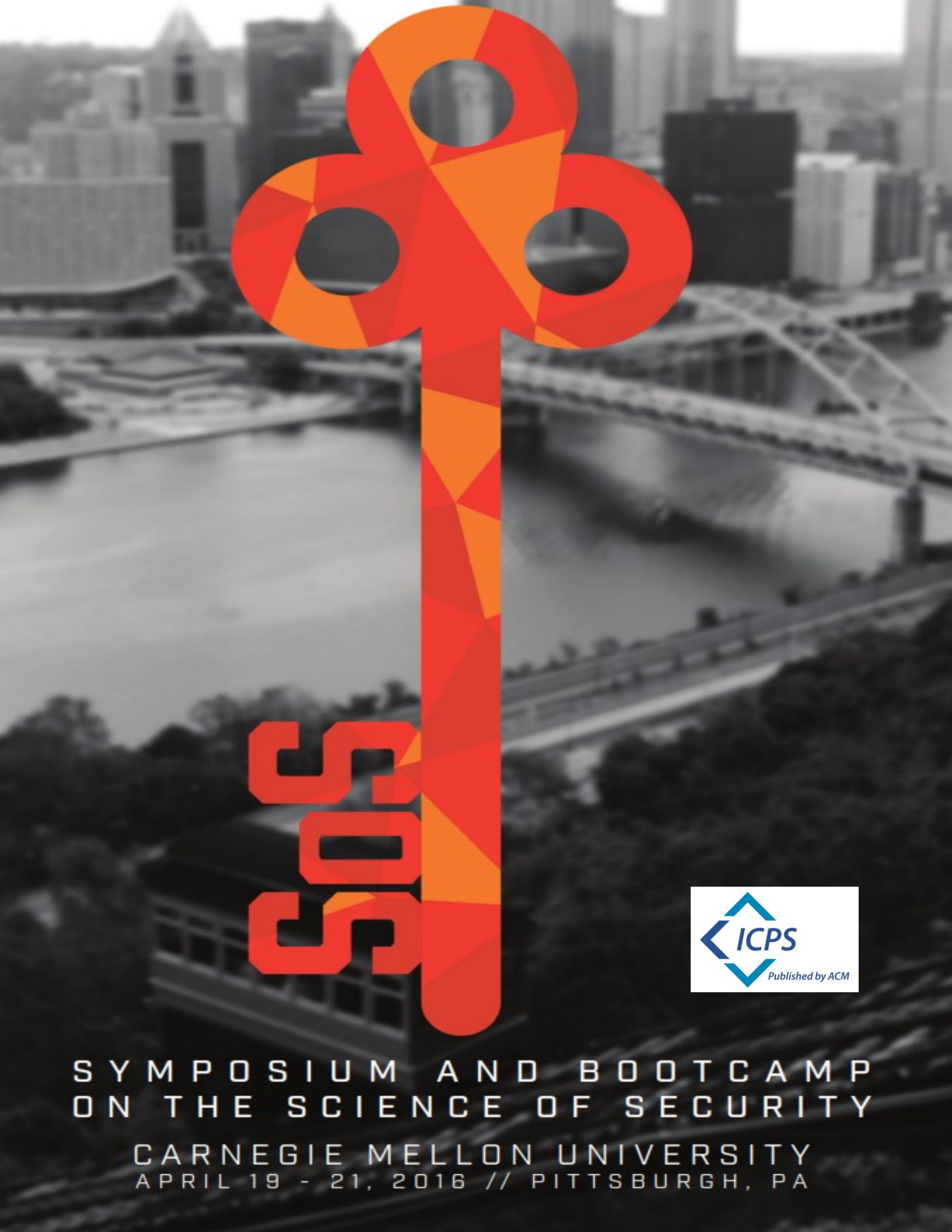


ICPS
Published by ACM

SYMPOSIUM AND BOOTCAMP ON THE SCIENCE OF SECURITY

CARNEGIE MELLON UNIVERSITY
APRIL 19 - 21, 2016 // PITTSBURGH, PA

Preface

Science of Security (SoS) emphasizes the advancement of research methods as well as the development of new research results. This dual focus is intended to improve both the confidence we gain from scientific results and also the capacity and efficiency through which we address increasingly challenging technical problems.

The HotSoS conferences have focused on work related to one or more of the five Hard Problems identified by the Science of Security community:

- Scalability and composability in the construction of secure systems
- Policy-governed collaboration in handling data across different domains of authority for security and privacy protection
- Predictive security metrics to guide choice-making in security engineering and response
- Resilient architectures that can deliver service despite compromised components
- Human behavior, modeling users, operators, and adversaries to support improved design and analysis

A second and equally major focus of the conferences is on the advancement of scientific methods, including data gathering and analysis, experimental methods, and mathematical models for modeling and reasoning. This includes the exploration of interactions among these methods to enhance validity.

