

The 21ST World Conference on Information Security Applications

WISA 2020

August 26-28, 2020

MAISON GLAD, Jeju Island, Korea

Hosted by



Korea Institute of Information
Security & Cryptology

Sponsored by



Ministry of Science and ICT



NIS
National Intelligence
Service Korea

Co-Sponsored by



KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY



NSR
National Security Research Institute



ETRI
Electronics and Telecommunications
Research Institute

KONPA I

KONA
International

WINS

► Greetings from the General Chair

Warmly welcome all of you to the 21st World conference on Information Security and Application (WISA 2020) hosted in Jeju Island. We appreciate and thank you to each and every one of you for being here with us today. WISA, which is hosted by Korea Institute of Information Security & Cryptology (KIISC) -the first security research society in Korea, has become one of the top international security conferences where researchers and engineers in security areas have the opportunity to meet and discuss new ideas and technologies related to information security and applications. This year we are celebrating the 31st anniversary of KIISC, and I would like to take this opportunity to congratulate and express my deepest gratitude for three decades of fruitful works.

I would like to thank all participants around the world who showed their keen cooperation to make WISA 2020 a successful conference. As a General Chair of WISA 2020, I would also like to extend my appreciation, especially, to three research institutes of Korea - KISA (Korea Internet and Security Agency), ETRI (Electronics and Telecommunications Research Institute) and NSR (National Security Research Institute) - for their invaluable contributions to the preparation of this conference.

Due to the undeniable social changes caused by COVID-19, WISA is taking a new path that it has never experienced before. Especially, in order to overcome the obstacles caused by the pandemic, the conference will be held in a mixed way consisting of both live and recorded online presentations. This is clearly an important challenge that will promote WISA to make a meaningful leap forward by extending its scope to online.

WISA 2020 serves as an open forum for exchanging and sharing of an on-going common research interests and results of research, development and applications on information security areas. The program chair, Prof. Ilsun You, Soonchunhyang University, prepared valuable programs along with program committee members, whose countless dedication leads to another new success story of WISA.

We are specially honored to serve you with two keynote talks by Professor Matt Bishop, The University of California, on "An Extended View of Resilience", and Professor Suman Jana, Columbia University, on "Training Verifiably Robust Malware Classifiers". It is also our privilege to have two tutorial talks: from Professor Dan Dongseong Kim, The University of Queensland, on "Graphical Models and Analysis for Cybersecurity" and Doctor SeongHan Shin, National Institute of Advanced Industrial Science and Technology (AIST), on "Authenticated Key Exchange from Weak Secrets". Moreover, this year, WISA 2020 specially includes a poster session which is composed of 39 posters.

The conference has received a total of 81 papers (a 28% increase compared to last year's submission) covering all areas of information security, and among which only 31 papers from 7 countries, with 38% acceptance rate, were chosen after a rigorous review process. Amongst the selected 31 papers and 39 posters, the WISA 2020 selection committee has nominated 6 best papers (2 premium awards, 2 gold awards, 2 silver awards) and 6 best posters (2 premium awards, 2 gold awards, 2 silver awards).

Jeju Island holding WISA 2020 is a wonderful place offering a unique tourist experience as well as the greatest conference itself. I hope all the participants have a delightful experience in the beautiful island of Jeju and share valuable research results in information security applications. Finally, I would like to express my sincere gratitude to each of WISA organizing and program committee members as well as paper contributors. Without their dedication and professionalism, WISA 2020 could not have been held.

