WCC 2015 The 23rd IFIP World Computer Congress Daejeon, Korea

ifip

KOREAN INSTITUTE OF INFORMATION SCIENTISTS AND ENGINEERS

SCH 순천향대학교 SOON CHUN HYANG UNIVERSITY

R&BD CENTER FOR SECURITY AND SAFETY INDUSTRIES

AsiaARES 2015

The 2015 Asian Conference on Availability, Reliability and Security

In conjunction with ICT-EurAsia 2015

October 4th – 7th, 2015, Daejeon Convention Center, Daejeon, Korea

http://www.AsiaAres.org

Program

## Tuesday October 6th, 2015 (Room K (Room 205, 2F) 14.00 – 15.30 pm

Network Security (Session 1)

Session Chair: Ilsun You (Soon Chun Hyang University, Republic of Korea)

Key Agreement with Modified Batch Rekeying for Distributed Group in Cognitive Radio Networks
Renugadevi N, Mala C

Can We Securely Use CBC Mode in TLS1.0?
Takashi Kurokawa, Ryo Nojima, Shiho Moriai

Investigation of DDoS Attacks by Hybrid Simulation
Yana Bekeneva, Konstantin Borisenko, Andrey Shorov, Igor Kotenko

## Tuesday October 6th, 2015 (Room K (Room 205, 2F) 16.00 – 17.30 pm

Multimedia Security (Session 2)

Session Chair: Kangbin Yim (Soon Chun Hyang University, Republic of Korea)

A lossless data hiding strategy based on two-dimensional side-match predictions
Chi-Yao Weng, Sheng-Jie Wang, Shiuh-Jeng WANG

Face Recognition Performance Comparison between Real Faces and Pose Variant Face Images from Image Display Device
Mi-Young Cho and Young-Sook Jeong

Secure image deduplication in cloud storage
Han Gang, Hongyang Yan, Lingling Xu

## Wednesday October 7th, 2015 (Room K (Room 205, 2F) 11.00 – 12.30 pm

Dependable Systems and Applications I (Session 3)

Session Chair: Hsing-Chung Chen (Asia University, Taiwan)

Identification of Corrupted Cloud Storage in Batch Auditing for Multi-Cloud Environments
Sooyeon Shin, Taekyoung Kwon, Seungyeon Kim

An approach for evaluating softgoals using weight
Shuichiro Yamamoto

Secure database using order-preserving encryption scheme based on arithmetic coding and noise function
Mikhail Yakovlev, Sergey Krendelev, Maria Usoltseva

## Wednesday October 7th, 2015 (Room K (Room 205, 2F) 14.00 – 15.30 pm

Cryptography (Session 4)

Session Chair: Akihiro Yamamura (Akita University, Japan)

Hybrid Encryption Scheme using Terminal Fingerprint and its Application to Attribute-based Encryption without Key Misuse
Chunlu Chen, Hiroaki Anada, Junpei Kawamoto, Kouichi Sakurai

A Secure Multicast Key Agreement Scheme
Hsing-Chung Chen, Chung-Wei Chen

Secure mobility management for MIPv6 with identity-based cryptography
Nan Guo, Fangting Peng, Tianhan Gao

## Wednesday October 7th, 2015 (Room K (Room 205, 2F) 16.00 – 17.30 pm

Dependable Systems and Applications II (Session 5)

Session Chair: Ilsun You (Soon Chun Hyang University, Republic of Korea)

An Efficient Unsavory Data Detection Method for Internet Big Data
Peige Ren, Xiaofeng Wang, Hao Sun, Fen Xu, Baokang Zhao, Chunqing Wu

Differential Fault Attack on LEA
Dirmanto Jap, Jakub Breier

Efficient Almost Strongly Universal Hash Function for Quantum Key Distribution
Bo Liu, Baokang Zhao, Chunqing Wu, Wanrong Yu, Ilsun You