The HotSoS conferences bring together senior and junior researchers from diverse disciplines to promote advancement of work related to the science of security. The conference includes a mix of invited talks, tutorials, refereed papers, and poster presentations.

Submissions were subject to a rigorous reviewing process. Each submission received an average of more than three reviews. Just over half of submitted papers were accepted for the conference. This proceedings volume includes accepted papers and summaries of posters and tutorials. The conference is held at Carnegie Mellon University in Pittsburgh, April 19 – 21, 2016.

We appreciate the hard work of the program committee and the outside reviewers. We appreciate the support of the National Security Agency, the National Science Foundation, and the Army Research Office. Without the EasyChair infrastructure the job of the conference organizers would be much more difficult. We appreciate the assistance of our colleagues Jonathan Aldrich and Travis Breaux. And we particularly appreciate the support of the Carnegie Mellon staff team, including particularly Monika DeReno, Sharon Blazevich, Bernadette Dayak, Tom Pope, and Josh Quicksall, who have helped transform a set of technical papers into an engaging conference experience for all attendees.

William L. Scherlis
(General Chair and PC co-Chair)
David Brumley
(PC co-Chair)

April 2016
Pittsburgh, PA

Table of Contents

Poster: Abstract Runtime Structure for Reasoning about Security 1
Marwan Abi-Antoun, Ebrahim Khalaj, Radu Vanciu and Ahmad Moghimi

Poster: Efficient solving of string constraints for security analysis 4
Clark Barrett, Cesare Tinelli, Morgan Deters, Tianyi Liang, Andrew Reynolds and Nestan Tsiskaridze

Intrusion Detection in Enterprise Systems by Combining and Clustering Diverse Monitor Data 7
Atul Bohara, Uttam Thakore and William Sanders

Security is about Control: Insights from Cybernetics 17
Kevin Bush, Antonio Roque and Christopher Degni

Poster: Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment Framework 25
Susan Campbell, Lelyn Saner and Michael Bunting

A Framework for Generation, Replay and Analysis of Real-World Attack Variants 28
Phuong Cao, Eric Badger, Zbigniew Kalbarczyk and Ravishankar Iyer

Establishing a Baseline for Measuring Advancement in the Science of Security – an Analysis of the 2015 IEEE Security & Privacy Proceedings . 38
Jeffrey Carver, Morgan Burcham, Sedef Akinli Kocak, Ayse Bener, Michael Felderer, Matthias Gander, Jason King, Jouni Markkula, Markku Oivo, Clemens Sauerwein and Laurie Williams

Tutorial: Systematic Analysis of Qualitative Data in Security 52
Hanan Hibshi

Controller Synthesis for Linear Time-varying Systems with Adversaries . . 53
Zhenqi Huang, Yu Wang, Sayan Mitra and Geir Dullerud

Poster: Expressing and Reasoning about Conflicting Norms in Cybersecurity 63
Jiaming Jiang, Nirav Ajmeri, Rada Chirkova, Jon Doyle and Munindar Singh

Poster: Toward a Normative Approach for Forensicability: Extended Abstract 65
Ozgur Kafali, Munindar P. Singh and Laurie Williams

Poster: Modules in Wyvern: Advanced Control over Security and Privacy 68
Darya Kurilova, Alex Potanin and Jonathan Aldrich

Poster: A Model-based Approach to Anomaly Detection in Software Architectures 69
Hemank Lamba, Thomas Glazier, Bradley Schmerl, Javier Camara, David Garlan and Juergen Pfeffer

Optimal Thresholds for Intrusion Detection Systems 72
Aron Laszka, Waseem Abbas, Shankar Sastry, Yevgeniy Vorobeychik and Xenofon Koutsoukos

Safety-critical Cyber-physical Attacks: Analysis, Detection, and Mitigation 82
Hui Lin, Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk and Ravishankar Iyer

Poster: Decentralization and Security in Dynamic Traffic Light Control . . 90
Jian Lou and Yevgeniy Vorobeychik

Poster: Visualizing the variational callgraph of the Linux Kernel: An approach for reasoning about dependencies 93
Momin Malik, Jürgen Pfeffer, Gabriel Ferreira and Christian Kästner

Differences in Trust between Human and Automated Decision Aids 95
Carl Pearson, Allaire Welk, Dr. William Boettcher, Dr. Roger Mayer, Sean Streck, Dr. Joseph Simons-Rudolph and Dr. Christopher Mayhorn

Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment 99
Bradley Potteiger, Goncalo Martins and Xenofon Koutsoukos

Poster: Security Practices in DevOps 109
Akond Rahman and Laurie Williams

Operation-Level Traffic Analyzer Framework for Smart Grid 112
Wenyu Ren, Klara Nahrstedt and Tim Yardley

