

# JWIS2007

## The 2<sup>nd</sup> Joint Workshop on Information Security

August 6-7, 2007

Waseda University, Tokyo, Japan

### Program (Day 1: August 6, 2007)

#### PROGRAM SCHEDULE

Day 1 : August 6, 2007 (Monday)

Time	HALL A	HALL B
9:00-9:10	<b>Welcome Remarks</b>	
	General Co-Chairs (Hall A) Min Surp Rhee, Dankook University, Korea (Hall B) Koji Nakao, KDDI Inc. / NICT, Japan	
9:10-10:30	<b>Session 1 Biometrics, Watermarking</b> (Chair: SeongHan Shin, AIST, Japan)	<b>Session 2 Network Security I</b> (Chair: Miyoun Yoon, KISA, Korea)
	<b>“A New Joint Compression and Encryption Scheme of JPEG2000 Based on Arithmetic Coding”</b>  Yang Ou, Pukyong National University, Korea Deepak Kafle, Pukyong National University, Korea Kyung Hyune Rhee, Pukyong National University, Korea	<b>“Message Forwarding Strategies for Inter-AS Packet Traceback Network”</b>  Hiroaki Hazeyama, NAIST, Japan Yoshihide Matsumoto, NAIST, Japan Youki Kadobayashi, NAIST, Japan
	<b>“A Proposal on Biometric Template Database by using Mutual Correlation of Enrolled Templates”</b>  Yoshifumi Ueshige, Nagasaki University, Japan Kouichi Sakurai, Kyushu University, Japan Sei-ichiro Kamata, Waseda University, Japan	<b>“Flow Direction Inferring Using BGP Information Encapsulated in sFlow Packets”</b>  Gregory Blanc, Ecole Supérieure d'Informatique Électronique Automatique, France Hiroaki Hazeyama, NAIST, Japan Youki Kadobayashi, NAIST, Japan
	<b>“The Implementation of Fingerprint Strip Image Reconstruction Algorithm for Linear Sensor”</b>  Woong-Sik Kim, Konyang University, Korea	<b>“The proposal of anomaly traffic detection and response mechanism in real-time network”</b>  Seung-Hee Oh, ETRI, Korea Kiyong Kim, ETRI, Korea
	<b>“The Implementation of Fingerprint Payment Verification System &amp; User Security Method”</b>  Woong-Sik Kim, Konyang University, Korea	<b>“A Secure User Authentication Protocol based on FMIPv6 over IEEE 802.16e Networks”</b>  Mi-Joo Kim, Soonchunhyang University, Korea Rack-Hyun Kim, Soonchunhyang University, Korea Heung-Youl Youm, Soonchunhyang University, Korea Jae-Cheol Ryou, Chungnam National University, Korea
10:30-11:00	<b>Coffee Break</b>	
11:00-11:40	<b>Invited Talk I (Hall A)</b> (Chair: Ji Hong Kim, Semyung University, Korea)	
	<b>“Recent Activities of Information Security Research in Taiwan: TWISC and iCAST”</b>  Tzong-Chen Wu, National Taiwan University of Science & Technology / President of Chinese Cryptology and Information Security Association, Taiwan	

