IEEE ISI 2015 Conference Program

Securing the World through an Alignment of Technology, Intelligence, Humans and Organizations

May 27-29, 2015, Baltimore, MD

Conference Sponsors and Supporters

Conference Sponsor

IEEE Intelligent Transportation Systems Society

Generous Financial Support Received From

University of Maryland, Baltimore County

College of Engineering and Information Technology, University of Maryland, Baltimore County

The Department of Information Systems, University of Maryland, Baltimore County

Towson University

Program produced by the
IEEE ISI 2015 Organizing Committee

May 2015

Program Features

Welcome Reception (May 27, evening)

Keynote Speakers

Mark E. Segal, National Security Agency (May 27, morning)

Chief of Computer and Information Sciences
Central Security Service's Research Directorate
National Security Agency

Jeremy Epstein, National Science Foundation (May 27, afternoon)

Program Director
Secure and Trustworthy Cyberspace (SaTC), CPS-Security, and CRII programs
National Science Foundation

Jay F. Nunamaker, University of Arizona (May 28, morning)

Regent's and Soldwedel Professor of MIS, Computer Science and Communication
Director of the Center for the Management of Information and the National Center for Border Security and Immigration
University of Arizona

Donna F. Dodson, National Institute of Standards and Technology (May 28, afternoon)

Associate Director and Chief Cyber Security Advisor and Director
National Cybersecurity Center of Excellence, Information Technology Laboratory
National Institute of Standards and Technology

Alan Sherman, University of Maryland, Baltimore County (May 29, morning)

Professor of Computer Science and Electronic Engineering
Director of Cyber Defense Lab
University of Maryland, Baltimore County

Plenary Panel: Privacy and Security Challenges in Modern IoT Systems (May 28, morning)

Moderator: Nilanjan Banerjee, University of Maryland, Baltimore County

Panelists:
– Ryan Robucci, University of Maryland, Baltimore County

– Ram Dantu, University of North Texas
– Tim Grance, National Institute of Standards and Technology
– V.S. Subrahmanian, University of Maryland, College Park
– Tim Finin, University of Maryland, Baltimore County

Invited Speakers

Donald Norris, University of Maryland, Baltimore County (May 28, afternoon)

Professor and Director of the School of Public Policy
Director of the Maryland Institute for Policy Analysis and Research (MIPAR)
University of Maryland, Baltimore County

Adam J. Aviv, United States Naval Academy (May 28, afternoon)

Assistant Professor
Computer Science
United States Naval Academy

Meet the Authors Poster Session and Award Ceremony (May 27)

Parallel Paper Sessions

Track 1: Data Science and Analytics in Security Informatics

Track 2: Security Infrastructure and Tools

Track 3: Human Behavior in Security Applications

Track 4: Organizational, National, and International Issues in Counter-Terrorism and Security Protection

Keynote Speakers

Wednesday, May 27, 9:00 am

Dr. Mark Segal

Chief of Computer and Information Sciences
Central Security Service's Research Directorate
National Security Agency

"A Researcher's Perspective on Cybersecurity Operations Challenges"

Abstract: Almost every week there is a story in the news about how a complex cyber system has been exploited by a cyber actor. Many times the news story will describe how sensitive information was stolen or how the system itself was damaged or disabled. To prevent future cyber exploits from occurring, researchers in academia, industry, and government are constantly looking for new ways to make systems more robust, to detect malicious behavior, and to monitor system health. While scientifically interesting, many kinds of Cybersecurity research projects tend not to be directly applicable to organizations responsible for protecting cyber systems. There are also many operational challenges that are not addressed in current research. This talk will provide an operational perspective on Cybersecurity gaps in current practice and suggest potential research directions to address some of these gaps.

