REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
16-03-2019	Final Report	12-Jun-2015 - 11-Jun-2018

4. TITLE AND SUBTITLE
Final Report: ARO: Advanced Security Games For Cyber-Physical Systems

5a. CONTRACT NUMBER
W911NF-15-1-0277

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 California - Davis
Sponsored Programs
1850 Research Park Drive, Suite 300
Davis, CA 95618 -6153

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)
66589-CS.4

12. DISTRIBUTION AVAILIBILITY 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 contrued 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	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Prasant Mohapatra
UU	UU	UU	UU		19b. TELEPHONE NUMBER 530-754-8380

RPPR Final Report
as of 16-Apr-2019

Agency Code:

Proposal Number: 66589CS **Agreement Number: W911NF-15-1-0277**
INVESTIGATOR(S):

Name: Prasant Mohapatra
Email: pmohapatra@ucdavis.edu
Phone Number: 5307548380
Principal: Y

Organization: **University of California - Davis**
Address: Sponsored Programs, Davis, CA 956186153
Country: USA
DUNS Number: 047120084 EIN: 946036494
Report Date: 11-Sep-2018 Date Received: 16-Mar-2019
Final Report for Period Beginning 12-Jun-2015 and Ending 11-Jun-2018
Title: ARO: Advanced Security Games For Cyber-Physical Systems
Begin Performance Period: 12-Jun-2015 **End Performance Period:** 11-Jun-2018
Report Term: 0-Other
Submitted By: Prasant Mohapatra Email: pmohapatra@ucdavis.edu
Phone: (530) 754-8380
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 0

Major Goals: Advanced sophisticated cyber attacks is a major concern for the nation's infrastructure systems and the information technology systems in corporations. These attacks, often classified under the name, Advanced Persistent Threat, (APT), are launched by highly motivated attackers with abundant resources, and are persistent in compromising a system as long as the expected payoff is high. These attacks lead to significant degradation of our technological advantage and could inflict massive damage to our nation's infrastructure and its security. They are extremely difficult to combat because they are inherently adaptive, exhibiting dynamic behavior in response to defense actions. Developing defense mechanisms against these APT attacks is critical to the safety and security of our nation, its technological resources, and its secrets.

Many of today's cyber-physical systems (CPS) are organized in a networked and layered structure; each layer carries out a specific set of functions, which may depend on functions or impact functionality implemented at other layers. Such dependence is beneficial to the normal operation of the system, but can also be utilized by an attacker to harm the system. Moreover, a myopic defense action focusing on a specific attack observed at one level may lead to inefficiencies or vulnerabilities at other levels and trigger new attacks. Therefore, an efficient defense strategy against APT attacks must take the interdependencies among the components in a networked system into account. For a networked system with multiple interdependent levels and that are possibly operated by multiple entities with self-interest, it becomes even more critical to design defense mechanisms that are aligned to their incentives, for both the defenders and the attackers. The overall goal of the proposed research is to study game theoretical models to understand the incentives and fundamental tradeoffs involved in defending/attacking multi-level networked systems, and to design efficient defense strategy accordingly.

Although game theory has been extensively applied to cybersecurity and network security, traditional models are mainly static with complete information, and largely ignore the risk of a system being attacked at multiple levels that have inherent dependencies. We first propose a two-player dynamic game with imperfect/incomplete information to capture the persistency and adaptivity of the players. Our game model hinges on the interdependence structure of a networked system, which determines both the action spaces of the players and the information structure of the game. Building upon the dynamic game model, we will address the major challenges in defending against APT attacks by carrying out the following three tasks.

Defense against the Unknown: To defend against advanced attackers with unknown or uncertain behavior, we propose to develop adaptive defense strategies that can achieve a guaranteed payoff. By utilizing learning frameworks, we will further investigate the impact of stealth behavior and bounded rationality in the context of security games.

Multi-level Attack/Defense: In this thrust, we propose to investigate the impact of multi-level dependencies and design coordinated defense strategies accordingly. We propose to identify both the challenges and the opportunities imposed by the dependencies, and propose strategies that can minimize the impact of the attacks as a whole.

Multi-player Security Games: A large CPS often faces attacks of different types in terms of their dynamics and objectives. We propose to extend the game models to allow multiple independent attackers with diverse behavioral patterns. We will further consider the setting when a large system is managed by multiple entities (defenders) with self-interest, hence has to be protected through joint investment.

