GameSec 2018 - October 29-31, 2018
Seattle, WA

DAY 1 – MON OCT 29		
Time	**Session**	**Activity**
8:30-9:00		Registration & Coffee
Tutorial Session "Game-Theoretic Security" (Chair: Quanyan Zhu)		
9:00-10:15		Algorithms for Solving Dynamic Games with Imperfect Information *Branislav Bošanský, Czech Technical University*
10:15-10:45		Coffee Break
10:45 - 12:00		Game Theory for Cyber Deception *Jeff Pawlick, NYU*
12:00-13:30		Lunch (on own)
13:30-13:45		Opening Remarks (General Chairs, Tamer Başar and Radha Poovendran; TPC Chair, Linda Bushnell)
13:45-14:45		Plenary Talk #1: Security and Trust in Networked Systems: Logic, Analysis, Graphs and Games (Chair: Radha Poovendran) *John Baras, University of Maryland*
14:45-15:15		Coffee Break
Session 1: Security Mechanisms and Privacy (Chair: Linda Bushnell)		
15:15-15:40	1.A	Impact of Privacy on Free Online Service Markets *Chong Huang and Lalitha Sankar*
15:40-16:05	1.B	Cyber-warranties as a quality signal for information security products *Daniel W. Woods and Andrew C. Simpson*
16:05-16:30	1.C	Multi-sided Advertising Markets: Dynamic Mechanisms and Incremental User Compensations *Moran Feldman, Gonen Frim and Rica Gonen*
16:30-16:55	1.D	Game Theoretic Analysis of a Byzantine Attacker in Vehicular Mix-Zones *Nick Plewtong and Bruce Debruhl*
16:55-17:20	1E	A Differentially Private and Truthful Incentive Mechanism for Traffic Offload to Public Transportation *Luyao Niu and Andrew Clark*
17:30-18:30		Keynote Talk: "Radical View in S&T; Learn2Reason, CryptoFactory & BFT++" (Chair: Tamer Başar) *Sukarno Mertoguno, Office of Naval Research*

DAY 2 – TUE OCT 30

Time	Session	Activity
8:30-9:00		Registration & Coffee
9:00-10:00		Plenary Talk #2: Estimation in Cyber-Physical Systems Under Attack (Chair: Tamer Başar) *Joao Hespanha University of California, Santa Barbara*
10:00-10:30		Coffee Break
Session 2: Adversarial Games (Chair: Tansu Alpcan)		
10:30-10:55	2.A	Colonel Blotto Game with Coalition Formation for Sharing Resources *Joseph Heyman and Abhishek Gupta*
10:55-11:20	2.B	Distributed Aggregative Games on Graphs in Adversarial Environments *Bahare Kiumarsi and Tamer Başar*
11:20-11:45	2.C	Scaling-up Stackelberg Security Games Applications using Approximations *Arunesh Sinha, Aaron Schlenker, Donnabell Dmello and Milind Tambe*
11:45-12:10	2.D	An Initial Study of Targeted Personality Models in the FlipIt Game *Anjon Basak, Jakub Černý, Marcus Gutierrez, Curtis Shelby, Charles A Kamhoua, Daniel Jones, Branislav Bosansky and Christopher Kiekintveld*
12:10-13:30		Lunch (provided) and Panel
Lunch Panel: Real World Uses of Game Theory for Security (Chair: Milind Tambe)		
12:10-13:30		Detlof von Winterfeldt; USC for Physical Security Kevin Chan; Army Research Labs for Cybersecurity James Slade; SMART Partnership
Session 3: Deception and Security (Chair: Shana Moothedath)		
13:30-13:55	3.A	A Game-Theoretic Analysis of the Adversarial Boyd-Kuramoto Model *Antonin Demazy, Tansu Alpcan and Alex Kalloniatis*
13:55-14:20	3.B	Hypothesis Testing Game for Cyber Deception *Tao Zhang and Quanyan Zhu*
14:20-14:45	3.C	A Two-Stage Deception Game for Network Defense *Wei Wang and Bo Zeng*
14:45-15:10	3.D	Imbalanced Collusive Security Games *Han-Ching Ou, Milind Tambe, Bistra Dilkina and Phebe Vayanos*
15:10-15:40		Coffee Break
Session 4: Special Session: "Adversarial AI" (Chair: Eugene Vorobeychik)		
15:40-16:05	4.A	Training Set Camouflage *Ayon Sen, Scott Alfeld, Xuezhou Zhang, Ara Vartanian, Yuzhe Ma and Xiaojin Zhu*
16:05-16:30	4.B	Reinforcement Learning for Autonomous Defence in Software-Defined Networking *Yi Han, Benjamin Rubinstein, Tamas Abraham, Tansu Alpcan, Olivier De Vel, Sarah Erfani, David Hubczenko, Christopher Leckie and Paul Montague*
16:30-16:55	4.C	Data Poisoning Attacks in Contextual Bandits *Yuzhe Ma, Kwang-Sung Jun, Lihong Li and Xiaojin Zhu*
16:55-17:55		Panel Discussion
19:00-21:00		Conference Dinner: UW Club, 4020 E Stevens Way NE, Seattle, WA 98195 *Outstanding Paper Awards, Sponsored by MDPI Games*

