# WIFS'14 IEEE Workshop on Information Forensics and Security

*December 3-5, 2014*
*Atlanta, Georgia, USA*

Verona Systems, LLC

# Program at a glance

| | | | Wed, Dec 3, 2014 | Thu, Dec 4, 2014 | Fri, Dec 5, 2014 |
|---|---|---|---|---|---|
| 8:00 AM | - | 9:00 AM | GlobalSIP Plenary #1 | GlobalSIP Plenary #2 | GlobalSIP Plenary #3 |
| 9:00 AM | - | 9:20 AM | Coffee Break | Coffee Break | Coffee Break |
| 9:20 AM | - | 10:00 AM | WIFS Keynote #1<br>Min Wu | WIFS Keynote #2<br>Wade Trappe | Lecture Session #6<br>Forensic Analysis 2 |
| 10:00 AM | - | 10:10 AM | | | |
| 10:10 AM | - | 10:20 AM | | | |
| 10:20 AM | - | 10:30 AM | Lecture Session #1<br>Biometrics | Lecture Session #4<br>Special Session: Security and Internet of Things | |
| 10:30 AM | - | 10:40 AM | | | |
| 10:40 AM | - | 10:50 AM | | | |
| 10:50 AM | - | 11:30 AM | | | Lecture Session #7<br>Statistical Methods in Security |
| 11:30 AM | - | 11:40 AM | | | |
| 11:40 AM | - | 11:50 AM | Tutorial / Lunch<br>Differential Privacy<br>Kamalika Chaudhuri & Anand Sarwate | | |
| 11:50 AM | - | 12:00 PM | | Lunch | |
| 12:00 PM | - | 12:10 PM | | | |
| 12:10 PM | - | 12:20 PM | | | |
| 12:20 PM | - | 1:20 PM | | | Tutorial / Lunch<br>Securing IoT<br>Depeng Li |
| 1:20 PM | - | 2:30 PM | | Lecture Session #5<br>Forensic Analysis 1 | |
| 2:30 PM | - | 2:40 PM | Lecture Session #2<br>Watermarking and Steganography | | |
| 2:40 PM | - | 2:50 PM | | | |
| 2:50 PM | - | 3:00 PM | | Poster Session | |
| 3:00 PM | - | 3:10 PM | | | Lecture Session #8<br>Anomaly Detection |
| 3:10 PM | - | 3:20 PM | | | |
| 3:20 PM | - | 3:30 PM | | WIFS Social Event and Banquet<br>3:30pm - 5:45pm<br>Visiting CNN Studio<br>6:00pm - 9:00pm<br>Banquet<br>71th floor<br>Westin Peach tree Plaza<br>(Details on page 15) | |
| 3:30 PM | - | 3:40 PM | | | |
| 3:40 PM | - | 3:50 PM | | | |
| 3:50 PM | - | 4:00 PM | | | |
| 4:00 PM | - | 4:10 PM | Coffee Break | | |
| 4:10 PM | - | 4:20 PM | | | |
| 4:20 PM | - | 4:30 PM | Lecture Session #3:<br>Privacy-Preserving Computation and Communication | | |
| 4:30 PM | - | 4:40 PM | | | Coffee Break |
| 4:40 PM | - | 4:50 PM | | | |
| 4:50 PM | - | 5:50 PM | | | |
| Evening | | | 6:00pm – 7:30pm<br>GlobalSIP Reception, 1st floor | | |

*** Dec 2nd, 6:00pm–7:30pm, GlobalSIP welcome reception**

*** IFS-TC meeting, Dec 4, 12:00-1:20pm. (Location: Small meeting room in the lunch area, looking for IFS-TC sign)**

# Organizing Committee

*General Chairs*

Yan (Lindsay) Sun, University of Rhode Island
Vicky H. Zhao, University of Alberta

*Special Topic Area Chairs*

Nasir Memon, NYU Polytechnic School of Engineering
Rongshan Yu, Institute for Infocomm Research

*Tutorial Chair*

Yen-Kuang Chen, Intel Corporation

*Technical Chairs*

Shantanu Rane, Mitsubishi Electric Research Labs
Negar Kiyavash, University of Illinois

*Finance Chair*

Ashwin Swaminathan, Qualcomm Inc.

*Publicity Chairs*

Tomas Filler, Digimarc Corporation
Avinash Varna, Intel Corporation

*WIFS'14 General Program Committee*

Patrick Bas, LAGIS Ecole Centrale de Lille
Dinei Florencio, Microsoft Research
Anthony T.S. Ho, University of Surrey
Jiwu Huang, Shenzhen University
Ching-Yung Lin, IBM T. J. Watson Res. Center
Anderson Rocha, University of Campinas
Husrev T. Sencar, TOBB University
Yun Q. Shi, New Jersey Institute of Tech.
Yan (Lindsay) Sun, University of Rhode Island
Adnan Alattar, Digimarc Corporation
Samson Cheung, University of Kentucky
Pedro Comesana-Alfaro, University of Vigo
Athanassios N. Skodras, University of Patras
Ashwin Swaminathan, Qualcomm Inc.
Chiou-Ting (Candy) Hsu, National Tsing Hua University
Herve Chabanne, Morpho
Oscar Au, Hong Kong University