August, 2020

Professor Souhwan Jung
General Chair of WISA 2020

Conference Committee ◀

▶ GENERAL CHAIR

Souhwan Jung Soongsil University, Korea

▶ PROGRAM COMMITTEE CHAIR

Il-sun You Soonchunhyang University, Korea

▶ PROGRAM COMMITTEE

| | |
|---------------------|--|
| Pelin Angin | Middle East Technical University, Turkey |
| Joonsang Baek | University of Wollongong, Australia |
| Sang Kil Cha | KAIST, Korea |
| Xiaofeng Chen | Xidian University, China |
| Jin-Hee Cho | Virginia Tech, USA |
| Doocho Choi | ETRI, Korea |
| Swee-Huay Heng | Multimedia University, Malaysia |
| Hsu-Chun Hsiao | National Taiwan University, Taiwan |
| Qiong Huang | South China Agricultural University, China |
| Eul Gyu Im | Hanyang University, Korea |
| Yeongjin Jang | Oregon State University, USA |
| Hiroaki Kikuchi | Meiji University, Japan |
| Dongseong Kim | The University of Queensland, Australia |
| Jong Kim | POSTECH, Korea |
| Jongkil Kim | University of Wollongong, Australia |
| Jonghoon Kwon | ETH Zurich, Switzerland |
| Byoungyoung Lee | Seoul National University, Korea |
| Kyu Hyung Lee | University of Georgia, USA |
| Shengli Liu | Shanghai Jiao Tong University, China |
| Masakatsu Nishigaki | Shizuoka University, Japan |
| Jason Nurse | University of Kent, UK |
| Aziz Mohaisen | University of Central Florida, USA |
| Kirill Morozov | University of North Texas, USA |
| Kazumasa Omote | University of Tsukuba, Japan |
| Ki-Woong Park | Sejong University, Korea |
| Marcus Peinado | Microsoft, USA |
| Junghwan Rhee | NEC Laboratories, USA |

► Conference Committee

| | |
|--------------------|--|
| Ulrich Rührmair | LMU Munich, Germany |
| Kouichi Sakurai | Kyushu University, Japan |
| Junji Shikata | Yokohama National University, Japan |
| Dongwan Shin | New Mexico Tech, USA |
| SeongHan Shin | AIST, Japan |
| Sang Uk Shin | Pukyong National University, Korea |
| Amril Syalim | University of Indonesia, Indonesia |
| Gang Tan | The Pennsylvania State University, USA |
| Samuel Woo | Dankook University, Korea |
| Toshihiro Yamauchi | Okayama University |
| Naoto Yanai | Osaka University, Japan |
| Siu Ming Yiu | The University of Hong Kong, Hong Kong |
| Taek-Young Youn | ETRI, Korea |
| Meng Yu | Roosevelt University, USA |

► ORGANIZING COMMITTEE CHAIR

| | |
|----------------|--------------------------|
| Jong-Hyoun Lee | Sejong University, Korea |
|----------------|--------------------------|

► ORGANIZING COMMITTEE

| | |
|---------------|--|
| Hyo-Beom Ahn | Kongju National University, Korea |
| Kangbin Yim | Soonchunhyang University, Korea |
| Manhee Lee | Hannam University, Korea |
| Jongsung Kim | Kookmin University, Korea |
| Changhoon Lee | Seoul National University of Science and Technology, Korea |
| Jungtaek Seo | Soonchunhyang University, Korea |
| Deok Gyu Lee | Seowon University, Korea |
| Dong-Guk Han | Kookmin University, Korea |
| KyengHwa Do | Konkuk University, Korea |
| Youngho Park | Sejong Cyber University, Korea |
| Ji Sun Shin | Sejong University, Korea |
| Joobeom Yun | Sejong University, Korea |
| Ki-Woong Park | Sejong University, Korea |
| Young-Gab Kim | Sejong University, Korea |
| Daesub Park | Sejong University, Korea |
| Jin Kwak | Ajou University, Korea |



Conference Committee ◀

| | |
|-----------------|--|
| Tai Hyo Kim | Formal Works Inc., Korea |
| Hyoung Chun Kim | NSR, Korea |
| Woo-Nyon Kim | NSR, Korea |
| Yangseo Choi | ETRI, Korea |
| Byung-Chul Choi | ETRI, Korea |
| Jonghyun Kim | ETRI, Korea |
| Jin Cheol Kim | KEPCO Knowledge, Data & Network Co., Ltd., Korea |
| Seoklae Lee | KISA, Korea |
| JungHee Kim | KISA, Korea |
| Soonjoung Byun | KISA, Korea |

