## Monday, June 4  Pre-Conference Workshops

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 - 10:30</td>
<td>BCC</td>
<td>CPSS</td>
<td>RESEC</td>
<td>SCC</td>
<td></td>
</tr>
<tr>
<td>10:30 - 11:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 - 12:30</td>
<td>BCC</td>
<td>CPSS</td>
<td>RESEC</td>
<td>SCC</td>
<td></td>
</tr>
<tr>
<td>12:30 - 14:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>14:00 - 15:30</td>
<td>BCC</td>
<td>CPSS</td>
<td>RESEC</td>
<td>SCC</td>
<td></td>
</tr>
<tr>
<td>15:30 - 16:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16:00 - 17:30</td>
<td>BCC</td>
<td>CPSS</td>
<td>RESEC</td>
<td>SCC</td>
<td></td>
</tr>
</tbody>
</table>

## Tuesday, June 5  AsiaCCS Main Conference

<table>
<thead>
<tr>
<th>Time</th>
<th>Diamond Hall (2F)</th>
<th>Ruby Hall (2F) Research Track 1</th>
<th>Emerald Hall (2F) Research Track 2</th>
<th>Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 - 09:30</td>
<td>Welcome Message (General Chair/Program Committee Chair)</td>
<td>Keynote Cliff Wang (US Army Research) “Cyber Deception: an emergent research area”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:30 - 10:30</td>
<td>Coffee Break</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30 - 11:00</td>
<td>Embedded System Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 - 12:20</td>
<td>Applied Crypto 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:20 - 13:50</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:50 - 15:20</td>
<td>Authentication Mobile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Personal Identification Chord: A Four Button Authentication System for Smartwatches
Ian Oakley (UNIST); Jun Ho Huh (Samsung Electronics); Junsung Cho, Geumhwan Cho (Sungkyunkwan University); Rasel Islam (UNIST); and Hyoongshick Kim (Sungkyunkwan University)

2MA: Verifying Voice Commands via Two Microphone Authentication
Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor (University of Florida)

Beat-PIN: A User Authentication Mechanism for Wearable Devices Through Secret Beats
Ben Hutchins, Anudeep Reddy, Wenqiang Jin, Michael Zhou, Ming Li, and Lei Yang (University of Nevada, Reno)

Oracle: Automated Evaluation of Access Control Policies in iOS
Luke Deshoteils (North Carolina State University); Razvan Deaconescu, Costin Carabas, Iulia Mandu (University POLITEHNICA of Bucharest); William Enck (North Carolina State University); Mihai Chiroiu (University POLITEHNICA of Bucharest); Ninghui Li (Purdue University); and Ahmad-Reza Sadeghi (Technische Universität Darmstadt)

Source Attribution of Cryptographic API Misuse in Android Applications
Ildar Muslukhov (The University of British Columbia); Yazan Boshmaf (Qatar Computing Research Institute); and Konstantin Beznosov (The University of British Columbia)

Don't throw me away: Threats Caused by the Abandoned Internet Resources Used by Android Apps
Elkana G Pariwono (Waseda University); Daiki Chiba, Mitsuaki Akiyama (NTT Secure Platform Laboratories); and Tatsuya Mori (Waseda University)

Machine Learning 1
Protecting Intellectual Property of Deep Neural Networks with Watermarking
Jialong Zhang, Zhongshu Gu, Jiyong Jang, Hui Wu, Marc P Stockeclin, Heqing Huang, and Ian M Molloy (IBM Research)

Towards Fast and Semi-supervised Identification of Smart Meters launching Data Falsification Attacks
Shameek Bhattacharjee, Aditya Thakur, and Sajal K. Das (Missouri University of Science and Technology)

Detecting Malicious PowerShell Commands using Deep Neural Networks
Danny Hendler (Ben-Gurion University of the Negev); Shay Kels (Microsoft); and Amir Rubin (Ben-Gurion University of the Negev)