<b>11:40 - 13:00</b>	<b>Lunch</b>	
<b>13:00 - 14:00</b>	<b>Session 3 Cryptographic Protocol</b> (Chair: Chung-Huang Yang, National Kaohsiung Normal University, Taiwan)	<b>Session 4 Network Security II</b> (Chair: Woong-Sik Kim, Konyang University, Korea)
	“Privacy-Preserving Identification Protocols with Multiple Acquaintances for Consumer Goods with RFID Tags”  Yoonjeong Kim, Seoul Women's University, Korea	“Network Behavior Modeling for Anomaly Detection”  Myeong Seok Cha, KrCERT, Korea Won Tae Sim, KrCERT, Korea
	“A Secret Voting Method for Network Meetings by Using a One-way Homomorphic Function”  Tetsuji Kobayashi, Nippon Institute of Technology, Japan	“M-NDP Mechanism Using PKC and AC”  Jong Hyun Lee, Inha University, Korea Jae Hoon Nah, ETRI, Korea Ji Hong Kim, Semyung University, Korea
	“A Robust Buyer-Seller Watermarking Protocol”  M. Mahboob Yasin, COMSATS Institute of Information Technology, Pakistan Huma M. Yasin, COMSATS Institute of Information Technology, Pakistan Amna AbdulWahid, COMSATS Institute of Information Technology, Pakistan	“STATISTICALLY BASED INTRUSION ALERT POINT DETECTION”  Michael W. David, Cubic Corporation, Belgium Deepak Kumar Dalai, Indian Statistical Institute, India J. Mitra, Indian Statistical Institute, India Kouichi Sakurai, Kyushu University, Japan
<b>14:00 - 14:30</b>	<b>Coffee Break</b>	
<b>14:30 - 15:50</b>	<b>Session 5 Authentication</b> (Chair: Shih-Jeng Wang, Central Police Univ., Taiwan)	<b>Session 6 Malware and Anti Spam Calling</b> (Chair: S Myeong Seok Cha, KrCERT, Korea)
	“Enhancing Privacy and Authentication for Location Based Service using Trusted Authority”  Kyusuk Han, Information and Communications University, Korea Kwangjo Kim, Information and Communications University, Korea	“A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities”  Koji Nakao, NICT, Japan Katsunari Yoshioka, NICT, Japan Daisuke Inoue, NICT, Japan Masashi Eto, National Institute of Information and Communications Technology, Japan
	“A User Authentication Scheme with Privacy Protection for Wireless Sensor Networks”  Sungjune Yoon, Information and Communications University, Korea Hyunrok Lee, Information and Communications University, Korea Sungbae Ji, Information and Communications University, Korea Kwangjo Kim, Information and Communications University, Korea	“Classification of Port-scans via Distributed Observation”  Hiroaki Kikuchi, Tokai University, Japan Naoya Fukuno, Tokai University, Japan Tomohiro Kobori, Tokai University, Japan Masato Terada, Hitachi, Ltd., Japan
	“Robust Authentication Mechanism Allowing Dynamic Position of Sensors for Wireless Sensor Network using Multicast Security Technique”  Miyoun Yoon, KISA, Korea Yoojae Won, KISA, Korea Yongtae Shin, Soongsil University, Korea	“Message Authentication for Protecting Spam Calls in SIP-based VoIP Services”  Jaeduck Choi, Soongsil University, Korea Yujung Jang, Soongsil University, Korea Souhwan Jung, Soongsil University, Korea Yoojae Won, KISA, Korea Youngduk Cho, KISA, Korea
“Securing Wireless Sensor Networks with Stream Cipher Based Authenticated Encryption”  Shu-Yun Lim, Dongseo University, Korea Chuan-Chin Pu, Dongseo University, Korea Hyo Taek Lim, Dongseo University, Korea Hoon Jae Lee, Dongseo University, Korea	“A Development of Secure VoIP Application Service based on XCAP”  Taijin Lee, KISA, Korea Yonggeun Won, KISA, Korea Daehee Seo, KISA, Korea Yoojae Won, KISA, Korea	
<b>15:50 - 16:20</b>	<b>Coffee Break</b>	
<b>16:20 - 17:40</b>	<b>Invited Talk II, III (Hall A)</b> (Chair: Hiroaki Kikuchi, Tokai University, Japan)	
	“Intrusion Forecasting Framework for Early Warning System against Cyber Attack”  Sehun Kim, Korea Advanced Institute of Science and Technology, Korea	
<b>18:00 - 20:00</b>	“Trend of Biometrics Technology in Japan”  Naohisa Komatsu, Waseda University, Japan	
	<b>Banquet</b>	