Biography: *Dr. Mark E. Segal* is Chief of Computer and Information Sciences Research in the National Security Agency/Central Security Service's Research Directorate. In this role, Dr. Segal is responsible for leading an organization conducting research in computer science, data science, and natural language processing, and applying the results of this research to NSA/CSS's Signals Intelligence, and Information Assurance missions. Prior to this assignment, Dr. Segal was the Deputy Director of NSA/CSS's Laboratory for Telecommunications Sciences, whose research focus was telecommunications and computer networking. Dr. Segal also served as a Director of Cybersecurity Operations in the NSA/CSS Threat Operations Center, where he led a team in a 24x7 operations center focused on protecting DoD networks from cyber exploits. Dr. Segal is the recipient of a National Intelligence Meritorious Unit Citation and a Presidential Rank Award. Prior to joining NSA, Dr. Segal worked at Telcordia (formerly Bellcore) as a research manager and researcher. He served as Executive Director of Software Technology Research at Telcordia, and conducted research in distributed computing, multimedia systems, dependable systems, and cyber security. Dr. Segal holds BS, MS and PhD degrees in Computer and Communications Sciences from the University of Michigan in Ann Arbor.

Wednesday, May 27, 2:30 pm

Jeremy Epstein

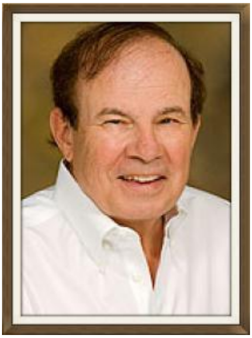
Program Director
Secure and Trustworthy Cyberspace (SaTC),
CPS-Security, and CRII programs
National Science Foundation

"Internet Voting – A Technical, Social, and Policy View"

Abstract: Internet voting is both an inevitable development and a technical impossibility. This talk will explore the policy imperatives, the social drivers, and the technical challenges that must be addressed - and the implications of moving forward before the issues are addressed.

Biography: *Jeremy Epstein* leads the National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program, which is NSF's flagship cybersecurity research program with over 670 active research grants and $75M in annual investments. He's on loan from SRI International, where his research areas include voting system security and software assurance. Jeremy is associate editor in chief of IEEE Security & Privacy magazine, and founder of the Scholarship for Women Studying Information Security.

Thursday, May 28, 9:00 am



Dr. Jay F. Nunamaker

Regent's and Soldwedel Professor of MIS, Computer Science and Communication
Director of the Center for the Management of Information and the National Center for Border Security and Immigration
University of Arizona

"Achieving Rigor and Relevance in Security Research: The Evolution of the AVATAR"

Abstract: This talk is about the development of an automated security kiosk called the AVATAR for interviewing subjects and assessing their credibility regarding security issues. We will also describe an approach and the steps for achieving rigor and relevance by going the Last Research Mile (LRM). This process involves guiding the AVATAR through successful transition into security environments. The AVATAR is equipped with a number of sensors that records an individual's physiological and behavioral reactions when interviewed. Going the Last Research Mile means using scientific knowledge and methods from psychology, linguistics, neuro science, engineering, computer science and information systems to address important problems for real people (border crossers, passengers) with real stakes in the outcome. The AVATAR is being developed by the University of Arizona (BORDERS) through support from the Department of Homeland Security (DHS), Office of University Programs. BORDERS researchers have investigated over 500 cues including vocalics, linguistics, kinesics, cardiorespiratory, eye behavior and facial skin temperatures and many others.

The LRM proceeds in three stages: *Proof-of-concept* research to demonstrate the functional feasibility of the AVATAR, does it work; *proof-of-value* research to investigate whether the AVATAR can create value across a variety of conditions; and *proof-of-use* research to address complex issues of operational feasibility at airports and ports-of-entry. The last research mile ends only when practitioners (border agents, security personnel) routinely use the AVATAR in the field. We argue that going the LRM negates the assumption that one must trade off rigor and relevance, showing it to be a false dilemma. Security researchers who take their solutions through the last research mile may ultimately have the greatest impact on science and society. We demonstrate the LRM with an example of the evolution of the AVATAR as it progresses through each phase of the Last Research Mile. The ultimate test of the AVATAR is whether it can identify subjects that exhibit anomalous behavior.