Poster: Raindroid – A System for Run-time Mitigation of Android Intent Vulnerabilities 115
Bradley Schmerl, Jeff Gennari, Javier Cámara Moreno and David Garlan

Poster: Modeling, Analyzing, and Consistency Checking Privacy Requirements using Eddy 118
Daniel Smullen and Travis Breaux

Poster: Risk-Based Attack Surface Approximation 121
Christopher Theisen and Laurie Williams

Tutorial: Text Analytics for Security 124
Tao Xie and William Enck

Poster: The Persuasive Phish: Examining the Social Psychological Principles Hidden in Phishing Emails 126
Olga Zielinska, Allaire Welk, Christopher Mayhorn and Emerson Murphy-Hill

Program Committee

Marwan Abi-Antoun	Wayne State University
Alessandro Acquisti	Carnegie Mellon University
Jonathan Aldrich	Carnegie Mellon University
Michael Bailey	University of Illinois at Urbana-Champaign
Lujo Bauer	Carnegie Mellon University
Travis Breaux	Carnegie Mellon University
David Brumley	Carnegie Mellon University
Kathleen Carley	Carnegie Mellon University
Michel Cukier	University of Maryland
Serge Egelman	UC Berkeley
David Garlan	Carnegie Mellon University
Limin Jia	Carnegie Mellon University
Jonathan Katz	University of Maryland
Stuart Krohn	NSA
Michael Maass	Carnegie Mellon University
Sam Malek	University of California at Irvine
David Malcolm Nicol	University of Illinois at Urbana-Champaign
Andre Platzer	Carnegie Mellon University
William Sanders	University of Illinois
William Scherlis	Carnegie Mellon University
Munindar Singh	NCSU
Witawas Srisa-An	University of Nebraska-Lincoln
Joshua Sunshine	Carnegie Mellon University
Adam Tagert	National Security Agency

Additional Reviewers

Atul Bohara
Carmen Cheh
Hongying Du
Fawazt Ahmed
Joshua Garcia
Ozgur Kafali
João G. Martins
Uttam Zawadzki
Erik Thakore

Author Index

Abbas, Waseem 72
Abi-Antoun, Marwan 1
Ajmeri, Nirav 63
Akinli Kocak, Sedef 38
Aldrich, Jonathan 68
Alemzadeh, Homa 82

Badger, Eric 28
Barrett, Clark 4
Bener, Ayse 38
Boettcher, Dr. William 95
Bohara, Atul 7
Breaux, Travis 118
Bunting, Michael 25
Burcham, Morgan 38
Bush, Kevin 17

Camara, Javier 69
Campbell, Susan 25
Cao, Phuong 28
Carver, Jeffrey 38
Chen, Daniel 82
Chirkova, Rada 63
Cámara Moreno, Javier 115

Degni, Christopher 17
Deters, Morgan 4
Doyle, Jon 63
Dullerud, Geir 53

Enck, William 124

Felderer, Michael 38
Ferreira, Gabriel 93

Gander, Matthias 38
Garlan, David 69, 115
Gennari, Jeff 115
Glazier, Thomas 69

Hibshi, Hanan 52
Huang, Zhenqi 53

Iyer, Ravishankar 28, 82

Jiang, Jiaming 63

Kafali, Ozgur 65
Kalbarczyk, Zbigniew 28, 82
Khalaj, Ebrahim 1
King, Jason 38
Koutsoukos, Xenofon 72, 99
Kurilova, Darya 68
Kästner, Christian 93

Lamba, Hemank 69
Laszka, Aron 72
Liang, Tianyi 4
Lin, Hui 82
Lou, Jian 90

Malik, Momin 93
Markkula, Jouni 38
Martins, Goncalo 99
Mayer, Dr. Roger 95
Mayhorn, Christopher 126
Mayhorn, Dr. Christopher 95
Mitra, Sayan 53
Moghimi, Ahmad 1
Murphy-Hill, Emerson 126

Nahrstedt, Klara 112

Oivo, Markku 38

Pearson, Carl 95
Pfeffer, Juergen 69
Pfeffer, Jürgen 93
Potanin, Alex 68
Potteiger, Bradley 99

Rahman, Akond 109
Ren, Wenyu 112
Reynolds, Andrew 4
Roque, Antonio 17

Sanders, William 7
Saner, Lelyn 25
Sastry, Shankar 72
Sauerwein, Clemens 38
Schmerl, Bradley 69, 115
Simons-Rudolph, Dr. Joseph 95

Singh, Munindar 63
Singh, Munindar P. 65
Smullen, Daniel 118
Streck, Sean 95

Thakore, Uttam 7
Theisen, Christopher 121
Tinelli, Cesare 4
Tsiskaridze, Nestan 4

