REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
27-05-2020	Final Report	9-May-2016 - 31-Dec-2019

4. TITLE AND SUBTITLE
Final Report: Correct Enforcement of Access Control Policy in Modern Operating Systems

5a. CONTRACT NUMBER
W911NF-16-1-0299

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
North Carolina State University
2701 Sullivan Drive
Admin Srvcs III, 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)
67888-CS.13

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			William Enck
UU	UU	UU	UU		19b. TELEPHONE NUMBER 919-513-7905

RPPR Final Report
as of 28-May-2020

Agency Code:

Proposal Number: 67888CS **Agreement Number: W911NF-16-1-0299**
INVESTIGATOR(S):

Name: Dr. William Enck
Email: WHENCK@NCSU.EDU
Phone Number: 9195137905
Principal: Y

Organization: **North Carolina State University**
Address: 2701 Sullivan Drive, Raleigh, NC 276957514
Country: USA
DUNS Number: 042092122 EIN: 566000756
Report Date: 31-Mar-2020 Date Received: 27-May-2020
Final Report for Period Beginning 09-May-2016 and Ending 31-Dec-2019
Title: Correct Enforcement of Access Control Policy in Modern Operating Systems
Begin Performance Period: 09-May-2016 **End Performance Period:** 31-Dec-2019
Report Term: 0-Other
Submitted By: Dr. William Enck Email: WHENCK@NCSU.EDU
Phone: (919) 513-7905
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 4

Major Goals: The modern consumer operating system evolved significantly with the introduction of the Android and iOS smartphone platforms. Android marketshare now approaches that of Microsoft Windows, and both Android and iOS are transcending a wide variety of consumer and government computing devices. These modern OSes include feature-rich runtime environments that caused designers to re-think access control. The underlying theme of this project is to understand the access control policy of modern OSes and to design techniques that ensure its correct enforcement.

The project has three main thrusts to achieve this goal:

Mining access control policy: A modern OS has a multitude of access control policies that include traditional discretionary access control (e.g., Unix permissions), traditional mandatory access control (e.g., SELinux), as well as hard-coded checks throughout the runtime environment. This policy must be extracted and modeled for analysis.

Analyze access control policy: The notion of “correctness” for least privilege access control policies is ill-defined, with ground-truth residing only in the mind of the system designer or developer, if at all. We seek to approximate correctness through latent signals (e.g., patterns of consistency) while taking into consideration subtleties of the various enforcement mechanisms (e.g., delegation).

Design comparison: Access control mechanisms are included for various reasons, including legacy dependencies, ad hoc response to threats, and perceived system hardening. We seek to understand the value-add of individual access control mechanisms with respect to their composition in the whole. We further seek to compare access control mechanisms across platforms.

Accomplishments: Over the course of the project, we performed deep investigation of both Android and iOS while accomplishing the stated goals.

Android: We designed several semi-automated analysis frameworks that identify access control vulnerabilities in the Android platform. Our Access Control Miner (ACMiner) static program analysis framework mines access control policy from each remote procedure call (RPC) entry point into Android’s system services. A key novelty of ACMiner is the ability to not only identify permission and UID checks, but also service-specific access control logic. The ACMiner tool uses association rule mining to identify inconsistent access control checks and also suggest changes, which significantly aids the task of a security analyst. ACMiner also forms the foundation of two subsequent

analysis frameworks. The Android Redelegation Finder (ARF) identifies confused deputy vulnerabilities that occur when RPC entry points to system services call other RPC entry points. We discover that Android's RPC entry points are highly interconnected and ARF optimizes the analysis by modeling the access control logic between them. Finally, our File Re-Delegation (FReD) framework extends ARF's confused deputy analysis to include files accessed through RPC entry points, taking into account the Unix permissions that are assigned to those files. Finally, we studied SEAndroid policy, identifying over-permissive access patterns and flaws that occur at the confluence of MAC and DAC specification. All discovered vulnerabilities were reported to Google.

iOS: We perform the first deep analysis of access control policy for the iOS platform. We created SandBlaster to reverse engineer Apple's Sandbox Policy Language from its binary form back into its human readable Scheme-like language. Next, we created SandScout to formally model the policy rules using Prolog, upon which we performed logic queries to identify access control policy vulnerabilities. We then created iOracle to extend our access control analysis to incorporate Unix Permissions, allow us to perform a system-wide analysis and identify gadgets that can be used as part of device jailbreaks. Finally, we created Kobold to extend our analysis to Apple's NSXPC, the predominant form of inter-process communication (IPC) used by system services and daemons. Since source code is not available for iOS, we performed dynamic testing to extract a profile of access control checks for each RPC entry point, identifying a number of missing checks in the process. All discovered vulnerabilities were reported to Apple.