Biography: *Dr. Jay F. Nunamaker, Jr.* is Regents and Soldwedel Professor of MIS, Computer Science and Communication. He is Director of the Center for the Management of Information and the National Center for Border Security and Immigration at the University of Arizona funded by the Department of Homeland Security (DHS) Center of Excellence program. Dr. Nunamaker was inducted into the Design Science Hall of Fame, May 2008. Dr. Nunamaker received the LEO Award for Lifetime Achievement from the Association of Information Systems (AIS) at ICIS in Barcelona, Spain, December 2002. He was elected a fellow of the AIS in 2000. He was featured in the July 1997 Forbes Magazine issue on technology as one of eight key innovators in information technology. He is widely published with an H index of greater than 60. He has produced over 368 journal articles, book chapters, books and refereed proceedings and has been a major professor for 97 Ph.D. students. His specialization is in the fields of system analysis and design, collaboration technology and deception detection. He has co-founded five spin-off companies based on his research. The commercial product of GroupSystems, ThinkTank based upon Nunamaker's research, is often referred to as the gold standard for structured collaboration systems. He was a research assistant funded by the IS-DOS project in industrial engineering at the University of Michigan and an associate professor of computer science and industrial administration at Purdue University. In his career he has received 100+ million dollars as the PI or Co-PI on sponsored research at the University of Arizona, Purdue University and the University of Michigan. He founded the MIS department at the University of Arizona in 1974 and served as department head for 18 years. From 1976-1991, Nunamaker served as chairman of the ACM Curriculum Committee on Information Systems and as a committee member from 2009-2014. Dr. Nunamaker received his Ph.D. in operations research and systems engineering from Case Institute of Technology, an M.S. and B.S. in engineering from the University of Pittsburgh, and a B.S. from Carnegie Mellon University. He received his professional engineer's license in 1965.

Thursday, May 28, 2:00 pm

Donna F. Dodson

Associate Director and Chief Cyber Security Advisor and Director
National Cybersecurity Center of Excellence,
Information Technology Laboratory
National Institute of Standards and Technology

"Cybersecurity - Facing the Nation's Challenges Together"

Our nation is at risk. The cybersecurity vulnerabilities in our public and private sectors are a risk to national security, public safety, and economic prosperity. Donna Dodson will discuss the challenges facing the nation and describe standards and best practices to understand the risks and address the vulnerabilities in our information technology infrastructure. She will describe national initiatives in cybersecurity education, identity management and cybersecurity implementations.

Biography: Donna F. Dodson is the Chief Cybersecurity Advisor for the National Institute of Standards and Technology and Director of NIST's National Cybersecuity Center of Excellence. Dodson oversees cyber security program to conduct research, development and outreach necessary to provide standards, guidelines, tools, metrics and practices to protect the information and communication infrastructure. This includes collaborations with industry, academia and other government agencies in research areas such as security management and assurance, cryptography and systems security, identity management, security automation, secure system and component configuration, test validation and measurement of security properties of products and systems, security awareness and outreach and emerging security technologies. She received two Department of Commerce Gold Medals and three NIST Bronze Medals. She was a Fed 100 Award winner for her innovations in cybersecurity and in 2011 was included in the top 10 influential people in government information security.

Friday, May 29, 9:00 am

Dr. Alan T. Sherman

Professor of Computer Science and Electronic Engineering
Director of Cyber Defense Lab
University of Maryland, Baltimore County

"End-To-End Voter-Verifiable Elections: Scantegrity and Random-Sample Elections"

Abstract: Voting presents a difficult security engineering challenge because the requirements include both results integrity and unlinkability of votes to voters. Technologies now exist that enable voters to verify the integrity of the election outcome without revealing how they voted. These technologies do not base their results integrity on correct procedures, software, or hardware; instead, they are "implementation independent" in that any error in implementation that changes the election outcome will, with overwhelming confidence, be detected by the voters. I will discuss two of these technologies: Scantegrity and Random Sample Elections (RSE). In November of 2009 and 2011, voters in Takoma Park, Maryland, cast ballots for the mayor and city council members using the Scantegrity II voting system—the first time any End-to-End (E2E) voting system with ballot unlinkability has been used in a binding governmental election. This election demonstrated that E2E cryptographic voting systems can be effectively used and are appreciated by the general public.

RSE reduces the costs of elections by a factor of a thousand by replacing mass elections with a much smaller election by a randomly-chosen anonymous sample of the registered voters. A crucial technical feature of this system is the "verifiable randomness" used to select the sample in a way that cannot be manipulated or predicted by even a national laboratory, yet is verifiable by anyone after the election. One application of RSE is to empower grassroots organizations to conduct their own verifiable elections to demonstrate substantial support for a single referendum question. An interdisciplinary team is refining and implementing the RSE concept and proving properties about it.

