

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 13-02-2019		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 5-Aug-2018 - 31-Dec-2018	
4. TITLE AND SUBTITLE Final Report: 9th Conference on Decision and Game Theory for Security			5a. CONTRACT NUMBER W911NF-18-1-0333		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 611102		
6. AUTHORS			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES University of Washington Office of Sponsored Programs 4333 Brooklyn Ave NE Box 359472 Seattle, WA 98195 -9472			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 73447-NS-CF.3		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Linda Bushnell
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 206-221-6717

RPPR Final Report

as of 21-Feb-2019

Agency Code:

Proposal Number: 73447NSCF

Agreement Number: W911NF-18-1-0333

INVESTIGATOR(S):

Name: Linda Bushnell

Email: lb2@uw.edu

Phone Number: 2062216717

Principal: Y

Organization: **University of Washington**

Address: Office of Sponsored Programs, Seattle, WA 981959472

Country: USA

DUNS Number: 605799469

EIN: 916001537

Report Date: 31-Mar-2019

Date Received: 13-Feb-2019

Final Report for Period Beginning 05-Aug-2018 and Ending 31-Dec-2018

Title: 9th Conference on Decision and Game Theory for Security

Begin Performance Period: 05-Aug-2018

End Performance Period: 31-Dec-2018

Report Term: 0-Other

Submitted By: Linda Bushnell

Email: lb2@uw.edu

Phone: (206) 221-6717

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees:

STEM Participants:

Major Goals: The 9th annual GameSec conference was held in Seattle, WA on October 29-31, 2018. We had 72 attendees. ARO was one of the sponsors.

Recent advances in information and communication technologies pose significant security challenges that impact all aspects of modern society. The 9th Conference on Decision and Game Theory for Security in Seattle, Washington, USA, focuses on protection of heterogeneous, large-scale and dynamic systems as well as managing security risks faced by critical infrastructures through rigorous and practically-relevant analytical methods. GameSec 2018 invites novel, high-quality theoretical and practical-relevant contributions, which apply decision and game theory, as well as related techniques such as distributed optimization, dynamic control and mechanism design, to build resilient, secure, and dependable networked systems. The goal of GameSec 2018 is to bring together academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results that highlight the connections between game theory, control, distributed optimization, economic incentives and real-world security, reputation, trust and privacy problems.

Accomplishments: There were 28 regular and 8 poster papers for GameSec 2018. Springer LNCS printed a book on the papers and they appear in Springer LNCS volume 11199. Two outstanding paper awards were given. Two plenary lectures were given. A special session on Adversarial AI and a tutorial session on Game-Theoretic Security were presented. Many students attended the three-day conference. Forty-four people were in the Technical Program Committee. This committee handled the reviews for the submitted papers.

Training Opportunities: Nothing to Report

Results Dissemination: Dissemination is via the website:

<http://www.gamesec-conf.org/>

and the Springer LNCS vol. 11199 book:

<https://www.springer.com/us/book/9783030015534>

eBook ISBN

978-3-030-01554-1

DOI

10.1007/978-3-030-01554-1

RPPR Final Report as of 21-Feb-2019

Honors and Awards: Two outstanding paper awards were given:

Perfectly Secure Message Transmission against Rational Timid Adversaries

Maiki Fujita, Kenji Yasunaga and Takeshi Koshiba

and

A Differentially Private and Truthful Incentive Mechanism for Traffic Offload to Public Transportation

Luyao Niu and Andrew Clark

Protocol Activity Status:

Technology Transfer: Special Track on "Adversarial AI"

AI techniques have made significant inroads into security applications, such as crime prediction and detection in physical security, and intrusion and malware detection in cybersecurity. An important challenge in such adversarial applications of AI is that sophisticated malicious parties can manipulate the AI decision process, for example, by changing the decision environment or poisoning data used for learning, in order to degrade its effectiveness. The research area of Adversarial AI aims to understand vulnerabilities of AI systems to such adversarial tampering, as well as to develop techniques which make intelligent autonomous decision making robust to adversarial subversion. This special track invites submissions on approaches for attacking and defending AI systems, including research on adversarial machine learning, planning in adversarial settings, adversarial crowdsourcing, and more broadly on the use of AI in security and privacy. Please submit to the special track under the topic "Adversarial AI".

Tutorial Session on "Game-Theoretic Security"

Cyber attacks on both databases and critical infrastructure have threatened public and private sectors. Meanwhile, ubiquitous tracking and wearable computing have infringed upon privacy. Advocates and engineers have recently proposed using defensive deception as a means to leverage the information asymmetry typically enjoyed by attackers as a tool for defenders. In this tutorial, we give the audience an overview on the application of game theory to model deception for cybersecurity and privacy. The goal of this tutorial is to elaborate the taxonomy of deception, to provide the state-of-art literature, and to discuss recent advances in deceptive technologies in cybersecurity and privacy. Presentations from the tutorials will be posted here and here.

PARTICIPANTS:

Participant Type: PD/PI

Participant: Linda Bushnell

Person Months Worked: 2.00

Funding Support:

Project Contribution:

International Collaboration:

International Travel:

National Academy Member: N

Other Collaborators:

Participant Type: Other Professional

Participant: Too Many to list

Person Months Worked: 1.00

Funding Support:

Project Contribution:

International Collaboration:

International Travel:

National Academy Member: N

Other Collaborators:

BOOKS:

Publication Type: Book

Peer Reviewed: Y **Publication Status:** 1-Published

Publication Identifier Type: DOI

Publication Identifier: 10.1007/978-3-030-01554-1

Book Edition: Volume: 11199 Publication Year: 2018 Date Received:

Publication Location: DOI 10.1007/978-3-030-01554-1

RPPR Final Report
as of 21-Feb-2019

Publisher: Springer LNCS

Book Title: Decision and Game Theory for Security

Authors: Linda Bushnell, Radha Poovendran, Tamer Basar

Editor:

Acknowledged Federal Support: Y

WEBSITES:

URL: <http://www.gamesec-conf.org/>

Date Received:

Title: GameSec 32018

Description: Website for GameSec 2018

"Nothing to report in the uploaded pdf (see accomplishments)"