DAY 3 – WED OCT 31

Time	Session	Activity
8:30-9:00		Registration & Coffee
Session 5: APT (Chair: Erik Miehling)		
9:00-9:25	5.A	Multi-Stage Dynamic Information Flow Tracking Game *Shana Moothedath, Dinuka Sahabandu, Andrew Clark, Sangho Lee, Wenke Lee and Radha Poovendran*
9:25-9:50	5.B	Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-physical Systems *Linan Huang and Quanyan Zhu*
9:50-10:15	5.C	Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud *Sailik Sengupta, Ankur Chowdhary, Dijiang Huang and Subbarao Kambhampati*
10:15-10:40	5.D	A Game Theoretical Framework for Inter-Process Adversarial Intervention Detection *Muhammed Sayin, Hossien Hosseini, Radha Poovendran and Tamer Başar*
10:40-11:10		Coffee Break
Session 6: Poster Session (Chair: Linda Bushnell)		
11:10-12:15	6.A	Less is More: Culling the Training Set to Improve Robustness of Deep Neural Networks *Yongshuai Liu, Jiyu Chen and Hao Chen*
11:10-12:15	6.B	Optimal Placement of Honeypots for Network Defense *Justin Mauger, Mark Bilinski and Ryan Gabrys*
11:10-12:15	6.C	A Game Theoretic Analysis of the Twitter Follow-Unfollow Mechanism *Jundong Chen, Md Hossain, Matthias Brust and Naomi Johnson*
11:10-12:15	6.D	Disappointment-Aversion in Security Games *Jasmin Wachter, Stefan Rass, Sandra König and Stefan Schauer*
11:10-12:15	6.E	Deep Learning Based Game-Theoretical Approach to Evade Jamming Attacks *Sandamal Weerasinghe, Tansu Alpcan, Sarah M. Erfani, Christopher Leckie, Peyam Pourbeik and Jack Riddle*
11:10-12:15	6.F	A Learning and Masking Approach to Secure Learning *Linh Nguyen, Sky Wang and Arunesh Sinha*
11:10-12:15	6.G	Cyber-Insurance as a Signaling Game: Self-Reporting and External Security Audits *Aron Laszka, Emmanouil Panaousis and Jens Grossklags*
11:10-12:15	6.H	Algorithms for Subgame Abstraction with Applications to Cyber Defense *Anjon Basak, Marcus Gutierrez and Christopher Kiekintveld*
11:45-13:00		Lunch (provided)

Session 7: Models for Security (Chair: Aron Laszka)

13:00-13:25	7.A	Game Theoretic Security Framework for Quantum Key Distribution *Walter Krawec and Fei Miao*
13:25-13:50	7.B	Perfectly Secure Messsage Transmission against Rational Timid Adversaries *Maiki Fujita, Kenji Yasunaga and Takeshi Koshiba*
13:50-14:15	7.C	Rational Trust Modeling *Mehrdad Nojoumian*
14:15-14:40	7.D	A Bayesian Multi-armed Bandit Approach for Identifying Human Vulnerabilities *Erik Miehling, Baicen Xiao, Radha Poovendran and Tamer Başar*
14:40-15:10		Coffee Break

Session 8: Logic (Chair: Bhaskar Ramasubramanian)

15:10-15:35	8.A	Towards Scientific Incident Response *Jonathan M Spring and David Pym*
15:35-16:00	8.B	Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness *Naif Alzahrani and Nirupama Bulusu*
16:00-16:25	8.C	Approximating Power Indices to Assess Cybersecurity Criticality *Daniel Clouse and David Burke*
16:25-16:50	8.D	A Robust Optimization Approach to Designing Near-Optimal Strategies for Constant-Sum Monitoring Games *Aida Rahmattalabi, Phebe Vayanos and Milind Tambe*
16:50-17:05		Closing Remarks (General Chairs, Tamer Başar and Radha Poovendran)