Biography: Dr. *Alan T. Sherman* is a professor of computer science at the University of Maryland, Baltimore County and Director of UMBC's Center for Information Security and Assurance. His main research interest is high-integrity voting systems. He has carried out research in election systems, algorithm design, cryptanalysis, theoretical foundations for cryptography, applications of cryptography, cloud forensics, and cybersecurity education. Dr. Sherman is also an editor for Cryptologia and a private consultant performing security analyses. Sherman earned the PhD degree in computer science at MIT in 1987 studying under Ronald L. Rivest.

Plenary Panel
"Privacy and Security Challenges in Modern IoT Systems"

Thursday, May 28, 11:45 am

Moderator:

- **Nilanjan Banerjee**, Ph.D., is an Assistant Professor in Computer Science and Electronic Engineering at University of Maryland at Baltimore County. He currently directs the Mobile, Pervasive, and Sensor Systems lab and is a member of the Cybersecurity Center at UMBC. He is an awardee of NSF Early CAREER Award, NSF-NIH Smart and Connected Health grant and TEDCO grant on wearable computing.

Panelists:

- **Ryan Robucci**, Ph.D., is an Assistant Professor in Computer Science and Electronic Engineering at University of Maryland at Baltimore County. His research in security relates to hardware implementation. Topics of interest include protection against side-channel attacks, Trojan circuits, and the use of physically-unclonable functions. He has been awarded NSF-NIH Smart and Connected Health grant and TEDCO grant on wearable computing.
- **Ram Dantu,** Ph.D., is a Professor in Computer Science and Engineering at University of North Texas, and a visiting professor at MIT. He is the director of Network Security Lab and the Center for Information and Computer Security at UNT. His research interests include wireless networks and network security. He has received a number of NSF research grants.
- **Tim Grance,** is a senior computer scientist in Computer Security Division at the National Institute of Standards and Technology, where he has held a variety of positions including Group Manager for Systems and Network Security and Program Manager for Cyber and Network Security. He has led a broad portfolio of projects including high profile projects such as the NIST Hash Competition, Cloud Computing, Security Content Automation Protocol (SCAP), Protocol Security (DNS, BGP, IPv6), Combinatorial Testing, and the National Vulnerability Database. He is presently a senior researcher supporting projects in cloud computing, mobile devices/applications and big data. He has extensive public and private experience in accounting, law enforcement and computer security and has written on diverse topics including cloud computing, incident handling, intrusion detection, privacy, metrics, contingency planning, forensics, and identity management. He was named in 2003 to the Fed 100 by Federal Computer Week as one of the most influential people in Information Technology for the US Government and is also a two-time recipient of the

Department of Commerce's highest award—a Gold Medal, from the Secretary of Commerce.

- **V.S. Subrahmanian**, Ph.D., is a Professor of Computer Science and Director of the Lab for Computational Cultural Dynamics and Director of the Center for Digital International Government at the University of Maryland. He previously served a 6.5 year stint as Director of the University of Maryland Institute for Advanced Computer Studies. His work stands squarely at the intersection of big data analytics for increased security, policy, and business needs. Prof. Subrahmanian is one of the world leaders in the design, analysis, and application of big data analytics to real world problems so that optimal decisions can be made by governments and companies. In cyber-security, Prof. Subrahmanian developed some of the first secure query processing algorithms, flexible authentication frameworks, unexplained behavior detection and scalable detection of known threats. Prof. Subrahmanian is an elected fellow of AAAI and AAAS.
- **Tim Finin,** Ph.D., is a Professor of Computer Science and Electrical Engineering at the University of Maryland, Baltimore County. He has over 30 years of experience in applications of Artificial Intelligence to problems in information systems and language understanding. His current research is focused on the Semantic Web, mobile computing, analyzing and extracting information from text and online social media, and on enhancing security and privacy in information systems. Prof. Finin has chaired of the UMBC Computer Science Department, served on the Computing Research Association board of directors, been a AAAI councilor, and chaired several major research conferences. He is AAAI Fellow, received an IEEE Technical Achievement award in 2009 and was selected as the UMBC Presidential Research Professor in 2012.