Detection under Privileged Information
Z. Berkay Celik, Patrick McDaniel (penn state); Raul Izmailov (Vencore Labs); Nicolas Papernot, Ryan Sheatsley, Raquel Alvarez (penn state); and Ananthram Swami (Army Research Laboratory)

Entwining Sanitization and Personalization Tutorial Talk 1: Continue on Databases
Sébastien Gambs (UQAM); Julien Loline (Universite Rennes 1); and Jean-Marc Robert (ETS)

Large-Scale Privacy-Preserving Statistical Computations for Distributed Genome-Wide Association Studies
Oleksandr Tkachenko, Christian Weinert, Thomas Schneider, and Kay Hamacher (TU Darmstadt)

Secure Similar Sequence Query on Outsourced Genomic Data
Ke Cheng, Yantian Hou (Boise State University); and Liangmin Wang (Jiangsu University)

A Linear Distinguisher and its Application for Analyzing Privacy-Preserving Transformation Used in Verifiable (Outsourced) Computation
Liang Zhao (Sichuan University) and Liqun Chen (University of Surrey)

Privacy 1

Poster Session
Welcome Reception

Wednesday, June 6
AsiaCCS Main Conference

Time    Diamond Hall (2F)    Ruby Hall (2F) Research Track 1    Emerald Hall (2F) Research Track 2    Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk
09:00 - 10:00   Keynote Jaeyeon Jung
10:00 - 10:30   Coffee Break
10:30 - 12:30   Keynote Jaeyeon Jung

Cellular, Phone, and Email    Trust
FBSleuth: Fake Base Station Forensics via Radio Frequency Fingerprinting
Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu (Zhejiang University); Zhenhua Li (Tsinghua University); and Yunhao Liu (Tsinghua University, Michigan State University)

Augmenting Telephone Spam Blacklists by Mining Large CDR Datasets
Jienan Liu (University of Georgia); Babak Rahbarinia (Auburn University Montgomery); Roberto Perdisci (University of Georgia); Haitao Du, and Li Su (China Mobile Research Institute)

Towards Measuring the Role of Phone Numbers in Twitter-Advertised Spam
Payas Gupta (Pindrop); Roberto Perdisci (University of Georgia); and Mustaque Ahamad (Georgia Institute of Technology)

Use-After-FreeMail: Generalizing the Use-After-Free Problem and Applying it to Email Services
Daniel Gruss, Michael Schwarz (Graz University of Technology); Matthias Wübbeling (Fraunhofer FKIE & University of Bonn); Simon Guggi (Graz University of Technology); Timo Malderle (University of Bonn); Stefan More, and Moritz Lipp (Graz University of Technology)

Temporal Consistency of Integrity-Ensuring Computations and Applications to Embedded Systems Security
Xavier Carpent (University of California, Irvine); Karim Eldefrawy (SRI International); Norrathep Rattanavipanon, and Gene Tsudik (University of California, Irvine)

SALAD: Secure and Lightweight Attestation of Highly Dynamic and Disruptive Networks
Florian Kohnhäuser, Niklas Büscher, and Stefan Katzenbeisser (TU Darmstadt)

Can You Trust Your Encrypted Cloud? An Assessment of SpiderOakONE’s Security
Anders P. K. Dalskov and Claudio Orlandi (Aarhus University)

On the strategy and behavior of Bitcoin mining with N-attackers
Hanqing Liu, Na Ruan, Rongtian Du, and Weijia Jia (Shanghai Jiao Tong University)

Invited Talk 2: T-Fuzz: fuzzing by program transformation, Mathias Payer (Purdue)

Sponsor Talk 1: IFAA Powers the Creating of the Online Trusted Identities, Feng, Chunpei (Ant Financial)
Thursday, June 7
AsiaCCS Main Conference