Through these efforts, we achieved our third goal of comparing the access control designs of Android and iOS. We found that iOS has evolved significantly over the years, approaching an architecture similar to Android by moving more access control decisions into system services that check entitlements (which are similar to Android's install-time permissions). Through our interactions with Apple, we learned that some of our vulnerability discoveries have motivated some of this re-architecting.

2) SPECIFIC OBJECTIVES

Mining access control policy: Our analysis frameworks (ACMiner, SandBlaster, Kobold) successfully mine access control policy specification from code using a range of static and dynamic program analysis.

Analyzing access control policy: Our analysis frameworks (ACMiner, ARF, FReD, SPOKE, SandScout, iOracle, Kobold) create a formal representation of access control policy and define invariants and rules to identify policy flaws.

Design comparison: Our analysis of the access control architectures and Android and iOS identified many similarities and have helped better understand their defenses.

3) SIGNIFICANT RESULTS

Our work led to the discovery of hundreds of vulnerabilities, which were reported to Google and Apple. The vulnerabilities have been fixed and a number of them were deemed significant enough to issue CVEs:

Android CVEs:

CVE-2019-2098
CVE-2019-2092
CVE-2019-2091
CVE-2019-2090
CVE-2019-9351
CVE-2019-9377
CVE-2019-9438
CVE-2020-0208
CVE-2020-0209
CVE-2020-0210

iOS CVEs:

CVE-2015-7001
CVE-2016-4719

CVE-2016-4620
CVE-2016-4686
CVE-2016-4664
CVE-2016-4665
CVE-2018-4446
CVE-2019-8502
CVE-2019-8698

4) KEY OUTCOMES

We have characterized the access control frameworks of both Android and iOS, designing algorithmic frameworks for semi-automatically identifying access control vulnerabilities. Our findings have led to important security fixes in both Android and iOS, and in some cases have caused system designers to rethink how access control enforcement is performed.

Training Opportunities: This project formed the central contributions of the dissertations of two PhD students, Luke Deshotels and Sigmund Gorski, both of which have successfully defended. It has also aided the training of several other PhD students who participated in the research for the papers.

Results Dissemination: The papers were presented at many academic conferences both domestically and internationally. See the publications for the list of conference venues.

It was also presented as invited talks at both conferences and universities, including:

College of William and Mary, Williamsburg, VA
King's College London (KCL), London, UK
CyberSecurity@KAIST International Workshop, Daejeon, Korea
BSides Raleigh, Raleigh, NC

Note that BSides Raleigh is a venue attended by security practitioners who are not typically exposed to academic research.

Honors and Awards: Distinguished Paper, ACM Asia Conference on Computer and Communications Security (ASIACCS), 2017

Protocol Activity Status:

Technology Transfer: Open source projects:

ACMiner: https://github.com/wspr-ncsu/acminer
ARF: https://github.com/wspr-ncsu/arf
SandBlaster: https://github.com/malus-security/sandblaster
iExtractor: https://github.com/malus-security/iExtractor

Additionally, we are interacting with Google to encourage internal use of ACMiner, ARF, and eventually FReD.