► Conference Program

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

DAY 1 August 26 (Wednesday), 2020

| Time \ Room | AUG. 25 (TUE) | AUG. 26 (WED) | |
|-------------|-------------------|--|---|
| | The Jade Hall | The Crystal Hall I | The Crystal Hall II |
| 11:00-12:00 | | Registration | |
| 12:00-13:30 | | Lunch Break | |
| 13:30-14:30 | | Opening Ceremony (The Crystal Hall) | |
| 14:30-15:00 | | Break Time | |
| 15:00-16:30 | Welcome Reception | Session 1 AI Security and Intrusion Detection 1 | Session 2 Steganography and Malware |
| 16:30-17:00 | | Break Time | |
| 17:00-18:30 | | Session 3 Application, System, and Hardware Security 1 | Session 4 Cryptography 1 |

DAY 2 August 27 (Thursday), 2020

| Time \ Room | The Crystal Hall I | The Crystal Hall II |
|-------------|---|--|
| 08:30-09:00 | Registration | |
| 09:00-10:30 | Session 5 Application, System, and Hardware Security 2 | Session 6 Cryptography 2 |
| 10:30-11:00 | Break Time | |
| 11:00-12:00 | Keynote 1: An Extended View of Resilience Prof. Matt Bishop (University of California, Davis, USA) | |
| 12:00-13:30 | Lunch Break | |
| 13:30-14:30 | Keynote 2: Training Verifiably Robust Malware Classifiers Prof. Suman Jana (Columbia University, USA) | |
| 14:30-15:00 | Break Time | |
| 15:00-16:30 | Session 7 Cyber Security | Session 8 Application, System, and Hardware Security 3 |
| 16:30-17:00 | Break Time | |
| 17:00-18:30 | Tutorial 1 Graphical Models and Analysis for Cybersecurity Prof. Dongseong Kim (The University of Queensland, Australia) | Tutorial 2 Authenticated Key Exchange from Weak Secrets Dr. SeongHan Shin (National Institute of Advanced Industrial Science and Technology, Japan) |

Conference Program ◀

DAY 3 August 28 (Friday), 2020

| Room Time | The Crystal Hall I | The Crystal Hall II |
|--------------|---|--|
| 08:30-09:00 | Registration | |
| 09:00-10:30 | Session 9 AI Security and Intrusion Detection 2 | Session 10 Advances in Network Security and Attack Defense |
| 10:30-11:00 | Break Time | |
| 11:00-12:00 | Closing Ceremony (The Crystal Hall) | |

- Recorded Online Presentation: Keynote 1, Keynote 2, Tutorial 1, Tutorial2, Session 2, Session 4, Session 6, Session 8, Session 10
- Live Online Presentation: Session 1, Session 3, Session 5, Session 7, Session 9
- Recorded poster session presentations are available through youtube.

▶ Registration

▶ INTERNATIONAL PARTICIPANTS PAYMENT METHOD

Registration and Payment

We use Online Registration to complete the registration for participants. Please click <https://kiisc.or.kr/payment/pay/18> to the registration page.

The online registration fee will cover (a) the access to the online conference and (b) the access to the online proceedings.

Once the registration is completed, you will receive an email receipt from PayPal. Please forward that email to kiisc@kiisc.or.kr so that we can issue your registration receipt.

Please contact kiisc@kiisc.or.kr regarding any issues related to registration and payment

Author registration deadline: August 10, 2020 (23:59 UTC-12)

▶ KOREAN PARTICIPANTS 사전등록 : 2020년 8월 18일(화)까지

▷ 학회 홈페이지(www.kiisc.or.kr)접속 → 학회행사 → 사전등록바로가기 → WISA 2020 (KOREAN PARTICIPANTS) 클릭

▷ 사전등록 송금처

- 예금주 : 한국정보보호학회

- 계좌번호 : (국민은행) 754-01-0008-146

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

* 온라인 프로시딩, 프로그램북 제공

* 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.