Vanciu, Radu 1
Vorobeychik, Yevgeniy 72, 90

Wang, Yu 53
Welk, Allaire 95, 126
Williams, Laurie 38, 65, 109, 121

Xie, Tao 124

Yardley, Tim 112

Zielinska, Olga 126

Keyword Index

ifdef 93

anomaly detection 7, 69
aptitude testing 25
architectural risk analysis 1
attack replay 28
attack surface 121
attack variants 28
automation 95

baseline 38

callgraph 93
capabilities 68
clustering 7
computational complexity 72
configuration complexity 93
constraint-based synthesis 53
control systems 17
controller synthesis 53
crash dumps 121
cyber-physical security 53
cyber-physical systems 82, 99
cybernetics 17
cybersecurity 126
cybersecurity workforce 25

data flow tracing 118
data practices 118
decentralization and security 90
decision-making 95
description logic 118
devops 109
dominance relation 63

economics of security 72
Eddy 118
emails 126
extract-abstract-check 1

forensic logging 65

game theoretical model 90
game theory 72

grounded analysis 52

intrusion detection 7
intrusion detection system 72

job analysis 25

Linux kernel 93
literature review 38

machine learning 7
metrics 121
mobile security 124
model-based graph clustering 69
module system 68
monitoring 7

network security 112
norm 63
normative system 63

ontology 118
outlier detection 69

persuasion 126
phishing 126
power grids 82
privacy 68
privacy requirements 118

qualitative research 52
quantitative risk assessment 99

reliance 95
reproducible security experiments 28
requirements 65
requirements specification 118
risk 95
runtime architecture 1

science of security 38
security 7, 17, 65, 68, 109, 115, 121, 124
security analysis 4, 52
security requirements 124
selection 25
self-adaptation 115
simulation-based method 90
Smart Grid 112

SMT 4
social norms 65
sociotechnical systems 65
software architecture 69, 115
software practices 109
stack traces 121
Stackelberg equilibrium 72
strain 95
string constraints 4
surgical robot 82

task analysis 25
text analytics 124
threat modeling 99
traffic analysis 112
Traffic Control System 90
trust 95

visualization 93
vulnerabilities 93

workload 95

Systematic Analysis of Qualitative Data in Security

Hanan Hibshi
Institute for Software Research
Carnegie Mellon University
Pittsburgh, USA
hhibshi@cs.cmu.edu

ABSTRACT

This tutorial will introduce participants to Grounded Theory, which is a qualitative framework to discover new theory from an empirical analysis of data. This form of analysis is particularly useful when analyzing text, audio or video artifacts that lack structure, but contain rich descriptions. We will frame Grounded Theory in the context of qualitative methods and case studies, which complement quantitative methods, such as controlled experiments and simulations. We will contrast the approaches developed by Glaser and Strauss, and introduce coding theory - the most prominent qualitative method for performing analysis to discover Grounded Theory. Topics include coding frames, first- and second-cycle coding, and saturation. We will use examples from security interview scripts to teach participants: developing a coding frame, coding a source document to discover relationships in the data, developing heuristics to resolve ambiguities between codes, and performing second-cycle coding to discover relationships within categories. Then, participants will learn how to discover theory from coded data. Participants will further learn about inter-rater reliability statistics, including Cohen's and Fleiss' Kappa, Krippendorf's Alpha, and Vanbelle's Index. Finally, we will review how to present Grounded Theory results in publications, including how to describe the methodology, report observations, and describe threats to validity.

Keywords

Grounded theory; qualitative; security analysis

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

WOODSTOCK '97 El Paso, Texas USA

© 2016 ACM. ISBN 123-4567-24-567/08/06…$15.00

DOI: http://dex.doi.org/10.1145/2898375.2898387

Modules in Wyvern: Advanced Control over Security and Privacy

[Poster Abstract]

Darya Kurilova
Carnegie Mellon University
darya@cs.cmu.edu

Alex Potanin
Victoria University of Wellington
alex@ecs.vuw.ac.nz

Jonathan Aldrich
Carnegie Mellon University
aldrich@cs.cmu.edu

ABSTRACT

In today's systems, restricting the authority of untrusted code is difficult because, by default, code has the same authority as the user running it. Object capabilities are a promising way to implement the principle of least authority, but being too low-level and fine-grained, take away many conveniences provided by module systems. We present a module system design that is capability-safe, yet preserves most of the convenience of conventional module systems. We demonstrate how to ensure key security and privacy properties of a program as a mode of use of our module system. Our authority safety result formally captures the role of mutable state in capability-based systems and uses a novel non-transitive notion of authority, which allows us to reason about authority restriction: the encapsulation of a stronger capability inside a weaker one.

Keywords

Language-based security; capabilities; modules; authority

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

HotSoS '16 April 19-21, 2016, Pittsburgh, PA, USA

© 2016 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-4277-3/16/04…$15.00

DOI: http://dx.doi.org/10.1145/2898375.2898376