Tomas Filler, Digimarc Corporation
Jiangtao Li, Intel Corporation
Sarath Pankanti, IBM Thomas J. Watson Research Center
Arun Ross, Michigan State University
T. Charles Clancy, Virginia Tech
Jana Dittmann, Otto-von-Guericke Universität Magdeburg
Tanya Ignatenko, Eindhoven University of Technology
Hitoshi Kiya, Tokyo Metropolitan University
Matthias Kirchner, University of Munster
Negar Kiyavash, University of Illinois at Urbana-Champaign
Y.-W. Peter Hong, National Tsing Hua University
Marco Tagliasacchi, Politecnico di Milano
Patrizio Campisi, Università Degli Studi Roma Tre
Mauro Barni, University of Siena
Andrew Teoh, Yonsei University
Gweanel Doerr, Technicolor R&D
Zekeriya Erkin, Delft University of Technology
Jessica Fridrich, SUNY, Binghamton
Teddy Furon, INRIA - Rennes - Bretagne Atlantique
Karthik Nandakumar, IBM
Stefan Katzenbeisser, TU Darmstadt
Farinaz Koushanfar, Rice University
Fernando Perez-Gonzalez, University of Vigo
Ahmed Reza-Sadeghi, TU Darmstadt
Svyatoslav Voloshynoskiy, University of Geneva
Ye Wang, Mitsubishi Electric Research Laboratories

*Special Topic Program Committee*

Ahmed M. Abdelgawad, Central Michigan University
Magdy Bayoumi, University of Louisiana at Lafayette
Zhenzhong Chen, Wuhan University
Ray Cheung, City University of Hong Kong
Shao-Yi Chien, National Taiwan University
Shashikant Patil, NMIMS University
Miodrag Potkonjak, UCLA
Sergio Saponara, University of Pisa
Zheng-Hua Tan, Aalborg University
Andy Wu, National Taiwan University
Jianqing Zhang, Intel Labs
Fa-Long Luo, Element CXI, Inc and Anyka, Inc.

## Keynote Speaker

Professor Min Wu
University of Maryland, College Park

**Traces in the Environment: Exploring Power Network Signatures for Information Forensics**

***Abstract:*** Osama bin Laden's video propaganda prompted numerous information forensic questions: given a video under question, when and where was it shot? Was the sound track captured together at the same time/location as the visual, or superimposed later? Similar questions about the time, location, and integrity of multimedia and other sensor recordings are important to provide evidence and trust in crime solving, journalism, infrastructure monitoring, smart grid management, and other informational operations.

An emerging line of research toward addressing these questions exploits novel signatures induced by the power network. An example is the small random-like fluctuations of the electricity frequency known as the Electric Network Frequency (ENF), owing to the dynamic control process to match the electricity supplies with the demands in the grid. These environmental signatures reflect the attributes and conditions of the power grid and become naturally "embedded" into various types of sensing signals. They carry time and location information and may facilitate integrity verification of the primary sensing data.

This talk will provide an overview of recent information forensics research on ENF carried out by our Media and Security Team (MAST) at University of Maryland, and discuss some on-going and open research issues in and beyond security applications.

***Biography:*** Dr. Min Wu is an ADVANCE Professor of Electrical and Computer Engineering and a Distinguished Scholar-Teacher at the University of Maryland, College Park. She received her Ph.D. degree in electrical engineering from Princeton University in 2001. At UMD, she leads the Media and Security Team (MAST), with main research interests on information security and forensics and multimedia signal processing. Her research and education have been recognized by a NSF CAREER award, a TR100 Young Innovator Award from the MIT Technology Review Magazine, an ONR Young Investigator Award, a Computer World "40 Under 40" IT Innovator Award, a University of Maryland Invention of the Year Award, an IEEE Mac Van Valkenburg Early Career Early Career Teaching Award, IEEE Distinguished Lecturer, and several paper awards from IEEE SPS, ACM, and EURASIP. She was elected IEEE Fellow for contributions to multimedia security and forensics. Dr. Wu chaired the IEEE Technical Committee on Information Forensics and Security (2012-2013), and has served as Vice President - Finance of the IEEE Signal Processing Society (2010-2012), Technical Program Co-Chair of the 2013 IEEE International Conference on Image Processing, and Founding Chief Editor of IEEE SigPort initiative (2013-2014). She has been appointed Editor-in-Chief (2015-2017) for the IEEE Signal Processing Magazine - one of the top impact journals in electrical and computer engineering worldwide.