▶ REGISTRATION FEE

| | General Registration | Student Registration |
|---------------------------------------|-------------------------|-------------------------|
| Registration (On/Before Aug.18, 2020) | USD\$ 580 (700,000 won) | USD\$ 420 (500,000 won) |

▶ REGISTRAR 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

No refunds after Aug. 18, 2020. Substitutes are permitted. \$100 (\110,000) cancellation fee for cancellations received before Aug 18, 2020

▶ Attendance Guideline

Online Attendance: We will send live youtube links to mobile phones and e-mails written at registration the day before the event

Offline Attendance: Use KI-PASS (Korea Internet-Pass) below

Offline

Access to the Accessibility System (KI-PASS)



<https://nid.naver.com/login/privacyQR>

Perform pre-certification → Enter after site QR scan

CONTENTS

The 2020 WISA Poster Session

Chair Hwankuk Kim (Sangmyung University, Korea)

(1) Cryptography & Authentication

- Poster: Acceleration of Pairing Product Operation Using Precomputation 21
Seong-Yun Jeon and Mun-Kyu Lee
- Poster: Ternary Encoding Algorithm for Integer Comparison using Multiple Inner Products **Best Poster Premium** 22
Turabek Gaybullaev and Mun-Kyu Lee
- Poster: Compactly Committing Authenticated Encryption Based on Lesamnta-LW 23
Shoichi Hirose
- Poster: Random Word Error-based Improved Differential Fault Attack on LEA 24
Seong-Hyuck Lim, Jong-Hyeok Lee and Dong-Guk Han
- Poster: TVLA Statistics Test for SEED Hardware Implementation 25
Jaegun Moon, Tae-Ho Lee, Yoo-Jin Baek and Dong-Guk Han
- Poster: Novel Single-Trace ML profiling Attack on NIST Round 2 Candidate Masked qTESLA Digital Signature Algorithm 26
Il-Ju Kim, Bo-yeon Sim, Taeho Lee, Jaeseung Han and Dong-Guk Han
- Poster: Efficient Method of CPA on Bitslice Block Ciphers 27
Jaeseung Han, Yeon-Jae Kim, Soo-jin Kim, Bo-Yeon Sim and Dong-Guk Han
- Poster: Novel Differential Fault Attack Utilizing Multiple Fault Injection 28
Han-Byeol Park, Han-Seop Lim, Jong-Hyeok Lee and Dong-Guk Han
- Poster: Faster ECC Scalar Multiplication on FPGA 29
Asep Muhamad Awaludin, Jonguk Park and Howon Kim
- Poster: Novel Single-Trace Attack on Countermeasures against Instruction-related Timing Attack
- NIST 2-Round LAC and HQC - 30
Bo-Yeon Sim and Dong-Guk Han
- Poster: Proposal for User Authentication Method using FIDO based Password Management 31
Hyunjin Kim, Seongmin Yoo, Jaecheol Ryou and Seokjin Choi

(2) Advanced Cyber Threat Response

- Poster: Ensuring Safety of Medical Cyber Physical Systems Through Misbehavior Detection of Integrated Medical Embedded IoT Devices - A Case Study of Patient-Controlled Analgesia Device **Best Poster Gold** 32
Philip Virgil Astillo, Gaurav Choudhary, Jiyeon Kim, Hoonyong Park, Ilsun You and Ing-Ray Chen
- Poster: Research on cyber threat intelligence sharing model utilizing cloud computing in a smart city 33
Hoonyong Park, Jaejun Heo, Bonam Kim and Ilsun You
- Poster: Analysis of SMB Protocol Vulnerability - Will there be a second WannaCry crisis? - 34
Woosung Yun, Yeseong Hwang, Jieon Kim, Jaeyeon Lee, Sukdea Yu and Sangjin Lee
- Poster: Dynamic Mobile App Unpacking Based on Bytecode Instrumentation 35
Geochang Jeon, Sunjun Lee and Jeong Hyun Yi
- Poster: Method of Generating a Blacklist for Mobile Devices by Searching Malicious Websites 36
Takashi Ishihara, Masaya Sato and Toshihiro Yamauchi
- Poster: Parallel De-concealment of SUCI using GPU for 5G Multi-Access **Best Poster Silver** 37
Chan-Guk Jang, Juhong Han and Okyeon Yi
- Poster: Study on Method to Evaluate Impact of Security Configuration Scanning Tool on PLC 38
Hansaem Wi, Jinhyeok Oh, Juhong Han, Chan-Guk Jang, Yeop Chang, Okyeon Yi
- Poster: Comparative Analysis of Security Vulnerability Response Policy and the Role of the Government 39
Ji-Hun Lim, Sang-Pil Yoon and Hun-Yeong Kwon
- Poster: Identification of device motion status via Bluetooth discovery 40
Shing Ki Wong and Siu Ming Yiu
- Poster: HAL based resource manipulation monitoring on AOSP 41
Thien Phuc Doan and Souhwan Jung
- Poster: StreamingHyp Streaming Data in Lightweight Hypervisor Environment 42
Hoang Nguyen Huy and Souhwan Jung
- Poster: The Impact of Almost Identical Techniques On Android Security 43
Ngoc-Tu Chau and Souhwan Jung