PARTICIPANTS:

Participant Type: PD/PI
Participant: William Enck
Person Months Worked: 7.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Luke Deshotels
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Sigmund Albert Gorski III
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Adwait Nadkari
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Benjamin Andow
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ACM Conference on Computer and Communications Security (CCS)
Date Received: 23-Aug-2017 Conference Date: 24-Oct-2016 Date Published:
Conference Location: Vienna, Austria
Paper Title: SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles,
Authors: Luke Deshotels, Razvan Deaconescu, Mihai Chiroiu, Lucas Davi, William Enck, and Ahmad-Reza Sade
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 28-May-2020

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ACM Asia Conference on Computer and Communications Security (ASIACCS)
Date Received: 23-Aug-2017 Conference Date: 02-Apr-2017 Date Published:
Conference Location: Abu Dhabi, United Arab Emirates
Paper Title: SPOKE: Scalable Knowledge Collection and Attack Surface Analysis of Access Control Policy for Security Enhanced Android
Authors: Ruowen Wang, Ahmed M. Azab, William Enck, Ninghui Li, Peng Ning, Xun Chen, Wenbo Shen, and Yu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Annual Computer Security Applications Conference (ACSAC)
Date Received: 22-Aug-2018 Conference Date: 04-Dec-2017 Date Published: 04-Dec-2017
Conference Location: San Juan, Puerto Rico, USA
Paper Title: Analysis of SEAndroid Policies: Combining MAC and DAC in Android
Authors: Haining Chen, Ninghui Li, William Enck, Yousra Aafer, and Xiangyu Zhang
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2018 ACM Asia Conference on Computer and Communications Security
Date Received: 22-Aug-2018 Conference Date: 04-Jun-2018 Date Published: 04-Jun-2018
Conference Location: Incheon, Republic of Korea
Paper Title: iOracle: Automated Evaluation of Access Control Policies in iOS
Authors: Luke Deshotels, Razvan Deaconescu, Costin Carabas, Iulia Manda, William Enck, Mihai Chiroiu, Ninghu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ACM CODASPY 2019
Date Received: 22-Aug-2019 Conference Date: 25-Mar-2019 Date Published:
Conference Location: Dallas, TX
Paper Title: PolicyMiner: Extraction and Analysis of Authorization Checks in Android's Middleware
Authors: Sigmund Albert Gorski III, Benjamin Andow, Adwait Nadkarni, Sunil Manandhar, William Enck, Eric Bod
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)
Date Received: 22-Aug-2019 Conference Date: 15-May-2019 Date Published: 15-May-2019
Conference Location: Miami, FL, USA
Paper Title: ARF: Identifying Re-Delegation Vulnerabilities in Android System Services
Authors: Sigmund Albert Gorski III, William Enck
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 2-Awaiting Publicat
Conference Name: IEEE Symposium on Security and Privacy
Date Received: 12-May-2020 Conference Date: 18-May-2020 Date Published:
Conference Location: San Francisco, CA
Paper Title: Kobold: Evaluating Decentralized Access Control for Remote NSXPC Methods on iOS
Authors: Luke Deshotels, Costin Carabas, Jordan Beichler, Razvan Deaconescu, William Enck
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 28-May-2020

Publication Type: Conference Paper or Presentation **Publication Status:** 5-Submitted
Conference Name: USENIX Security
Date Received: 12-May-2020 Conference Date: 12-Aug-2020 Date Published:
Conference Location: Boston, MA
Paper Title: FReD: Identifying File Re-Delegation in Android System Services
Authors: Sigmund Albert Gorski III, William Enck, Haining Chen
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 5-Submitted
Conference Name: USENIX Security
Date Received: 12-May-2020 Conference Date: 12-Aug-2020 Date Published:
Conference Location: Boston, MA
Paper Title: PolyScope: Multi-Policy Access Control Analysis to Compute Authorized Attack Operations in Android Systems
Authors: Yu-Tsung Lee, William Enck, Haining Chen, Hayawardh Vijayakumar, Ninghui Li, Giuseppe Petracca, D
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: North Carolina State University
Date Received: 22-Aug-2019 Completion Date: 8/3/18 2:55PM
Title: Automated Evaluation of Access Control in the iPhone Operating System
Authors: Luke Deshotels
Acknowledged Federal Support: **Y**

Publication Type: Thesis or Dissertation
Institution: North Carolina State University
Date Received: 12-May-2020 Completion Date: 1/31/20 8:58PM
Title: Semi-Automated Evaluation of Access Control Enforcement in the Android Platform
Authors: Sigmund Albert Gorski III
Acknowledged Federal Support: **Y**

Nothing to report in the uploaded pdf (see accomplishments)