<table>
<thead>
<tr>
<th>Time</th>
<th>Diamond Hall (2F)</th>
<th>Ruby Hall (2F)</th>
<th>Emerald Hall (2F)</th>
<th>Sapphire Hall (3F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 - 09:30</td>
<td>Keynote Kevin Fu (University of Michigan)</td>
<td>Tutorial, Invited, Sponsor Talk</td>
<td></td>
<td>Invited Talk 5: The Hazards of Coarse Control: Understanding and Protecting Smart Device Control Surfaces, XiaoFeng Wang (Indiana Univ)</td>
</tr>
<tr>
<td>09:30 - 09:50</td>
<td>Privacy 2</td>
<td>Research Track 1</td>
<td></td>
<td>09:50 – 10:50</td>
</tr>
<tr>
<td>09:50 - 11:10</td>
<td>Zhihao Shan (State University of New York at Buffalo); Zhan Qin (The University of Texas at San Antonio); Leslie Ying, and Kui Ren (State University of New York at Buffalo)</td>
<td>Single Trace Attack against RSA Key Generation in Intel SGX SSL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly-Efficient Fully-Anonymous Dynamic Group Signatures</td>
<td>Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zhihao Shan (State University of New York at Buffalo); Zhan Qin (The University of Texas at San Antonio); Leslie Ying, and Kui Ren (State University of New York at Buffalo)</td>
<td>Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vireshwar Kumaran, He Li, Noah Luther, Pranav Asokan, Jung-Min (Jerrry) Park (Virginia Tech); Martin B. H. Weiss, and Taieb Znati (University of Pittsburgh)</td>
<td>Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You Are Your Photographs: Detecting Multiple Identities of Vendors in the Darknet Marketplaces
Xiangwen Wang, Peng Peng, Chun Wang, and Gang Wang (Virginia Tech)

Intriguing Web Defacement Campaigns at Large
Federico Maggi, Marco Balduzzi (Trend Micro Italy s.r.l.); Ryan Flores (Forward-looking Threat Research Team); Lion Gu, and Vincenzo Ciancaglini (Trend Micro, Inc.)

Detect Malware: Myth or Fact?
Boyou Zhou, Anmol Gupta, Rasoul Jahanshahi, Manuel Egele, and Ajay Joshi (Boston University)

le-git-imate: Towards Verifiable Web-based Git Repositories
Hammad Afzali (New Jersey Institute of Technology); Santiago Torres-Arias (New York University); Reza Curtmola (New Jersey Institute of Technology); and Justin Cappos (New York University)

Chaudhry Mujeeb Ahmed (Singapore University of Technology and Design); and Martin Ochoa (Singapore University of Technology and Design & Department of Applied Mathematics and Computer Science, Universidad del Rosari); Jianying Zhou, Aditya P. Mathur, Rizwan Qadeer (Singapore University of Technology and Design); Carlos Murguia (Melbourne University); and Justin Ruths (UT Dallas)

Electromagnetic Induction Attacks Against Embedded Systems
Jayaprakash Selvaraj (Iowa State University); Gokcen Yilmaz Dayanikli (Virginia Tech); Neelam Prabhu Gaukhar (Iowa State University); David Ware (Utah State University); Ryan M Gerdes (Virginia Tech); and Mani Mina (Iowa State University)

Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack
Shohei Nashimoto, Daisuke Suzuki (Mitsubishi Electric); Takeshi Sugawara, and Kazuo Sakiyama (University of Electro-Communications)

TABOR: A Graphical Framework for Anomaly Detection in Industrial Control Systems
Qin Lin (Delft University of Technology); Sridha Adepulu (Singapore University of Technology and Design); Sicco Verwer (Delft University of Technology); and Aditya Mathur (Singapore University of Technology and Design)

Invited Talk 4: Analog cyber security— from 0101 to mixed signals. Wenyuan Xu (Zhejiang Univ) 15:50 – 16:50