## Keynote Speaker

Professor Wade Trappe<br>
Rutgers University

### Security for Low-End IoT Devices: When Energy is Not Enough, What is One to Do?

***Abstract:*** There is a push to extend the boundary of the Internet to include a wide array of nontraditional computing devices, ranging from programmable thermostats to wearable systems to devices that monitor and track people/objects. Many of these new networkable devices, which constitute the Internet of Things (IoT), are low-end, low-energy and lightweight computing devices. This talk will present the (controversial) viewpoint that securing the low-end of the IoT cannot be addressed using the cryptographic tools as the operating energy and computational regime for this portion of the IoT will not be conducive for traditional security approaches. The low-end, low-energy, and lightweight computing that will characterize the edge of the Internet of Things, will come with considerable restrictions on how one designs their various functions. For these low-end devices, most of the available energy and computation resources must be devoted to executing core application functionality and, unfortunately, there may be little left over for supporting security and privacy requirements. Thus what is needed is a change of perspective, where at the outset one takes into account the resource sparsity and the limitations that might result in terms of security. In this talk, we examine the challenge of securing devices that are characterized as having significant limitations in functionality (computation and communication), and energy resources. We outline the various security objectives that one might desire in the Internet of Things. Next, we argue that there is no simple solution that will provide enough energy to allow these low-end IoT devices to operate on their own and allow one to support additional functionality beyond the basic (non-security) functions of these devices. Further, we also examine conventional cryptographic methods and make the case that it is unlikely that strong cipher suites will ever be suitably designed and implemented to operate in such an energy-sparse setting. We thus arrive at the main thesis of this talk, which suggests alternative approaches for providing security for low-end IoT devices. We identify a few directions that can be taken out at the device itself, as well as suggesting that one powerful avenue for supporting security involves exploiting an inherent asymmetry in the typical deployment scenarios: low-end devices are typically communicating with higher-end, more resource-rich devices that can perform more computation (and, in particular, signal analysis) to ensure the sanctity of their low-end counterpart's communication. The talk concludes by highlighting future directions in supporting security for light-weight devices.

***Biography:*** Dr. Wade Trappe (S’98-A’02-M’03-SM’13-F’14) received his B.A. in Mathematics from The University of Texas at Austin in 1994 and his Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently a Professor in the Electrical and Computer Engineering Department at Rutgers University, and Associate Director of the Wireless Information Network Laboratory (WINLAB), where he directs WINLAB’s research in wireless security. He has led several federally funded in the area of cybersecurity and communication systems, projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources (the ORBIT testbed, www.orbit-lab.org), and new RFID technologies. Prof. Trappe led a DARPA initiative into validating and prototyping physical layer security mechanisms, an Army Research Office project on the theory of physical layer security, and is currently leading an Army CERDEC project on cognitive radio networks and MIMO communications. He has developed several cross-layer security mechanisms for wireless networks, jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods. He has published over 100 papers, including six best papers awards (two in media security, one in Internet design, one in cognitive radio systems, one in mobile computing, and one in wireless security). His papers have appeared in numerous IEEE/ACM journals and premier conferences, spanning the areas of signal processing and security (e.g., "Subverting MIMO Wireless Systems by Jamming the Channel Estimation Procedure," in Proceedings of the third ACM Conference on Wireless Network Security; "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in Proceedings of the 19th USENIX Security Symposium). His experience in network security and wireless spans over 15 years, and he has co-authored a popular textbook in security, Introduction to Cryptography with Coding Theory, as well as several notable monographs on wireless security, including Securing Wireless Communications at the Physical Layer and Securing Emerging Wireless Systems: Lower-layer Approaches. Professor Trappe has served as an editor for IEEE Transactions on Information Forensics and Security (TIFS), IEEE Signal Processing Magazine (SPM), and IEEE Transactions on Mobile Computing (TMC). He served as the lead guest editor for September 2011 special issue of the Transactions on Information Forensics and Security on "Using the Physical Layer for Securing the Next Generation of Communication Systems" and also served IEEE Signal Processing Society as the SPS representative to the governing board of IEEE TMC.

## Tutorial: Differential Privacy for Signal Processing and Machine Learning

***Abstract:*** Large institutions such as government agencies, medical centers, and private companies are now collecting digital information about citizens, patients, and customers on a massive scale. Much of this data is private or sensitive, so there has been a growing literature on methods for learning about the population without violating the privacy of individuals. In this tutorial, we will describe the differential privacy framework which arose in the cryptographic literature and has now expanded to fields such as data mining, programming languages, machine learning, and signal processing. We will discuss the basics of differential privacy and general mechanisms for creating differentially private algorithms for machine learning and signal processing. We will also describe several applications on real problems, some related privacy directions, and connections to other areas, illustrating some of the breadth as well as challenges in differentially private algorithm design.

### Organizers

Dr. Kamalika Chaudhuri is an Assistant Professor in Computer Science and Engineering at UC San Diego. She received her PhD from the University of California at Berkeley in 2007, and was a postdoctoral researcher at UC San Diego from 2007-2010. Her research is on the theoretical foundations of machine learning, and she is interested in a variety of topics including unsupervised learning, confidence in prediction, and privacy-preserving machine learning. She is the recipient of an NSF CAREER Award in 2013.