(3) Applying AI Security

- Poster: Black-box Attacks by Retraining Substitute Model using Adversarial Training 44
Gwonsang Ryu, Hosung Park and Daeseon Choi
- Poster: Comparison of Federated learning and Original learning using Numeric data 45
Jinhyeok Jang and Daeseon Choi
- Poster: Building Novel CNN-Based Intrusion Detection System 46
Wooyeon Jo, Hyunjin Kim and Taeshik Shon
- Poster: Deep Mobile Malware Detection and Classification Based on Supervised CNN 47
Younghun Ban, Eunbyeol Ko, Jinsung Kim and Jeong Hyun Yi
- Poster: Design of Machine Learning based Side Channel Attack Models for Effective Non-Profiling Analysis
Best Poster Premium 48
Han-Seop Lim, Bo-Yeon Sim, Jaeseung Han, Ju-Hwan Kim and Dong-Guk Han
- Poster: ML Profiling Attack with traces collected from other boards and cards 49
Taeho Lee, Seong-Hyuck Lim, Jaeseung Han and Dong-Guk Han
- Poster: Anomaly Detection using Interpretable Probabilistic K Nearest Neighbor Classification 50
Hyeonjun Ju and Jiwon Yoon
- Poster: AdMat: From Malware Detection To Image Classification 51
Long Nguyen-Vu and Souhwan Jung

(4) Blockchain & Data Security

- Poster: Risk Assessment of "Ostrich ZIP" 52
Michihiro Nakayama and Akira Kanaoka
- Poster: Proposal of a Data Sharing Framework for Implementing a Fully Decentralized Data Sharing Society 53
Siwan Noh and Kyung-Hyune Rhee
- Poster: Linkability Concerns of Smart Contracts within Federated Learning Schemes **Best Poster Silver** 54
Sandi Rahmadika and Kyung-Hyune Rhee
- Poster: Implementation of Data Sharing Model for the Connected Car based on Hyperledger Fabric 55
Byeong-Gyu Jeong, Kangwoo Cho and Sang Uk Shin

- Poster: On Blockchain Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks 56
Muhammad Firdaus and Kyung-Hyune Rhee
- Poster: A Design of a Blockchain-based Auction Service for Understanding Performance Characteristics 57
Minsun Shim, Hyesong Kim, Hayoung You, Jiyoung Lee and Hyung-Jong Kim
- Poster: Blockchain Service Model Framework for Fake News Prevention 58
Lee Won Park and Hangbae Chang
- Poster: S-DEB : Self-Destructible Electronic Bracelets for personal information protection in Quarantine Monitoring System **Best Poster Gold** 59
Sung-Kyu Ahn, Hyelim Jung, Sung-Kyung Kim and Ki-Woong Park

CONTENTS

* indicates that the associate session is based on live online presentation and its presenters should give the presentation at the venue (for example: Session 1*)

Aug. 25 (Tuesday)

16:30~18:30 – Welcome Reception (Jade Room)

Aug. 26 (Wednesday)

13:30~14:30 – Opening Ceremony (The Crystal Hall)

14:30~15:00 – Break Time

15:00~16:30 – Session 1*: AI Security and Intrusion Detection 1 (The Crystal Hall1)

Session Chair: Taeshik Shon (Ajou University, Korea)