IEEE ISI 2015
CONFERENCE SCHEDULE

*Long papers: 30 minutes (25 minutes for presentation and 5 minutes for Q&A)
Short papers: 25 minutes (20 minutes for presentation and 5 minutes for Q&A)
⊛: Best paper nomination

May 26, 2015 (Tuesday)	
Time & Location	**Event**
6:00pm – 7:30pm *Level 2 Lobby*	Registration Open

May 27, 2015 (Wednesday)	
Time & Location	**Event**
7:00 – 5:30pm *Level 2 Lobby*	Registration
7:30 – 8:45am *Brighton*	Breakfast
8:45 – 9:00am *Whitehall*	Welcome and Conference Opening
9:00 – 10:00am *Whitehall*	**Keynote Speaker: Mark E. Segal,** *National Security Agency* “A Researcher’s Perspective on Cybersecurity Operations Challenges”
10:00 – 11:20am	**Sessions D-I, O-I**
10:00 – 11:20am *Guilford*	**Data Science and Analytics in Security Informatics (D-I)** *Session Chair: Jeffrey Proudfoot*
	⊛ Analysis of Criminal Social Networks with Typed and Directed Edges *Quan Zheng, David Skillicorn and Francesco Calderoni* Dynamic Social Sensor Analytics: Making Sense of Temporal Network Models in Social Media *Chase Dowling, Joshua Harrison, Arun Sathanur, Landon Sego and Courtney Corley*

	A Comparison of Features for Automatic Deception Detection in Synchronous Computer-Mediated Communication *Jinie Pak and Lina Zhou*
10:00 – 11:20am *Whitehall*	**Organizational, National, and International Issues in Counter-terrorism or Security Protection (O-I)** *Session Chair: Xiangyang Li*
	*Nonproliferation Informatics: Employing Bayesian Analysis, Agent Based Modeling, and Information Theory for Dynamic Proliferation Pathway Studies *Royal Elmore and William Charlton* *Multi-objective Evolutionary Algorithms and Multiagent Models for Optimizing Police Dispatch *Ricardo Guedes, Vasco Furtado and Tarcisio Pequeno* The relation between microfinancing and corruption by country: An analysis of an open source dataset *Heather Roy and Sue Kase*
11:20am – 11:45pm	Coffee break
11:45am – 1:00pm	**Sessions H-I, S-I**
11:45am – 1:00pm *Guilford*	**Human Behavior in the Security Applications (I)** *Session Chair: Joshua Harrison*
	Liar, Liar, IM on Fire: Deceptive Language-action Cues in Spontaneous Online Communication *Shuyuan Mary Ho, Jeffrey T. Hancock, Cheryl Booth, Xiuwen Liu, Shashanka Timmarajus and Mike Burmester* Multivariate Embedding based Causality Detection with Short Time Series *Chuan Luo and Daniel Zeng* Adolescent Bystanding Behavior in Cyberbullying: The role of empathy on cyber bullied support *Samuel Owusu and Lina Zhou*
11:45am – 1:00pm *Whitehall*	**Security Infrastructure and Tools (I)** *Session Chair: Murat Kantarcioglu*
	A Statistical Study of Covert Timing Channels Using Network Packet Frequency *Fangyue Chen, Yunke Wang, Heng Song and Xiangyang Li*

	A New Mobile Payment Protocol (GMPCP) By Using A New Key Agreement Protocol (GC) *Mohammad Vahidalizadehdizaj and Lixin Tao* Multi-granular Aggregation of Network Flows for Security Analysis *Tao Ding, Ahmed Aleroud and George Karabatis*
1:00 – 2:30pm	Lunch break (on your own)
2:30 – 3:30pm *Whitehall*	**Keynote Speaker: Jeremy Epstein**, *National Science Foundation* “Internet Voting – A Technical, Social, and Policy View”
3:30 – 4:00pm	Coffee Break
4:00pm – 5:30pm	**Sessions H-II, S-II**
4:00pm – 5:30pm *Guilford*	**Human Behavior in the Security Applications (II)** *Session Chair: Shuyuan Mary Ho*
	*Developing Understanding of Hacker Language through the use of Lexical Semantics *Victor Benjamin and Hsinchun Chen* *Exploring the Effect of Permission Notice on Users’ Initial Trust to An Application Store: The Case of China’s Android Application Market *Jie Gu, An'An Hu, Heng Xu and Lihua Huang* ⊛LECENing places to hide: Geo-Mapping Child Exploitation Material *Bryan Monk, Russell Allsup and Richard Frank*
4:00pm – 5:30pm *Whitehall*	**Security Infrastructure and Tools (II)** *Session Chair: Leonidas Deligiannidis*
	*Honeypot Based Unauthorized Data Access Detection in MapReduce Systems *Huseyin Ulusoy, Murat Kantarcioglu, Bhavani Thuraisingham and Latifur Khan* *A Privacy Protection Procedure for Large Scale Individual Level Data *Julius Adebayo and Lalana Kagal*

