REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
10-09-2020	Final Report	25-Jun-2013 - 24-Jun-2018

4. TITLE AND SUBTITLE
Final Report: Science of Security

5a. CONTRACT NUMBER
W911NF-13-1-0094

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
North Carolina State University
Office of Sponsored Programs and Regulatory Compli
Campus Box 7514
Raleigh, NC 27695 -7514

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)
63141-CS.67

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			Laurie Williams
UU	UU	UU	UU		19b. TELEPHONE NUMBER 919-513-4151

RPPR Final Report
as of 29-Jul-2022

Agency Code: 21XD

Proposal Number: 63141CS **Agreement Number: W911NF-13-1-0094**
INVESTIGATOR(S):

Name: Michael Rappa
Email: mrappa@ncsu.edu
Phone Number: 9195130480
Principal: N

Name: Laurie Ann Williams
Email: williams@csc.ncsu.edu
Phone Number: 9195134151
Principal: Y

Organization: **North Carolina State University**
Address: Office of Sponsored Programs and Regulatory Compliance, Raleigh, NC 276957514
Country: USA
DUNS Number: 042092122 EIN: 566000756

Report Date: 24-Sep-2018 Date Received: 10-Sep-2020
Final Report for Period Beginning 25-Jun-2013 and Ending 24-Jun-2018
Title: Science of Security
Begin Performance Period: 25-Jun-2013 **End Performance Period:** 24-Jun-2018
Report Term: 0-Other

Submitted By: Laurie Williams Email: williams@csc.ncsu.edu
Phone: (919) 513-4151

STEM Degrees: **STEM Participants:**

Major Goals: Beginning in September 2014, the majority of project expenses were charged directly to an NSA account.

The scientific progress is reported on that project. The goal of that project is threefold:

*Advance security research in five hard problem areas: Human Behavior, Security Metrics,Scalability and Composability, Resilience, and Policy-based Secure Collaboration

* Build a science of security community

* Advance the research methods used for cybersecurity research

Accomplishments: * Advance security research in five hard problem areas: Human Behavior, Security Metrics, Scalability and Composability, Resilience, and Policy-based Secure Collaboration - published papers in 4 of the 5 hard problems

* Build a science of security community - held a Science of Security community day

* Advance the research methods used for cybersecurity research - published guidelines on research methods - analyzed papers

Training Opportunities: Nothing to Report

Results Dissemination: All dissemination was reported on the NSA projec

Honors and Awards: Nothing to Report

RPPR Final Report
as of 29-Jul-2022

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Laurie Ann Williams
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Automatica
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.automatica.2014.05.012
Volume: 50 Issue: 8 First Page #: 1989
Date Submitted: Date Published:
Publication Location:
Article Title: Reachability for partially observable discrete time stochastic hybrid systems
Authors:
Keywords: Hybrid systems, Reachability, Optimal control, Stochastic control
Abstract: When designing optimal controllers for any system, it is often the case that the true state of the system is unknown to the controller. Imperfect state information must be taken into account in the controller's design in order to preserve its optimality. The same is true when performing reachability calculations. To estimate the probability that the state of a stochastic system reaches, or stays within, some set of interest in a given time horizon, it is necessary to find a controller that drives the system to that set with maximum probability, given the controller's knowledge of the true state of the system. To date, little work has been done on stochastic reachability calculations with partially observable states. The work that has been done relies on converting the reachability optimization problem to one with an additive cost function, for which theoretical results are well known. Our approach is to preserve the multiplicative cost structure when deriving a sufficient statistic tha
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support:

RPPR Final Report
as of 29-Jul-2022

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Dependable and Secure Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TDSC.2013.58
Volume: 11 Issue: 3 First Page #: 252
Date Submitted: Date Published:
Publication Location:
Article Title: Effective Risk Communication for Android Apps
Authors:
Keywords: Risk communication, usability, mobile security
Abstract: The popularity and advanced functionality of mobile devices has made them attractive targets for malicious and intrusive applications (apps). Although strong security measures are in place for most mobile systems, the area where these systems often fail is the reliance on the user to make decisions that impact the security of a device. As our prime example, Android relies on users to understand the permissions that an app is requesting and to base the installation decision on the list of permissions. Previous research has shown that this reliance on users is ineffective, as most users do not understand or consider the permission information. We propose a solution that leverages a method to assign a risk score to each app and display a summary of that information to users. Results from four experiments are reported in which we examine the effects of introducing summary risk information and how best to convey such information to a user. Our results show that the inclusion of risk-score i
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: EDBT/ICDT Workshops 2014: 415
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 415
Date Submitted: 3/21/18 12:00AM Date Published: 12/19/14 5:00AM
Publication Location:
Article Title: Data Anonymization: The Challenge from Theory to Practice
Authors: Ting Yu
Keywords: dataset privacy, data anonymization
Abstract: Data anonymization is an important technique for privacy protection when sensitive data are shared between organizations and with the public. Significant advances have been made in data anonymization in recent years, in terms of privacy models, anonymization algorithms and applications. Meanwhile, though we have seen quite a few instances where privacy is violated due to unsuccessful ad hoc anonymization schemes, many advanced techniques developed in the research community seem to have a hard time to be accepted and adopted in practice. In this talk, we will first provide a quick overview of the research development in data anonymization, and then discuss practical concerns and challenges to successfully apply these techniques in specific application domains.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **N**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution:
Date Received: 05-Sep-2014 Completion Date:
Title: Redundancy-Based Detection of Security Anomalies in Web-Server Environments
Authors:
Acknowledged Federal Support:

RPPR Final Report
as of 29-Jul-2022

Publication Type: Thesis or Dissertation
Institution:
Date Received: 05-Sep-2014 Completion Date:
Title: A Study of Fedora Security Profile
Authors:
Acknowledged Federal Support:

Partners

,

I certify that the information in the report is complete and accurate:
Signature:
Signature Date:

W911NF1310094 : Science of Security

Reporting Period: AUG 01, 2016 to JUL 31, 2017

Date Received: 2018-03-21 15:10:36.0

Submitter: Laurie Williams

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

Major Goals

Beginning in September 2014, the majority of project expenses were charged directly to an NSA account. The scientific progress is reported on that project. The goal of that project is threefold: * Advance security research in five hard problem areas: Human Behavior, Security Metrics, Scalability and Composability, Resilience, and Policy-based Secure Collaboration * Build a science of security community * Advance the research methods used for cybersecurity research

---

Accomplishments Under Goals

* Advance security research in five hard problem areas: Human Behavior, Security Metrics, Scalability and Composability, Resilience, and Policy-based Secure Collaboration - published papers in 4 of the 5 hard problems

* Build a science of security community - held a Science of Security community day

* Advance the research methods used for cybersecurity research - published guidelines on research methods - analyzed papers

---

Plans Next Period

Nothing to Report

Results Dissemination

All dissemination was reported on the NSA project

Honors and Awards

Nothing to Report

Training Opportunities

All graduate students attended a weekly seminar where research methods were taught and applied. Students presented their own work and got feedback on the work. We held a summer workshop on research methods.

Technology Transfer

Interaction with NSA.

Participants

Name	Role	Person Months
Williams, Laurie	PD/PI	12