로 기재해 주시기 바랍니다.예) WISA 홍길동 - "W홍길동" 기재

* 사전등록 시 등록비는 위의 계좌로 송금하시고, 입금자가 대리일 경우 통보바랍니다.

* 계산서 신청 시, 익일 안으로 등록하신 이메일로 청구용 계산서가 발행됩니다. 영수용 계산서가필요하신 경우, 사전에 학회로 연락 바랍니다.

* 등록확인서는 한국정보보호학회 홈페이지 상단 행사 등록확인서 바로 가기를 클릭하신 후 등록 시 기재하시 성함과 이메일을 기재하시면 출력 가능합니다.

* 참가확인서는 kiisc@kiisc.or.kr 로 행사명, 성명, 소속을 기재하시어 행사 종료 후 요청하시기 바랍니다.

* 학생은 다른 소속이 없는 전일제(학부생/대학원생)에 한합니다.

* 학생의 경우 kiisc@kiisc.or.kr로 학생증 사본 송부 바랍니다.

▶ Registration

▶ Registration Fees

Offline Attendance	Student	500,000 won
	General Participants	700,000 won
Online Attendance	-	150,000 won (\$140 USD)

(Offline) Registration includes online proceedings, 2 Lunches, 1 Banquet during the conference.

(Online) Registration only includes online proceedings during the conference.

▶ Registration Policy

At least one presenter per accepted paper, poster, or demo must register for the conference.

We are unable to offer refunds, cancellations, or substitutions for any registrations for this event.

▶ Registration Contact Information

Korea Institute of Information Security & Cryptology

- Seongji Heights 3-Cha Bldg., Room 909 507, Nonhyeon-ro, Gangnam-gu, Seoul 06132, Korea

- Tel : +82-2-564-9333(ext.2)

- Fax : +82-2-564-9226

- Email : kiisc@kiisc.or.kr

- Business Registration Number: 114-82-04432