	*Base Station Anonymity Distributed Self-Assessment in Wireless Sensor Networks *Jon Ward and Mohamed Younis*
5:30 – 6:00pm	Break and Set up Posters
6:00 – 8:30pm *Hamptons*	Poster Session, Welcome Reception and Awards Ceremony

May 28, 2015 (Thursday)	
Time & Location	**Event**
7:30am – 5:30pm *Level 2 Lobby*	Registration
7:45 – 9:00am *Brighton*	Breakfast
9:00 – 10:00am *Whitehall*	**Keynote Speaker: Jay F. Nunamaker**, *University of Arizona* "Achieving Rigor and Relevance in Security Research"
10:00 – 11:20am	**Sessions D-II, S-III**
10:00 – 11:20am *Guilford*	**Data Science and Analytics in Security Informatics (D-II)** *Session Chair: V.S. Subrahmanian*
	*SPINN: Suspicion Prediction in Nuclear Networks *Ian Andrews, Srijan Kumar, Francesca Spezzano and V.S. Subrahmanian* Inferring Social Influence and Meme Interaction with Hawkes Processes *Chuan Luo, Xiaolong Zheng and Daniel Zeng* Assessment of User Home Location Geoinference Methods *Joshua Harrison, Eric Bell, Chase Dowling, Andrew Cowell and Courtney Corley*
10:00 – 11:20am *Whitehall*	**Security Infrastructure and Tools (S-III)** *Session Chair: Elisa Bertino*
	*Cybersecurity for Product Lifecycle Management - A Research Roadmap *Elisa Bertino and Nathan Hartman* Change Detection in Evolving Computer Networks: Changes in Densification and Diameter Over Time *Josephine Namayanja and Vandana Janeja*

	Random Anonymization of Mobile Sensor Data -Modified Android Framework *Cynthia Claiborne, Ram Dantu and Cathy Ncube*
11:20am – 11:45pm	Coffee break
11:45am – 1:00pm *Whitehall*	**Plenary Panel: Privacy and Security Challenges in Modern IoT Systems** Moderator: *Nilanjan Banerjee*, *University of Maryland, Baltimore County*
	Panelists: *Ryan Robucci, University of Maryland, Baltimore County* *Ram Dantu, University of North Texas* *Tim Grance, NIST* *V.S. Subrahmanian, University of Maryland, College Park* *Tim Finin, University of Maryland, Baltimore County*
1:00 –2:00pm *Brighton*	Lunch
2:00 – 3:00pm *Whitehall*	**Keynote Speaker: Donna Dodson***, National Institute of Standards and Technology* *"*National Cybersecurity Challenges and NIST*"*
3:00 – 3:30pm	Coffee Break
3:30 – 5:00pm	**Sessions H-III, O-II**
3:30 – 5:00pm *Guilford*	**Human Behavior in Security Applications (H-III)** *Session Chair: Adam J. Aviv*
	*Deception is in the Eye of the Communicator: Investigating pupil diameter variations in automated deception detection interviews *Jeffrey Proudfoot, Jeffrey Jenkins, Judee Burgoon and Jay Nunamaker* *Analyzing the Social Media Footprint of Street Gangs *Sanjaya Wijeratne, Derek Doran, Amit Sheth and Jack Dustin* ⊛Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops *Victor Benjamin, Weifeng Li, Thomas Holt and Hsinchun Chen*