Accomplishments: There has been significant interest in studying security games for modeling the interplay of attacks and defenses on various systems involving critical infrastructure, financial system security, political campaigns, and civil safeguarding. However, existing security game models typically either assume additive utility functions, or that the attacker can attack only one target. Such assumptions lead to tractable analysis, but miss key inherent dependencies that exist among different targets in current complex networks. In the following papers [1], [2], we generalize the classical security game models to allow for non-additive utility functions. In [2], we also allow attackers to be able to attack multiple targets. We examine such a general security game from a theoretical perspective and provide a unified view. This work settles the following open questions in the security game domain: (1) How to compactly represent the security game with multiple attacker resources and the non-additive utility functions? (2) How to efficiently solve such a compactly represented game? (3) What is the complexity of the security game when we consider non-additive utility functions and allow the attackers to attack multiple attacker resources? To answer these questions, we provide the following contributions: (1) we first propose a polytope transformation and projection framework to equivalently and compactly represent the zero-sum and non-additive security game with only poly(n) variables; (2) We prove that the problem of determining the Nash equilibrium of the zero-sum and non- additive security game and the problem of optimizing a Pseudo Boolean function over a set system ε can be reduced to each other in polynomial time. The main technique we use is to exploit the geometric structure of the low-dimensional polytope to construct a polynomial time vertex mapping algorithm. (3) We then apply our framework to the non-zero-sum and non-additive security game, and further obtain a similar result that determining the strong Stackelberg equilibrium and the above combinatorial optimization problem is equivalent. (4) Finally, we examine the Nash equilibrium in the non-zero-sum but additive security game. We prove that determining the Nash equilibrium can be reduced to the linear optimization over a set system ε. The key technique we use is based on the transformation, projection of a polytope, and the ellipsoid method.
Cybersecurity is increasingly threatened by advanced and persistent attacks. As these attacks are often designed to disable a system (or a critical resource, e.g., a user account) repeatedly, it is crucial for the defender to keep updating its security measures to strike a balance between the risk of being compromised and the cost of security updates. Moreover, these decisions often need to be made with limited and delayed feedback due to the stealthy nature of advanced attacks. In addition to targeted attacks, such an optimal timing policy under incomplete information has broad applications in cybersecurity. Examples include key rotation, password change, application of patches, and virtual machine refreshing. However, rigorous studies of optimal timing are rare. Further, existing solutions typically rely on a pre-defined attack model that is known to the defender, which is often not the case in practice. In this work, we make an initial effort towards achieving optimal timing of security updates in the face of unknown stealthy attacks. In [3], we consider a variant of the influential FlipIt game model with asymmetric feedback and unknown attack time distribution, which provides a general model to consecutive security updates. The defender's problem is then modeled as a time associative bandit problem with dependent arms. We derive upper confidence bound based learning policies that achieve low regret compared with optimal periodic defense strategies that can only be derived when attack time distributions are known.

[1] S. Wang, F. Liu, and N. B. Shroff, "Non-additive Security Games," AAAI'17, San Francisco, CA, Feb. 2017
[2] S. Wang and N. B. Shroff, "Security Game with Non-additive Utilities and Multiple Attacker Resources," ACM SIGMETRICS'17, Urbana-Champaign, IL, Jun. 2017. (Kenneth C. Sevcik Outstanding Student Paper Award).
[3] Z. Zheng, N. B. Shroff, and P. Mohapatra, "When to Reset Your Keys: Optimal Timing of Security Updates via Learning," AAAI'17, San Francisco, CA, Feb. 2017.

Training Opportunities: During the execution of the project, a postdoctoral trainee and a graduate student gained very valuable experience.

Eventually, the Postdoctoral associate secured a job of Assistant Professor at UC Davis.