# JWIS2007

## Program (Day 2: August 7, 2007)

### PROGRAM SCHEDULE

Day 2 : August 7, 2007(Tuesday)

Time	HALL A	HALL B
9:00 - 10:00	<b>Session 7 (Hall A)</b> <b>Anti Phishing</b> (Chair: Yoshiaki Hori, Kyushu University, Japan)	
	<b>“Proposal for an Automated Phishing Protection System”</b> Masanori Hara, KDDI R&D Laboratories Inc., Japan Ayumu Kubota, KDDI R&D Laboratories Inc., Japan Yutaka Miyake, KDDI R&D Laboratories Inc., Japan	
	<b>“A Proposal of the AdaBoost-Based Detection of Phishing Sites”</b> Daisuke Miyamoto, NAIST, Japan Hiroaki Hazeyama, NAIST, Japan Youki Kadobayashi, NAIST, Japan	
	<b>“SpoofSifter: Scheme to Prevent Phishing by Detecting User's Posting to Spoofed Website”</b> Yuna Kim, Pohang University of Science and Technology, Korea Hun Seok Choi, Pohang University of Science and Technology, Korea Jong Kim, Pohang University of Science and Technology, Korea	
10:00 - 10:30	<b>Coffee Break</b>	
10:30 - 11:50	<b>Invited Talk IV, V (Hall A)</b> (Chair: Yutaka Miyake, KDDI R&D Laboratories, Inc., Japan)	
	<b>“Countermeasures for combating cyber attacks in Korea”</b> Heung Youl Youm, Soonchunhyang University, Korea	
	<b>“Recent view in the Internet threat environment and its counter measure”</b> Tadashi Yamanouchi, Symantec Japan Research Institute, Inc., Japan	
11:50 - 13:00	<b>Lunch</b>	
13:00 - 14:20	<b>Session 8</b> <b>Key Management</b> (Chair: Kyung Hyune Rhee, Pukyong National University, Korea)	<b>Session 9</b> <b>Incidents and Management</b> (Chair: Jaehoon Nah, ETRI, Korea)
	<b>“The Usage of Off-line Digital Certificates in the Mobile Phones”</b> Soon-Tae Park, KISA, Korea Seak-Lae Lee, KISA, Korea Jae-Il Lee, KISA, Korea	<b>“Message-based Open Framework for Security Incidents Prevention and Response”</b> Pilyong Kang, KISA, Korea Kyounghee Ko, KISA, Korea Yunegie Sung, KISA, Korea Wontae Sim, KISA, Korea
	<b>“Adding Authentication to Key Agreement using ESPAR”</b> SeongHan Shin, AIST, Japan Kazukuni Kobara, AIST, Japan Hideki Imai, AIST/ Chuo University, Japan	<b>“Estimating Economic Damages Caused by Information Security Incidents”</b> Sangho Gee, KISA, Korea Jinho Yoo, KISA, Korea Hyein Song, KISA, Korea
	<b>“Lightweight Group Key Management for Clustered Sensors in Self Organizing Sensor Network”</b> Shu-Yun Lim, Dongseo University, Korea Meng-Hui Lim, Dongseo University, Korea Sang Gon Lee, Dongseo University, Korea Hoon Jae Lee, Dongseo University, Korea	<b>“Improved Information Security Management with Network Security Map”</b> Kyounghee Ko, KISA, Korea Yunegie Sung, KISA, Korea Jun Yoon, KISA, Korea Pilyong Kang, KISA, Korea Wontae Sim, KISA, Korea