3:30 – 5:00pm *Whitehall*	**Organizational, National, and International Issues in Counter-terrorism or Security Protection (O-II)** *Session Chair: Heather Roy*
	⊛Linking Virtual and Real-World Identities *Yaqoub Alsarkal, Yilu Zhou and Nan Zhang* *Emotion Extraction and Entrainment in Social Media: The Case of U.S. Immigration and Border Security *Wingyan Chung, Saike He, Daniel Zeng and Victor Benjamin* ⊛Empirical Assessment of al Qaeda, ISIS, and Taliban Propaganda *David Skillicorn*
5:00 – 6:00pm *Whitehall*	**Invited Talks** Cyber-Security at the Grassroots: American State and Local Governments and the Management of Website Security *Donald Norris, University of Maryland, Baltimore County* Measuring Visual Perceptions of Security *Adam J. Aviv, United States Naval Academy*

May 29, 2015 (Friday)	
Time & Location	**Event**
7:30 – 11:30am *Level 2 Lobby*	Registration
7:45 – 9:00am *Brighton*	Breakfast
9:00 – 10:00am *Whitehall*	**Keynote Speaker: Alan Sherman,** *University of Maryland, Baltimore County* "End-to-end Voter-Verifiable Elections: Scantegrity and Random-Sample Elections"
10:00 – 10:30pm	Coffee Break

10:30am-12:30pm	**Sessions D-III, S-IV**
10:30am – 12:30pm *Guilford*	**Data Science and Analytics in Security Informatics (III)** *Session Chair: Baijian Yan*
	*Spectral Malware Behavior Clustering *Chris Giannella and Eric Bloedorn* *Learning Where to Inspect: Location Learning for Crime Prediction *Mohammad A. Tayebi, Uwe Glässer and Patricia Brantingham* *Exploring Hacker Assets in Underground Forums *Sagar Samtani, Ryan Chinn and Hsinchun Chen* *A Visual Analytics Approach to detecting Server Redirections and Data Exfiltration *Weijie Wang, Baijian Yang and Yingjie Chen*
10:30am – 12:30pm *Whitehall*	**Security Infrastructure and Tools (IV)** *Session Chair: Hongchi Shi*
	*Unintentional Bugs to Vulnerability Mapping in Android Applications *Garima Bajwa, Mohamed Fazeen Mohamed Issadeen, Ram Dantu and Sonal Tanpure* Persistent Threat Pattern Discovery *Faisal Quader, Vandana Janeja and Justin Stauffe* On Construction of Signcryption Scheme for Smart Card Security *Jayaprakash Kar and Daniyal M. Alghazzawi*
12:30 – 12:45pm *Whitehall*	Conference Closing

Poster Session

Data Infrastructure Building Blocks for Intelligence and Security Informatics Research and Community: Call for Community Participation
Hsinchun Chen, Mark Patton, and Catherine A. Larson

Filtering Spam in Weibo Using Ensemble Imbalanced Classification and Knowledge Expansion
Zhipeng Jin, Qiudan Li, Daniel Zeng and Lei Wang

Modeling Emotion Entrainment of Online Users in Emergency Events
Saike He, Xiaolong Zheng, Daniel Zeng, Bo Xu, Changliang Li, Guanhua Tian, Lei Wang and Hongwei Hao

Power-function-based Observation-weighting Method for Mining Actionable Behavioral Rules
Peng Su and Wenji Mao

Detection of Financial Statement Fraud - Is Accrual Really Useful as an Early Warning Indicator?
Naoto Oshiro

Elliptic Curve Cryptography in Java
Leonidas Deligiannidis

An opportunistic encryption extension for the DNS protocol
Theogene Bucuti and Ram Dantu

A Bottom-up Method for Constructing Topic Hierarchies
Yuhao Zhang, Wenji Mao and Xiaochen Li

Distributed LSI: Parallel Preprocessing and Vector Sharing
Roger Bradford

Pass-Pic: A Mobile User Authentication
Garima Bajwa, Ram Dantu and Ryan Aldridge

Research on Construction Methods of the Shanghai Cooperation Organization Meta-network Model
Kun Wang and Duoyong Sun

An Access Control Resistant to Shoulder-surfing
Jae-Jin Jang and Im Jung

Online/Off-line Ring Signature Scheme with Provable Security
Jayaprakash Kar