Dr. Anand D. Sarwate joined as an Assistant Professor in the Department of Electrical and Computer Engineering at Rutgers, the State University of New Jersey in 2014. He received B.S. degrees in Electrical Engineering and Mathematics from MIT in 2002, an M.S. in Electrical Engineering from UC Berkeley in 2005 and a PhD in Electrical Engineering from UC Berkeley in 2008. From 2008-2011 he was a postdoctoral researcher at the Information Theory and Applications Center at UC San Diego and from 2011-2013 he was a Research Assistant Professor at the Toyota Technological Institute at Chicago, a philanthropically endowed academic computer science institute located on the University of Chicago campus.

## Tutorial: Securing Internet of Things and Case Study

***Abstract:*** The Internet of Things (IoT) is becoming an emerging trend and a growing reality in our age. In IoT, a variety of smart objects (things) interacts and communicates with the environment by exchanging the information. Its pervasive presence offers the ability to measure the contextual indicators and to facilitate information sharing by enabling network connections among physical objects. However, the growing importance of Internet of Things (IoT) and its use to support critical applications have made security and privacy a central issue today. It becomes evident that weaknesses of IoT could open a door for adversaries and some vulnerability, inherent in IoT, could be targeted by the malicious users. The potential vulnerability of IoT may lead to a compromised system if there is no deployment of appropriate, well-designed countermeasures. This tutorial will carefully demonstrate the state-of-the-art security solutions for IoT. It will further introduce some interesting case studies such as smart home, mobile healthcare, wearable computing, smart grid, modern automobile, etc. More importantly, it will comprehensively explore security features which are critical for IoT, a future market with billions of customers in the next a couple of decades.

### Organizers

Dr. Depeng Li joined department of Information and Computer Sciences (ICS) at University of Hawaii at Manoa (UHM) working as an Assistant Professor in fall 2013. He received his BS degree and his Master Degree in computer science from Shandong University, Jinan, China. He obtained his Ph.D. in computer science from Dalhousie University, Halifax, Canada at 2010. After then he was a Post-Doc working for joint cyber security research project sponsored by Massachusetts Institute of Technology and Masdar Institute. He also has industry R&D experience: from 2008-2010, he had been worked in Microsoft Corp. Redmond, USA focusing on security analyses for Windows ecosystem including components such as IPsec, Firewall and IPv6 tunneling technology. He also participated in development and releasing of Windows 7 and Windows server. Prior to joining Microsoft, he had been worked in Research In Motion (RIM) developing blackberry smartphones. Since spring 2014, he had been actively collaborating with Massachusetts Institute of Technology. Dr. Li's research interests are centrally in information security, privacy, and applied cryptography. His research projects span across areas such as secure computation and privacy-preserving systems for Internet of Things, authentication, anonymity, and key management for Physical-Human-Cyber (Phc) security framework. Depeng Li's prior researches focus on enhancing security, privacy and performance in smart grid system and self-organized networks (e.g. wireless networks, sensor networks, MANET). He has served as the guest editor for some famous journals and has been invited to work as the onsite NSF panelist to review NSF grant proposals. He has given a number of research talks in US, Canada and Asia.

# Detailed Programs

## Wednesday, December 3

Wednesday, December 3, 10:20-11:40 Grand Ball Room

**Lecture Session #1: Biometrics**
**Chair: Dr. Pedro Comesaña Alfaro**

Minutiae Set to Bit-String Conversion using Multi-scale Bag-of-Words Paradigm
*Wei Jing Wong and M. L. Dennis Wong (Swinburne University of Technology Sarawak Campus, Malaysia); Yau Hee Kho (Nazarbayev University, Kazakhstan); Andrew Teoh Beng Jin (Yonsei University, Korea)*

Metadata-Based Understanding of Impostor Pair Score Variations
*Amanda Sgroi, Kevin Bowyer and Patrick Flynn (University of Notre Dame,USA)*

Face Recognition via Adaptive Sparse Representations of Random Patches
*Domingo Mery (Pontificia Universidad Catolica de Chile & University of Notre Dame, USA); Kevin Bowyer (University of Notre Dame, USA)*

Bidimensional Empirical Mode Decomposition-based unlighting for Face Recognition
*Miguel A. Ochoa-Villegas (Instituto Tecnologico y de Estudios Superiores de Monterrey, Mexico); Juan Nolazco Flores (Tecnologico de Monterrey, Campus Monterrey, Mexico); Olivia Barron-Cano (Instituto Tecnologico y de Estudios Superiores de Monterrey, Mexico); Ioannis Kakadiaris (University of Houston, USA)*

---

Wednesday, December 3, 10:40-14:30 Grand Ball Room

**Tutorial / Lunch: Differential Privacy for Signal Processing and Machine Learning**

---

Wednesday, December 3, 14:30-16:00 Grand Ball Room

**Lecture Session #2: Watermarking and Steganography**
**Chair: Dr. Jessica Fridrich, University of Binghamton**

Tardos codes for real
*Teddy Furon (Inria, France); Mathieu Desoubeaux (LAMARK, France)*