- Spatially Localized Perturbation GAN (SLP-GAN) for Generating Invisible Adversarial Patches
Best Paper Primium 69
Yongsu Kim, Hyoeun Kang, Afifatul Mukaroh, Naufal Suryanto, Harashta Tatimma Larasati and Howon Kim
- Detecting Block Cipher Encryption for Defense against Crypto Ransomware on Low-end Internet of Things 71
Hyunji Kim, Jaehoon Park, Hyeokdong Kwon, Kyoungbae Jang, Seungju Choi and Hwajeong Seo
- CAPTCHAs Are Still in Danger: An Efficient Scheme to Bypass Adversarial CAPTCHAs 73
Dongbin Na, Namgyu Park, Sangwoo Ji and Jong Kim

15:00~16:30 – Session 2: Steganography and Malware (The Crystal Hall2)

Session Chair: Hwajeong Seo (Hansung University, Korea)

- 3-Party Adversarial Steganography 75
Ishak Meraouche, Sabyasachi Dutta and Kouichi Sakurai
- Accessibility Service Utilization Rates in Android Applications Shared on Twitter 77
Shuichi Ichioka, Estelle Pouget, Takao Mimura, Jun Nakajima and Toshihiro Yamauchi
- Novel Reversible Acoustic Steganography Based on Carrier Orthogonality 79
Hung-Jr Shiu, Fang-Yie Leu, Chun-Ming Lai, and Yu-Chun Huang

16:30~17:00 – Break Time

17:00~18:30 – Session 3*: Application, System, and Hardware Security 1 (The Crystal Hall1)

Session Chair: Mun-Kyu Lee (Inha University, Korea)

- Compact Implementation of CHAM Block Cipher on Low-End Microcontrollers **Best Paper Silver** 81
Hyeokdong Kwon, Hyunji Kim, Seung Ju Choi, Kyoungbae Jang, Jaehoon Park, Hyunjun Kim and Hwajeong Seo
- The Gravy Value: A Set of Features for Pinpointing BOT Detection Method 83
Semi Park and Kyungho Lee
- Impact of Optimized Operations $A \cdot B$, $A \cdot C$ for Binary Field Inversion on Quantum Computers 85
Kyoungbae Jang, Seung Ju Choi, Hyeokdong Kwon, Zhi Hu and Hwajeong Seo

17:00~18:30 – Session 4: Cryptography 1 (The Crystal Hall2)

Session Chair: Kyung Chul Jeong (The Affiliated Institute of ETRI, Korea)

- Identity-based Unidirectional Proxy Re-Encryption in Standard Model: A Lattice-based Construction **Best Paper Gold** 87
Priyanka Dutta, Willy Susilo, Dung Hoang Duong, Joonsang Baek and Partha Sarathi Roy
- Efficient algorithm for computing odd-degree isogenies on Montgomery curves **Best Paper Gold** 89
Kenta Koderu, Chen-Mou Cheng and Atsuko Miyaji
- An Efficient Implementation of AES on 8-bit AVR-based Sensor Nodes 91
Youngbeom Kim and Seog Chung Seo

Aug. 27 (Thursday)**09:00~10:30 – Session 5*: Application, System, and Hardware Security 2 (The Crystal Hall 1)**

Session Chair: Bonam Kim (Soonchunhyang University, Korea)

- Virtualization Technologies in the Android Framework and Compatibility with SEAndroid 93
Jaehyeon Yoon, Tu Chau Ngoc, Hoang Nguyen Huy and Souhwan Jung
- Toward a Fine-Grained Evaluation of the Pwnable CTF: Extracting Common Assessment Points 95
Sungkyung Kim, Euntae Jang and Ki-Woong Park
- A Statistical Approach Towards Fraud Detection in the Horse Racing **Best Paper Silver** 97
Moohong Min, Jemin Lee, Hyunbeom Park, Hyojoung Shin and Kyungho Lee

09:00~10:30 – Session 6: Cryptography 2 (The Crystal Hall2)

Session Chair: Kyung Chul Jeong (The Affiliated Institute of ETRI, Korea)

- Revisiting the Minrank Problem on Multivariate Cryptography 99
Yacheng Wang, Yasuhiko Ikematsu, Shuhei Nakamura and Tsuyoshi Takagi
- Paid And Anonymous Usage Of Cloud Software 101
Kun Peng
- Optimization of PBKDF2-HMAC-SHA256 and PBKDF2-HMAC-LSH256 in CPU Environments 103
Hojin Choi and Seog Chung Seo
- Cryptanalysis of Two Fully Anonymous Attribute-Based Group Signature Schemes with Verifier-Local Revocation from Lattices 105
Yanhua Zhang, Ximeng Liu, Yupu Hu, Qikun Zhang, Huiwen Jia

