AFRL-AFOSR-VA-TR-2018-0295

YIP: A logical Foundation for Cybersecurity Built on Hyperproperties

Michael Clarkson
CORNELL UNIVERSITY

07/13/2018
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTA2
Arlington, Virginia 22203
Air Force Materiel Command

DISTRIBUTION A: Distribution approved for public release.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03-08-2018	Final Performance	30 Sep 2014 to 29 Mar 2018

4. TITLE AND SUBTITLE
YIP: A logical Foundation for Cybersecurity Built on Hyperproperties

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-14-1-0334

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Michael Clarkson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
CORNELL UNIVERSITY
373 PINE TREE RD
ITHACA, NY 14850-2820 US

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR RTA2

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-VA-TR-2018-0295

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Our research in this grant contributed to the science of security. We developed a verification methodology for a specific hyperproperty, and we provided a powerful new security mechanism for mobile devices, as well as other GUI-based, security-sensitive systems. We also made progress on a verification methodology that works for all hyperproperties expressible in HyperLTL, and on establishing the trustworthiness of that methodology.

15. SUBJECT TERMS
HYPERPROPERTIES, SCIENCE OF SECURITY

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					NGUYEN, TRISTAN
Unclassified	Unclassified	Unclassified	UU		**19b. TELEPHONE NUMBER** *(Include area code)* 703-696-7796

Final Report:
YIP: A Logical Foundation for Cybersecurity Built on Hyperproperties
FA9550-14-1-0334

PI: Michael R. Clarkson*

Dates covered by report:
30 September 2014 – 29 March 2018

1 Summary of Grant Objectives

The objectives of the proposed research were to develop logical foundations for cybersecurity using the theory of hyperproperties [2] as a basis. We proposed the following topics as questions of interest:

- How to prove that programs satisfy hyperproperties.
- Mechanization of the proof theory of hyperproperties in a proof assistant.
- The formal semantics of authorization logics.
- How to quantify the availability properties of programs by analysis of their source code, including how they consume and produce information and system resources.
- A mathematical theory that simultaneously characterizes confidentiality, integrity, and availability.

*Department of Computer Science, Cornell University, Ithaca, NY, 14853.

2 Highlights of Research

2.1 Verification of Apps that Declassify Information

In collaboration with a team at the University of Maryland, we developed a new framework for Android app security based on information flow control and user interactions [7]. The key idea behind our framework is that users naturally express their intentions about information release as they interact with an app. For example, clicking a button may permit an app to release a phone number over the Internet. Or, as another example, toggling a radio button from "coarse" to "fine" and back to "coarse" may temporarily permit an app to use fine-grained GPS location rather than a coarse-grained approximation.

To model these kinds of scenarios, we introduced *interaction-based declassification policies*, which extensionally specify what information flows may occur after which sequences of events. Events are GUI interactions (e.g., clicking a button), inputs (e.g., reading the phone number), or outputs (e.g., sending over the Internet). A policy is a set of declassification conditions, written in a logic based (like HyperLTL) on LTL. We formalized a semantic security condition, *interaction-based noninterference* (IBNI), over sets of event traces generated by an app. Intuitively, IBNI holds of an app and policy if the system appears to be a deterministic function of low inputs, after all inputs have been declassified according to the policy.

We built ClickRelease, a static analysis tool to check whether an Android app and its declassification policy satisfy IBNI. ClickRelease generates event traces using SymDroid [6], a Dalvik bytecode symbolic executor. ClickRelease works by simulating user interactions with the app and recording the resulting execution traces. In practice, it is not feasible to enumerate all program traces, so ClickRelease generates traces up to some input depth of n GUI events. ClickRelease then synthesizes a set of logical formulae that hold if and only if IBNI holds, and uses Z3 [4] to check their satisfiability.

To validate ClickRelease, we used it to analyze four Android apps, including both secure and insecure variants of those apps. We ran each app variant under a range of input depths, and confirmed that, as expected, ClickRelease scales exponentially. However, we manually examined each app and its policy, and found that an input depth of at most 5 is sufficient to guarantee detection of a security policy violation (if any) for these cases. We ran ClickRelease at these minimum input depths and found that it correctly passes and fails the secure and insecure app variants, respectively. Moreover, at these depths, ClickRelease takes just a few seconds to run.

Our research thus contributed to the science of security by

- developing a verification methodology for a specific hyperproperty; and
- providing a powerful new security mechanism for mobile devices, as well as other GUI-based, security-sensitive systems.

2.2 Verification of Hyperproperties

The theory of *trace properties*, which characterizes correct behavior of programs in terms of properties of individual execution paths, developed out of an interest in proving the correctness of programs. Verification of security, unfortunately, isn't directly possible with that theory, because some important security policies require sets of execution paths to model. But in our ongoing work on the theory of *hyperproperties* [2], we have shown that certain classes of security policies are amenable to verification. Specifically, in our work sponsored by AFOSR (under award FA9550-12-1-0034) in previous years, we developed logics named HyperLTL and HyperCTL* for automated model checking of hyperproperties [1]. That model checker, however, inherently works only for a fragment of HyperLTL, because of the model-checking algorithm it uses. So there are hyperproperties expressible in HyperLTL that we cannot hope to verify using that technique.

We worked to develop a *proof system* for HyperLTL—that is, a set of axioms and inference rules that could be used to prove all valid formulas of the logic. (The beginning of this work was funded through an NSA Science of Security Lablet at the University of Maryland, but when PI Clarkson moved from GW to Cornell, that funding was eliminated.) So far we have created the proof system and formalized it in Coq (a mechanized proof assistant),[1].