Security Analysis of Radial-based 3D Watermarking Systems
*Xavier Rolland-Nevière (Technicolor R&D France, France); Gwenaël Doërr (Technicolor R&D, France); Pierre Alliez (INRIA, France)*

Iterative Filtering for Semi-Fragile Self-Recovery
*Pawel Korus and Jarosław Białas (AGH University of Science and Technology,Poland); Andrzej Dziech (AGH University of Science and Technology & University Communication and Computer Engineering, Kielce, Poland)*

Modeling the flicker effect in camcorded videos to improve watermark robustness
*Séverine Baudry, Bertrand Chupeau and Mario de Vito (Technicolor, France); Gwenaël Doërr (Technicolor R&D, France)*

Selection-Channel-Aware Rich Model for Steganalysis of Digital Images
*Tomas Denemark, Vahid Sedighi and Vojtech Holub (Binghamton University, USA); Rémi Cogranne (Troyes University of Technology - ICD - LM2S - UMR STMR CNRS, France); Jessica Fridrich (SUNY, USA)*

Wednesday, December 3, 16:20-17:50 Grand Ball Room

**Lecture Session #3: Privacy-Preserving Computation and Communication**
**Chair: Dr. Mauro Barni, University of Sienna**

State estimation using an Extended Kalman Filter with privacy-protected observed inputs
*Francisco Javier Gonzalez Serrano (Universidad Carlos III de Madrid, Spain); Adrián Amor-Martín (University Carlos III of Madrid, Spain); Jorge Casamayón Antón (Airbus Defence and Space, Spain)*

Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE
*Aysajan Abidin and Aikaterini Mitrokotsa (Chalmers University of Technology, Sweden)*

Puzzling Face Verification Algorithms for Privacy Protection
*Binod Bhattarai, Alexis Mignon and Frédéric Jurie (University of Caen, France); Teddy Furon (Inria, France)*

Understanding the Effects of Real-World Behavior in Statistical Disclosure Attacks
*Simon Oya (University of Vigo, Spain); Carmela Troncoso (Gradiant, Spain); Fernando Pérez-González (University of Vigo, Spain)*

Asymptotic MIMO Artificial-Noise Secrecy Rates with Eigenmode Partitioning
*Andrew D. Harper (Georgia Institute of Technology, USA); Robert John Baxley*
*(Georgia Tech Research Institute, USA)*

# Thursday, December 4

Thursday, December 4, 10:20-11:50 Grand Ball Room

**Lecture Session #4: Special Session: Security and Internet of Things**
**Chair: Dr. Nasir Memon, New York University**

FiberID: Molecular-level Secret for Identification of Things
*Zhen Chen, Yongbo Zeng, Gerald Hefferman, Yan Sun and Tao Wei (University of Rhode Island, USA)*

Malicious Attacks on State Estimation in Multi-Sensor Dynamic Systems
*Jingyang Lu and Ruixin Niu (Virginia Commonwealth University, USA)*

Detecting Misreporting Attacks to the Proportional Fair Scheduler
*Jorge F. Schmidt (University of Klagenfurt, Austria); Roberto López-Valcarce (Universidad de Vigo, Spain)*

Botnet Identification Via Universal Anomaly Detection
*Shachar Siboni and Asaf Cohen (Ben-Gurion University of the Negev, Israel)*

Bootstrap-based Proxy Reencryption for Private Multi-user Computing
*Juan R. Troncoso-Pastoriza and Serena Caputo (University of Vigo, Spain)*

---

Thursday, December 4, 13:20-14:50 Grand Ball Room

**Lecture Session #5: Forensic Analysis 1**
**Chair: Dr. Gwenael Doerr, Technicolor**

Multiple JPEG compression detection by means of Benford-Fourier coefficients
*Cecilia Pasquini (DISI, University of Trento, Italy); Giulia Boato (University of Trento, Italy); Fernando Pérez-González (University of Vigo, Spain)*

Adaptive Matching for Copy-Move Forgery Detection
*Mohsen Zandi and Ahmad Mahmoudi-Aznaveh (Shahid Beheshti University, Iran); Azadeh Mansouri (Kharazmi University, Iran)*

Multi-Clue Image Tampering Localization
*Lorenzo Gaborini and Paolo Bestagini (Politecnico di Milano, Italy); Simone Milani (Politecnico di Milano & University of Padova, Italy); Marco Tagliasacchi and Stefano Tubaro (Politecnico di Milano, Italy)*

Unsupervised Feature Learning For Bootleg Detection Using Deep Learning Architectures
*Michele Buccoli and Paolo Bestagini (Politecnico di Milano, Italy); Massimiliano Zanoni (Politecnico di Milano University, Italy); Augusto Sarti and Stefano Tubaro (Politecnico di Milano, Italy)*

The optimal attack to histogram-based forensic detectors is simple(x)
*Pedro Comesaña and Fernando Pérez-González (University of Vigo, Spain)*

