

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 <i>Branislav Bošanský, Czech Technical University</i>
10:15-10:45		Coffee Break
10:45 - 12:00		Game Theory for Cyber Deception <i>Jeff Pawlick, NYU</i>
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 <i>John Baras, University of Maryland</i>)
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 <i>Chong Huang and Lalitha Sankar</i>
15:40-16:05	1.B	Cyber-warranties as a quality signal for information security products <i>Daniel W. Woods and Andrew C. Simpson</i>
16:05-16:30	1.C	Multi-sided Advertising Markets: Dynamic Mechanisms and Incremental User Compensations <i>Moran Feldman, Gonen Frim and Rica Gonen</i>
16:30-16:55	1.D	Game Theoretic Analysis of a Byzantine Attacker in Vehicular Mix-Zones <i>Nick Plewtong and Bruce Debruhl</i>
16:55-17:20	1E	A Differentially Private and Truthful Incentive Mechanism for Traffic Offload to Public Transportation <i>Luyao Niu and Andrew Clark</i>
17:30-18:30		Invited Talk: "Radical View in S&T; Learn2Reason, CryptoFactory & BFT++" <i>Sukarno Mertoguno, Office of Naval Research</i>

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) <i>Joao Hespanha University of California, Santa Barbara</i>
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 <i>Joseph Heyman and Abhishek Gupta</i>
10:55-11:20	2.B	Distributed Aggregative Games on Graphs in Adversarial Environments <i>Bahare Kiumarsi and Tamer Başar</i>
11:20-11:45	2.C	Scaling-up Stackelberg Security Games Applications using Approximations <i>Arunesh Sinha, Aaron Schlenker, Donnabell Dmello and Milind Tambe</i>
11:45-12:10	2.D	An Initial Study of Targeted Personality Models in the Flipit Game <i>Anjon Basak, Jakub Černý, Marcus Gutierrez, Curtis Shelby, Charles A Kamhoua, Daniel Jones, Branislav Bosansky and Christopher Kiekintveld</i>
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 <i>Antonin Demazy, Tansu Alpcan and Alex Kalloniatis</i>
13:55-14:20	3.B	Hypothesis Testing Game for Cyber Deception <i>Tao Zhang and Quanyan Zhu</i>
14:20-14:45	3.C	A Two-Stage Deception Game for Network Defense <i>Wei Wang and Bo Zeng</i>
14:45-15:10	3.D	Imbalanced Collusive Security Games <i>Han-Ching Ou, Milind Tambe, Bistra Dilkina and Phebe Vayanos</i>
15:10-15:40		Coffee Break
Session 4: Special Session: "Adversarial AI" (Chair: Eugene Vorobeychik)		
15:40-16:05	4.A	Training Set Camouflage <i>Ayon Sen, Scott Alfeld, Xuezhou Zhang, Ara Vartanian, Yuzhe Ma and Xiaojin Zhu</i>
16:05-16:30	4.B	Reinforcement Learning for Autonomous Defence in Software-Defined Networking <i>Yi Han, Benjamin Rubinstein, Tamas Abraham, Tansu Alpcan, Olivier De Vel, Sarah Erfani, David Hubczenko, Christopher Leckie and Paul Montague</i>
16:30-16:55	4.C	Data Poisoning Attacks in Contextual Bandits <i>Yuzhe Ma, Kwang-Sung Jun, Lihong Li and Xiaojin Zhu</i>
16:55-17:55		Panel Discussion
19:00-21:00		Conference Dinner: UW Club, 4020 E Stevens Way NE, Seattle, WA 98195 <i>Best Paper Awards, Sponsored by MDPI Games</i>

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 <i>Shana Moothedath, Dinuka Sahabandu, Andrew Clark, Sangho Lee, Wenke Lee and Radha Poovendran</i>
9:25-9:50	5.B	Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-physical Systems <i>Linan Huang and Quanyan Zhu</i>
9:50-10:15	5.C	Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud <i>Sailik Sengupta, Ankur Chowdhary, Dijiang Huang and Subbarao Kambhampati</i>
10:15-10:40	5.D	A Game Theoretical Framework for Inter-Process Adversarial Intervention Detection <i>Muhammed Sayin, Hossien Hosseini, Radha Poovendran and Tamer Başar</i>
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 <i>Yongshuai Liu, Jiyu Chen and Hao Chen</i>
11:10-12:15	6.B	Optimal Placement of Honeypots for Network Defense <i>Justin Mauger, Mark Bilinski and Ryan Gabrys</i>
11:10-12:15	6.C	A Game Theoretic Analysis of the Twitter Follow-Unfollow Mechanism <i>Jundong Chen, Md Hossain, Matthias Brust and Naomi Johnson</i>
11:10-12:15	6.D	Disappointment-Aversion in Security Games <i>Jasmin Wachter, Stefan Rass, Sandra König and Stefan Schauer</i>
11:10-12:15	6.E	Deep Learning Based Game-Theoretical Approach to Evade Jamming Attacks <i>Sandamal Weerasinghe, Tansu Alpcan, Sarah M. Erfani, Christopher Leckie, Peyam Pourbeik and Jack Riddle</i>
11:10-12:15	6.F	A Learning and Masking Approach to Secure Learning <i>Linh Nguyen, Sky Wang and Arunesh Sinha</i>
11:10-12:15	6.G	Cyber-Insurance as a Signaling Game: Self-Reporting and External Security Audits <i>Aron Laszka, Emmanouil Panaousis and Jens Grossklags</i>
11:10-12:15	6.H	Algorithms for Subgame Abstraction with Applications to Cyber Defense <i>Anjon Basak, Marcus Gutierrez and Christopher Kiekintveld</i>
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 <i>Walter Krawec and Fei Miao</i>
13:25-13:50	7.B	Perfectly Secure Message Transmission against Rational Timid Adversaries <i>Maiki Fujita, Kenji Yasunaga and Takeshi Koshiba</i>
13:50-14:15	7.C	Rational Trust Modeling <i>Mehrdad Nojoumian</i>
14:15-14:40	7.D	A Bayesian Multi-armed Bandit Approach for Identifying Human Vulnerabilities <i>Erik Miehlung, Baicen Xiao, Radha Poovendran and Tamer Başar</i>
14:40-15:10		Coffee Break

Session 8: Logic (Chair: Bhaskar Ramasubramanian)

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