Poster Session
Banquet
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 - 10:50</td>
<td>Cybercrime After the Sunrise: A Statistical Analysis of DNS Abuse in New gTLDs Maciej Korczynski (Grenoble Alps University); Maarten Wullink (SIDN Labs); Samaneh Tajalizadehkhooob (Delft University of Technology); Giovane C. M. Moura (SIDN Labs); Arman Noroozian (Delft University of Technology); Drew Bagley (Secure Domain Foundation / CrowdStrike); and Cristian Hesselman (SIDN Labs)</td>
<td>Who is knocking on Telnet Port: A Large-Scale Empirical Study of Network Scanning Hwanjo Heo (KAIST/ETRI) and Seungwon Shin (KAIST)</td>
<td>Achieving Flexibility for ABE with Outsourcing via Proxy Re-Encryption Zuxiu Yu (The Hong Kong Polytechnic University); Man Ho Au (The Hong Kong Polytechnic University); Rupeng Yang (Shandong University &amp; The Hong Kong University, Guangzhou &amp; State Key Laboratory of Cryptology); and Jiuliang Xu (Shandong University)</td>
<td>Pseudometric Isometries: A New Framework for Fuzzy Extractor Reusability Quentin Alamelou, Paul-Edmond Berthier, Chloe Cachet, Stephane Cauchois (equens/Worldline); Benjamin Fuller (University of Connecticut); Philippe Gaborit (Université de Limoges); and Sailesh Simhadri (University of Connecticut)</td>
</tr>
<tr>
<td>10:50 - 11:20</td>
<td>Towards Sustainable Evolution for the TLS Public-Key Infrastructure Taeho Lee, Christos Pappas (ETH Zurich); Pawel Szalachowski (SUTD); and Adrian Perrig (ETH Zurich)</td>
<td>Efficient Two-level Homomorphic Encryption in Prime-order Bilinear Groups and A Fast Implementation in WebAssembly Nuttapong Attrapadunan, Goichiro Hanaduka (AISt); Shigeo Mitsunari (Cybozu Labs, Inc.); Yusuke Sakai (AISt); Kana Shimizu (Waseda University); and Tadanori Teruya (AISt)</td>
<td>Coffee Break</td>
<td></td>
</tr>
<tr>
<td>11:20 - 12:50</td>
<td>No One In The Middle: Enabling Network Access Control Via Transparent Attribution Jeremy Erickson, Qi Alfred Chen, Xiaochen Yu, Erinjen Lin, Robert Levy, and Z. Morley Mao (University of Michigan)</td>
<td>Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications Mohammad Sadegh Riazi (University of California San Diego); Christian Weinert, Oleksandr Tkachenko (TU Darmstadt); Ebrahim Mohammadgholi Songhori (University of California San Diego); Thomas Schneider (TU Darmstadt); and Farinaz Koushanfar (University of California San Diego)</td>
<td>ProHarvester: Fully Automated Analysis of Proofs Side-Channel Leaks on Android Raphael Spreitzer, Felix Kirchengast, Daniel Gruss, and Stefan Mangard (Graz University of Technology)</td>
<td>Droid M+: Developer Support for Imbibing Android's New Permission Model Ioannis Gasparis, Azeem Asqil, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Rajiv Gupta (University of California, Riverside); and Edward Colbert (U.S. Army Research Lab)</td>
</tr>
<tr>
<td></td>
<td>A Data-driven Attack against Support Vector Machine Shigang Liu, Jun Zhang (Swinburne University of Technology); Yu Wang (Guangzhou University); Wanlei Zhou (Deakin University); Yang Xiang (Swinburne University of Technology); and Olivier Defelice (Defence Science &amp; Technology Group)</td>
<td>Efficient Repair of Polluted Machine Learning Systems via Causal Unlearning Yinzhi Cao (Lehigh University); Alexander Fangxiaoyu, Andrew Aday (Columbia University); Eric Stahl, Jon Merwine (Lehigh University); and Junfeng Yang (Columbia University)</td>
<td>Dazed Droids: A Longitudinal Study of Android Inter-App Vulnerabilities Ryan Johnson (Kryptowire / George Mason University); Mohamed Elsabagh (Kryptowire); Angelos Stavrou (Kryptowire / George Mason University); and Jeff Offutt (George Mason University)</td>
<td></td>
</tr>
</tbody>
</table>