---

Thursday, December 4, 14:50-15:30 Grand Ball Room

**Poster/Demo Session**
**Chair: Dr. H. Vicky Zhao, University of Alberta**

**Posters:**

Optimal Effective Capacity for Secure Information Transmission with Partial Channel Knowledge
*Gangming Lv; Chao Zhang and Hua Tian (Xi'an Jiaotong University, P.R. China)*

Visualization of Cascading Failures in Power Grids
*Yihai Zhu; Jun Yan; Yan Sun and Haibo He (University of Rhode Island, USA)*

A Theoretical Framework for Distributed Secure Outsourced Computing Using Secret Sharing
*Zhaohong Wang, Ting Gu and Sen-ching Samson Cheung (University of Kentucky, USA)*

**Demonstrations:**
Details are available at the conference.

# Friday, December 5

Friday, December 5, 09:20-10:50 Grand Ball Room

**Lecture Session #6: Forensic Analysis 2**
**Chair: Dr. Teddy Furon, INRIA**

Splicing Forgeries Localization through the Use of First Digit Features
*Rudy Becarelli and Irene Amerini (University of Florence, Italy); Roberto Caldelli (University of Florence & Interuniversity Consortium for Telecommunications - CNIT, Italy); Andrea Del Mastio (University of Florence, Italy)*

A feature-based approach for image tampering detection and localization
*Luisa Verdoliva, Davide Cozzolino and Giovanni Poggi (Università Federico II di Napoli, Italy)*

Forensic Characterization of Pirated Movies: Digital Cinema Cam vs. Optical Disc Rip
*Bertrand Chupeau and Séverine Baudry (Technicolor, France); Gwenaël Doërr (Technicolor R&D, France)*

Video forensics based on expression dynamics
*Duc-Tien Dang-Nguyen (DIEE - University of Cagliari, Italy); Valentina Conotter; Giulia Boato and Francesco G.B. De Natale (University of Trento, Italy)*

Theoretical Model of the FLD Ensemble Classifier Based on Hypothesis Testing Theory
*Rémi Cogranne (Troyes University of Technology - ICD - LM2S - UMR STMR CNRS, France); Tomas Denemark (Binghamton University, USA); Jessica Fridrich (SUNY, USA)*

---

Friday, December 5, 10:50-12:20 Grand Ball Room

**Lecture Session #7: Statistical Methods in Security**
**Chair: Dr. Juan Ramon Troncoso-Pastoriza, University of Vigo**

Analysis of the Security of Compressed Sensing with Circulant Matrices
*Tiziano Bianchi and Enrico Magli (Politecnico di Torino, Italy)*

Optimal Detection of OutGuess using an Accurate Model of DCT Coefficients
*Thanh Hai Thai (University of Technology of Troyes, France); Rémi Cogranne (Troyes University of Technology - ICD - LM2S - UMR STMR CNRS, France); Florent Retraint (UTT, France)*

Rich Model for Steganalysis of Color Images
*Miroslav Goljan (SUNY Binghamton, USA); Jessica Fridrich (SUNY, USA); Rémi Cogranne (Troyes University of Technology - ICD - LM2S - UMR STMR CNRS, France)*

Secure Compressed Sensing over Finite Fields
*Valerio Bioglio (Universita di Torino, Italy); Tiziano Bianchi and Enrico Magli (Politecnico di Torino, Italy)*

Source Distinguishability under Corrupted Training
*Benedetta Tondi and Mauro Barni (University of Siena, Italy)*

---

Friday, December 5, 15:00-16:30 Grand Ball Room

**Lecture Session #8: Anomaly Detection**
**Chair: Dr. Yan Lindsay Sun, University of Rhode Island**

Anomaly Traceback using Software Defined Networking
*Jérôme François (INRIA Nancy Grand Est, France); Olivier Festor (INRIA Nancy - Grand Est, France)*

Video Anomaly Detection based on Wake Motion Descriptors and Perspective Grids
*Roberto Leyva, Victor Sanchez and Chang-Tsun Li (University of Warwick, United Kingdom)*

Can Leakage Models Be More Efficient? Non-Linear Models in Side Channel Attacks
*Qizhi Tian (Queen's University Belfast & Center for Secure Information Technologies, United Kingdom); Maire O'Neill (Queen's University, United Kingdom); Neil Hanley (Queen's University Belfast, United Kingdom)*