	<p><b>“A Lightweight Cryptographic Capability Negotiation Mechanism based on MIKEY for VoIP”</b></p> <p>Seokung Yoon, KISA, Korea Joongman Kim, KISA, Korea Daehee Seo, KISA, Korea Yoojae Won, KISA, Korea</p>	<p><b>“Trust and Forgiveness for Retrust”</b></p> <p>Mozghan Tavakolifard, AmirKabir University of Technology, Iran Mohammad-Kazem Akbari, AmirKabir University of Technology, Iran Shahriar Pourazin, AmirKabir University of Technology, Iran</p>
<b>14:20-14:50</b>	<b>Coffee Break</b>	
<b>14:50-16:10</b>	<p><b>Session 10</b> <b>Public Key and Implementation</b> (Chair: Shiho Moriai, Sony Corporation, Japan)</p>	<p><b>Session 11</b> <b>Secure OS / Web / Test Tool</b> (Chair: Pilyong Kang, KISA, Korea)</p>
	<p><b>“Reliable Public Key Distribution Method for dynamic peer to peer Network”</b></p> <p>Hyeokchan Kwon, ETRI, Korea Sangchoon Kim, Gangwon National University, Korea Jaehoon Nah, ETRI, Korea Jongsoo Jang, ETRI, Korea</p>	<p><b>“Asynchronouns notification channel for exploitation-robust secure OS on virtual machine monitor”</b></p> <p>Ruo Ando, NICT, Japan Youki Kadobayashi, NICT, Japan Youichi Shinoda, NICT, Japan</p>
	<p><b>“Yet Another Sanitizable Signature from Bilinear Maps”</b></p> <p>Tetsuya Izu, FUJITSU LABORATORIES Ltd., Japan Noboru Kunihiro, The University of Electro-Communications, Japan Kazuo Ohta, The University of Electro-Communications, Japan Makoto Sano, The University of Electro-Communications, Japan Masahiko Takenaka, FUJITSU LABORATORIES Ltd., Japan</p>	<p><b>“Profile-based Web Application Security System with Positive Model Selection”</b></p> <p>Tae Hyung Kim, Pohang University of Science and Technology, Korea Kyungtae Kim, Pohang University of Science and Technology, Korea Jong Kim, Pohang University of Science and Technology, Korea Sung Je Hong, Pohang University of Science and Technology, Korea</p>
	<p><b>“A Multiplication Algorithm in <math>F_p^m</math> for Arbitrary Pairs of Characteristic <math>p</math> and Degree <math>m</math> Such That <math>p &gt; m</math>”</b></p> <p>Tomoki Yoshida, Okayama University, Japan Hidehiro Kato, Okayama University, Japan Yasuyuki Nogami, Okayama University, Japan Yoshitaka Morikawa, Okayama University, Japan</p>	<p><b>“Design and Development of an NIDS Evasion Test Tool with GUI”</b></p> <p>Chung-Huang Yang, National Kaohsiung Normal University, Taiwan Chih-Hung Lin, Institute for Information Industry, Taiwan Li-Chou Juan, Institute for Information Industry, Taiwan Jain-Shing Wu, Institute for Information Industry, Taiwan Tai-Yun Huang, National Kaohsiung Normal University, Taiwan</p>
	<p><b>“ASIC Performance Comparison for the ISO Standard Block Ciphers”</b></p> <p>Takeshi Sugawara, Tohoku University, Japan Naofumi Homma, Tohoku University, Japan Takafumi Aoki, Tohoku University, Japan Akashi Satoh, AIST, Japan</p>	
<b>16:10-16:20</b>	<b>Final wrap up</b>	

### Hosted by

Information and Communication System Security (ICSS) of the Institute of Electronics,  
Information and Communication Engineers (IEICE), Japan  
Korea Institute of Information Security and Cryptology (KIISC), Korea

### Sponsored by

National Institute of Information and Communications Technology (NICT), Japan  
National Institute of Advanced Industrial Science and Technology (AIST), Japan  
Korea Information Security Agency (KISA), Korea  
Electronics & Telecommunications Research Institute (ETRI), Korea  
Institute for Information Technology Advancement (ITTA), Korea

### Home Page

<http://www.ieice.org/~icss/jwis2007/index.html>