Our next goal was to prove the *soundness* and *completeness* of the proof system in Coq. Soundness would assure that the proof system itself cannot prove invalid formulas. Completeness would ensure that all valid formulas can be proved. We would then have a verification technique that can used for all hyperproperties expressible in HyperLTL.

This task remains unfinished at the end of the grant. When completed, it would contribute to the science of security by

[1] `http://coq.inria.fr`

- giving a verification methodology that works for all hyperproperties expressible in HyperLTL; and
- establishing the trustworthiness of that methodology by mechanically checking its correctness in Coq.

2.3 Other Research Supported

Andrew Hirsch, a PhD candidate at Cornell and former student of PI Clarkson, was funded for one semester on this grant. Hirsch worked on *authorization logics*, which are used to analyze the correctness of authorization mechanisms in distributed systems. Hirsch is developing Flow-Limited Authorization First-Order Logic (henceforth, FLAFOL), which is an authorization logic that incorporates *information-flow labels.* FLAFOL enables proof that authorization mechanisms cannot leak private information.

Tom Magrino and Isaac Sheff, both PhD candidates at Cornell, were funded for two semesters on this grant. They are working to develop a new consensus protocol that supports heterogeneous trust among the participants. The idea is that different participants can have different opinions about how trustworthy the other participants are. This consensus protocol is being used to develop a new kind of blockchain that allows organizations to support a blockchain together in a federated way [8].

3 Transitions

There are no transitions to report.

4 Publications

- *Quantification of Integrity.* See reference [3] below for details.
- *Du-Vote: Remote Electronic Voting with Untrusted Computers.* See reference [5] below for details.
- *Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution.* See reference [7] below for details.

5 Students Supported

- Steven Frink, PhD student at Cornell University, now at IBM
- Andrew Hirsch, PhD student at Cornell University
- Thomas Magrino, PhD student at Cornell University
- Isaac Sheff, PhD student at Cornell University
- Hunter Goldstein, undergraduate student at Cornell University (not supported financially, but advised by PI Clarkson and worked on research related to this award)

6 Technical Outcomes Achieved

Of the key technical outcomes originally proposed for this grant, we achieved the following:

- Original goal: Mechanization of a proof system for hyperproperties in Coq. *What we achieved: A formalization of the proof system, and a partial proof of soundness.*
- A case study using a proof system for hyperproperties to verify a piece of security-critical code. *What we achieved: A case study of using a symbolic executor to verify security of Android apps, especially as they declassify information. Although that project began by using a proof system for hyperproperties, we discovered that a simpler technique (based on symbolic execution and on trace properties) sufficed.*

References

[1] Michael R. Clarkson, Bernd Finkbeiner, Masoud Koleini, Kristopher K. Micinski, Markus N. Rabe, and César Sánchez. Temporal logics for hyperproperties. In *Proc. Conference on Principles of Security and Trust (POST)*, pages 265–284, April 2014.

[2] Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.

[3] Michael R. Clarkson and Fred B. Schneider. Quantification of integrity. *Mathematical Structures in Computer Science*, 25(2):207–258, 2015.

[4] Leonardo de Moura and Nikolaj Bjrner. Z3: An efficient SMT solver. In *Proc. of Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340, 2008.

[5] Gurchetan S. Grewal, Mark D. Ryan, Liqun Chen, and Michael R. Clarkson. Du-vote: Remote electronic voting with untrusted computers. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 155–169, July 2015.

[6] Jinseong Jeon, Kristopher K. Micinski, and Jeffrey S. Foster. SymDroid: Symbolic Execution for Dalvik Bytecode. Technical Report CS-TR-5022, Department of Computer Science, University of Maryland, College Park, July 2012.

[7] Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon, Jeffrey S. Foster, and Michael R. Clarkson. Checking interaction-based declassification policies for Android using symbolic execution. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, pages 520–538, September 2015.

[8] Isaac Sheff, Xinwen Wang, Andrew C. Myers, and Robbert van Renesse. A web of blocks. Technical Report arXiv:1806.06978 [cs.DC], Cornell University, June 2018.

AFOSR Deliverables Submission Survey

Response ID:9993 Data

1.

Report Type

Final Report

Primary Contact Email
Contact email if there is a problem with the report.

mrc26@cornell.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

6072550278

Organization / Institution name

Cornell University

Grant/Contract Title
The full title of the funded effort.

YIP: A Logical Foundation for Cybersecurity Built on Hyperproperties

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-14-1-0334

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Michael R Clarkson

Program Officer
The AFOSR Program Officer currently assigned to the award

Tristan Nguyen

Reporting Period Start Date

09/01/2014

Reporting Period End Date

03/29/2018

Abstract

Our research in this grant contributed to the science of security. We developed a verification methodology for a specific hyperproperty, and we provided a powerful new security mechanism for mobile devices, as well as other GUI-based, security-sensitive systems. We also made progress on a verification methodology that works for all hyperproperties expressible in HyperLTL, and on establishing the trustworthiness of that methodology.

Distribution Statement
This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement
If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

sf298.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

report.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

1. Quantification of Integrity. Mathematical Structures in Computer Science, 25(2):207-258, 2015. Michael R. Clarkson, Fred B. Schneider.

2. Checking Interaction-Based Declassification Policies for Android Using Symbolic Execution. In Proc. European Symposium on Research in Computer Security, pages 520-538, September 2015.

New discoveries, inventions, or patent disclosures:

Do you have any discoveries, inventions, or patent disclosures to report for this period?

No

Please describe and include any notable dates

Do you plan to pursue a claim for personal or organizational intellectual property?

Changes in research objectives (if any):

Change in AFOSR Program Officer, if any:

Extensions granted or milestones slipped, if any:

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Jun 28, 2018 14:39:44 Success: Email Sent to: mrc26@cornell.edu