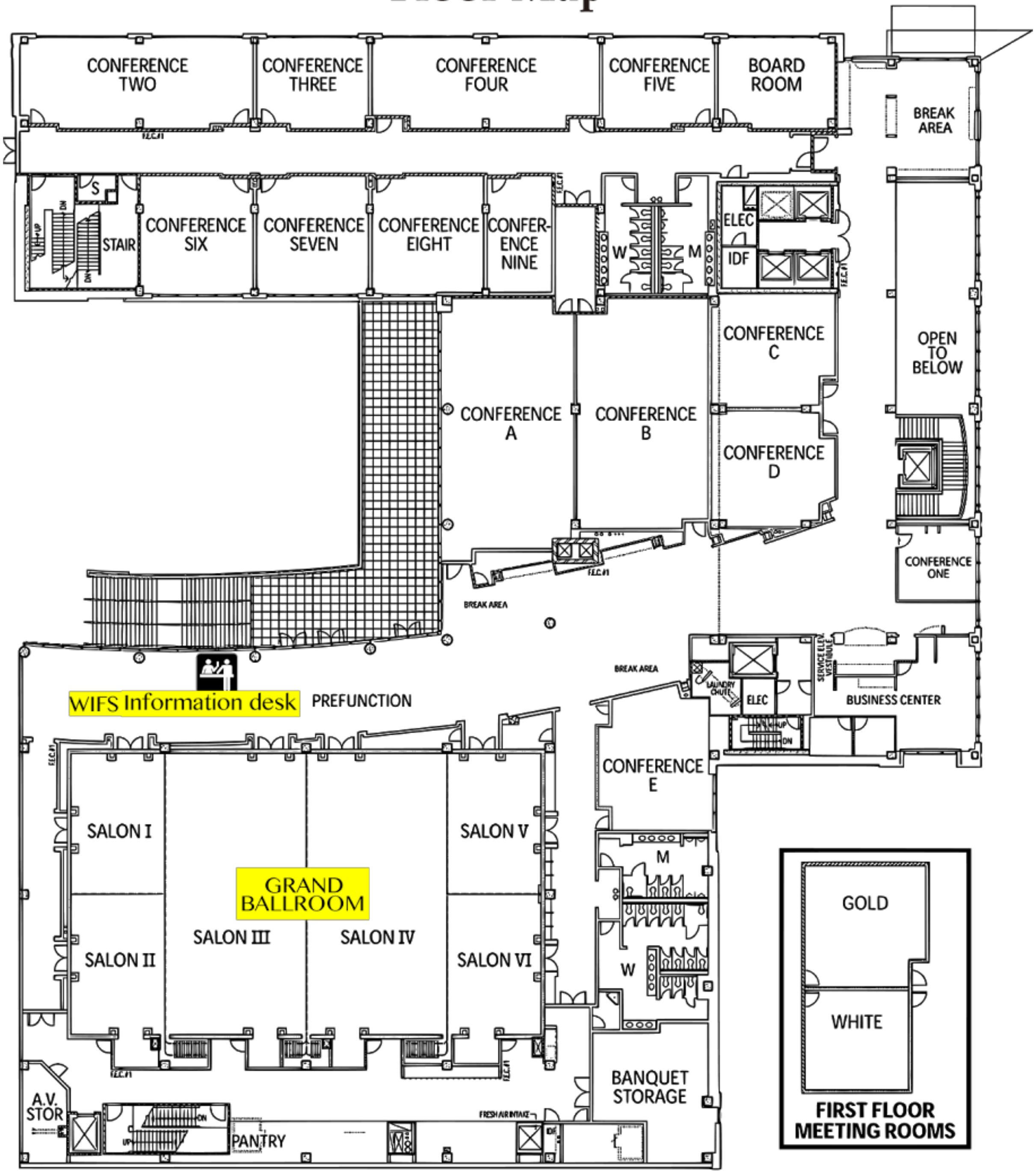
Malware Detection Using HTTP User-Agent Discrepancy Identification
*Martin Grill (Czech Technical University in Prague & Cisco Systems, Czech Republic); Martin Rehak (Czech Technical University in Prague & Cognitive Security, Czech Republic)*

Fair Resource Allocation Under an Unknown Jamming Attack: A Bayesian Game
*Andrey Garnaev and Wade Trappe (WINLAB, Rutgers University, USA)*