RPPR Final Report
as of 16-Apr-2019

Results Dissemination: The results were disseminated through the three publication uploaded along with this report.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Prasant Mohapatra
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Ness Shroff
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Postdoctoral (scholar, fellow or other postdoctoral position)
Participant: Zizhan Zheng
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Hao Fu
Person Months Worked: 6.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

CONFERENCE PAPERS:

RPPR Final Report
as of 16-Apr-2019

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: AAAI 2017
Date Received: 02-Oct-2017 Conference Date: 01-Feb-2017 Date Published: 01-Feb-2017
Conference Location: San Francisco
Paper Title: Non-additive Security Games
Authors: S. Wang, F. Liu, N. B. Shroff
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: AAAI 2017
Date Received: 16-Mar-2019 Conference Date: 02-Feb-2017 Date Published: 02-Feb-2017
Conference Location: San Francisco, CA
Paper Title: When to Reset Your Keys: Optimal Timing of Security Updates via Learning
Authors: Z. Zheng, N. B. Shroff, P. Mohapatra
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE INFOCOM
Date Received: 16-Mar-2019 Conference Date: 01-May-2017 Date Published: 02-May-2017
Conference Location: Atlanta, GA
Paper Title: LeakSemantic: Identifying Abnormal Sensitive Network Transmissions in Mobile Applications
Authors: H. Fu, Z. Zheng. S. Bose. M. Bishop, P. Mohapatra
Acknowledged Federal Support: **Y**

There has been significant interest in studying security games for modeling the interplay of attacks and defenses on various systems involving critical infrastructure, financial system security, political campaigns, and civil safeguarding. However, existing security game models typically either assume additive utility functions, or that the attacker can attack only one target. Such assumptions lead to tractable analysis, but miss key inherent dependencies that exist among different targets in current complex networks. In the following papers [1], [2], we generalize the classical security game models to allow for non-additive utility functions. In [2], we also allow attackers to be able to attack multiple targets. We examine such a general security game from a theoretical perspective and provide a unified view. This work settles the following open questions in the security game domain: (1) How to compactly represent the security game with multiple attacker resources and the non-additive utility functions? (2) How to efficiently solve such a compactly represented game? (3) What is the complexity of the security game when we consider non-additive utility functions and allow the attackers to attack multiple attacker resources? To answer these questions, we provide the following contributions: (1) we first propose a polytope transformation and projection framework to equivalently and compactly represent the zero-sum and non-additive security game with only poly(n) variables; (2) We prove that the problem of determining the Nash equilibrium of the zero-sum and non- additive security game and the problem of optimizing a Pseudo Boolean function over a set system ε can be reduced to each other in polynomial time. The main technique we use is to exploit the geometric structure of the low-dimensional polytope to construct a polynomial time vertex mapping algorithm. (3) We then apply our framework to the non-zero-sum and non-additive security game, and further obtain a similar result that determining the strong Stackelberg equilibrium and the above combinatorial optimization problem is equivalent. (4) Finally, we examine the Nash equilibrium in the non-zero-sum but additive security game. We prove that determining the Nash equilibrium can be reduced to the linear optimization over a set system ε. The key technique we use is based on the transformation, projection of a polytope, and the ellipsoid method.

Cybersecurity is increasingly threatened by advanced and persistent attacks. As these attacks are often designed to disable a system (or a critical resource, e.g., a user account) repeatedly, it is crucial for the defender to keep updating its security measures to strike a balance between the risk of being compromised and the cost of security updates. Moreover, these decisions often need to be made with limited and delayed feedback due to the stealthy nature of advanced attacks. In addition to targeted attacks, such an optimal timing policy under incomplete information has broad applications in cybersecurity. Examples include key rotation, password change, application of patches, and virtual machine refreshing. However, rigorous studies of optimal timing are rare. Further, existing solutions typically rely on a pre-defined attack model that is known to the defender, which is often not the case in practice. In this work, we make an initial effort towards achieving optimal timing of security updates in the face of unknown stealthy attacks. In [3], we consider a variant of the influential FlipIt game model with asymmetric feedback and unknown attack time distribution, which provides a general model to consecutive security updates. The defender's problem is then modeled as a time associative bandit problem with dependent arms. We derive upper confidence bound based learning policies that achieve

low regret compared with optimal periodic defense strategies that can only be derived when attack time distributions are known.

[1] S. Wang, F. Liu, and N. B. Shroff, "Non-additive Security Games," AAAI'17, San Francisco, CA, Feb. 2017

[2] S. Wang and N. B. Shroff, "Security Game with Non-additive Utilities and Multiple Attacker Resources," ACM SIGMETRICS'17, Urbana-Champaign, IL, Jun. 2017. (Kenneth C. Sevcik Outstanding Student Paper Award).

[3] Z. Zheng, N. B. Shroff, and P. Mohapatra, "When to Reset Your Keys: Optimal Timing of Security Updates via Learning," AAAI'17, San Francisco, CA, Feb. 2017.