10:30~11:00 – Break Time

11:00~12:00 – Keynote 1 (The Crystal Hall)

Session Chair: Dong Hoon Lee (Korea University, Korea)

- Title: An Extended View of Resilience
Prof. Matt Bishop (University of California, Davis, USA)

12:00~13:30 – Lunch Break

13:30~14:30 – Keynote 2 (The Crystal Hall)

Session Chair: Sooel Son (KAIST, Korea)

- Title: Training Verifiably Robust Malware Classifiers
Prof. Suman Jana (Columbia University, USA)

14:30~15:00 – Break Time

15:00~16:30 – Session 7*: Cyber Security (The Crystal Hall 1)

Session Chair: Jemin Lee (Korea University, Korea)

- Filtering-based Correlation Power Analysis (CPA) with signal envelopes against shuffling methods
Best Paper Primium 107
Youngbae Jeon and Ji Won Yoon
- The Proposal of Risk Informed Cyber Security Assessment Methodology in Nuclear Power Plant 109
Jeck-Chae Euom and Sangjoon Lee

- Security Problems of 5G Voice Communication 111
Seongmin Park, Hyungjin Cho, Youngkwon Park, Bomin Park, Dowon Kim and Kangbin Yim

15:00~16:30 – Session 8: Application, System, and Hardware Security 3 (The Crystal Hall 2)

Session Chair: Bonam Kim (Soonchunhyang University, Korea)

- On the Cost-Effectiveness of TrustZone Defense on ARM Platform 113
Naiwei Liu, Meng Yu, Wanyu Zang and Ravi Sandhu
- Detection on GPS spoofing in location based mobile games 115
Shing Ki Wong and Siu Ming Yiu
- Push For More: On Comparison of Data Augmentation and SMOTE With Optimised Deep Learning Architecture For Side-Channel 117
Yoo-Seung Won, Dirmanto Jap and Shivam Bhasin

16:30~17:00 – Break Time

17:00~18:30 – Tutorial 1 (The Crystal Hall1)

Session Chair: So Jeong Kim (The Affiliated Institute of ETRI, Korea)

- Title: Graphical Models and Analysis for Cybersecurity
Prof. Dongseong Kim (The University of Queensland, Australia)

17:00~18:30 – Tutorial 2 (The Crystal Hall2)

Session Chair: Mun-Kyu Lee (Inha University, Korea)

- Title: Authenticated Key Exchange from Weak Secrets
Dr. SeongHan Shin (National Institute of Advanced Industrial Science and Technology, Japan)

Aug. 28 (Friday)

09:00~10:30 – Session 9*: AI Security and Intrusion Detection 2 (The Crystal Hall1)

Session Chair: Bo-Yeon Sim (Kookmin University, Korea)

- Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less labeling Effort 119
Kyung Ho Park, Eunji Park and Huy Kang Kim
- Entropy-based Feature Grouping in Machine Learning for Android Malware Classification 121
Hyunseok Shim and Souhwan Jung
- DLDDO: Deep Learning to Detect Dummy Operations 123
Jonghyeok Lee and Dong-Guk Han

09:00~10:30 – Session 10: Advances in Network Security and Attack Defense (The Crystal Hall2)

Session Chair: Jemin Lee (Korea University, Korea)

- Analysis on Malicious Residential Hosts Activities Exploited by Residential IP Proxy Services 125
Akihiro Hanzawa and Hiroaki Kikuchi
- Insights into Attacks' Progression: Prediction of Spatio-Temporal Behavior of DDoS Attacks 127
Ahmed Abusnaina, Mohammed Abuhamad, Daehun Nyang, Songqing Chen, An Wang and David Mohaisen
- Methods to Select Features for Android Malware Detection Based on the Protection Level Analysis 129
Chaeun Lee, Eunnae Ko and Kyungho Lee

10:30~11:00 – Break Time

11:00~12:00 – Closing Ceremony (The Crystal Hall)