# Conference Venue

Georgia Tech Hotel & Conference Center
800 Spring St. NW
Atlanta, GA 30308

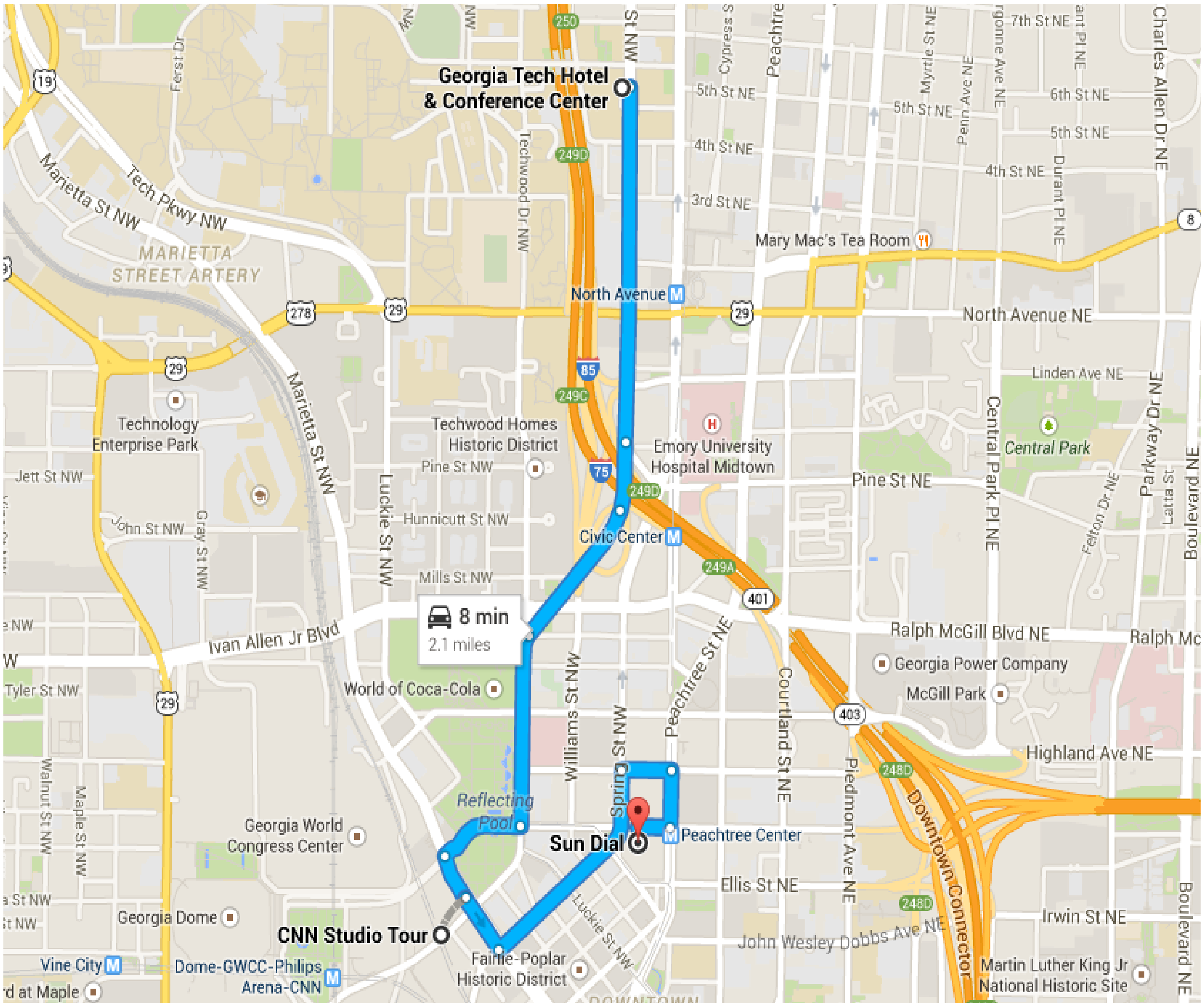
# Floor Map



# Social Program Details & Schedule

## Dec 4, 2014

| | |
|---|---|
| **3:30pm** | Bus departure from Georgia Tech Hotel & Conference Center |
| **4:00pm** | Arrive at CNN Center<br>*190 Marietta St, NW, Atlanta, GA* |
| **4:20pm - 5:30pm** | Visiting the Global Headquarter of CNN (guided tour) |
| **5:40pm** | Bus departure from CNN Center |
| **6:00pm - 9:00pm** | Sun Dial Restaurant Bar & View<br>at the 71th Floor of The Westin Peachtree Plaza<br>*210 Peachtree St, NW, Atlanta, GA.* |


Georgia Tech Hotel & Conference Center
8 min
2.1 miles
Sun Dial
CNN Studio Tour
Marietta St NW
Tech Pkwy NW
MARIETTA STREET ARTERY
North Avenue
North Avenue NE
Mary Mac's Tea Room
Technology Enterprise Park
Techwood Homes Historic District
Emory University Hospital Midtown
Civic Center
Ivan Allen Jr Blvd
World of Coca-Cola
Reflecting Pool
Georgia World Congress Center
Georgia Dome
Dome-GWCC-Philips Arena-CNN
Vine City
Fairlie-Poplar Historic District
Peachtree Center
Ellis St NE
John Wesley Dobbs Ave NE
Downtown Connector
Martin Luther King Jr National Historic Site
Ralph McGill Blvd NE
Georgia Power Company
McGill Park
Highland Ave NE
Irwin St NE
Central Park
Central Park Pl NE
Pine St NE
Linden Ave NE
Courtland St NE
Piedmont Ave NE
Peachtree St NE
Williams St NW
Spring St NW
Luckie St NW
Techwood Dr NW
Pine St NW
Hunnicutt St NW
Mills St NW
Jett St NW
John St NW
Gray St NW
Tyler St NW
Walnut St NW
Maple St NW
5th St NE
4th St NE
3rd St NE
6th St NE
7th St NE
Charles Allen Dr NE
Parkway Dr NE
Boulevard NE
Ferst Dr
85
75
29
278
19
401
403
8
250
249D
249C
249A
248D