SSCA Virtual Forum

March 2, 2022

Program Agenda

11:00 Opening Remarks

11:05 Session One: ***Composable Security: The Challenge of Security Models That Can Span from the Silicon to Software & Systems***

Speaker:
Dr. Jeremy Bellay, is a principal investigator in Battelle's Cyber Trust and Analytics Division

Abstract:
Cybersecurity, by its nature, is a complex and continuously evolving field. Recently, understanding of the supply chain's role in security has received new emphasis due to the high-profile Solar Winds attack, and the increasing movement of state-of-the-art silicon manufacturing off American shores. This raises the question of how we integrate security models used at the factory or by the supplier with security assessment estimates that are required later in the lifecycle and at the system level. In this talk we review the resources currently available to describe cyber vulnerabilities and weaknesses in hardware, software, and systems. We then look at what is required to characterize vulnerabilities in hardware and software components, compound components, and systems. Finally we describe how this infrastructure could support the goal of security models that are composable and meaningful across the abstractions and contexts of real systems.

11:50 **Break**

11:55 Session Two: ***A New Doctrine for Hardware Security***

Speaker:
Dr. Simha Sethumadhavan, Professor at Columbia University and
Adam Hastings, PhD Candidate, Computer Science at Columbia University

Abstract:
Recent woes in hardware security are not only because of a lack of convincing technical solutions but also because market forces and incentives prevent those with the ability to fix problems from doing so. At the root of the problem is the fact that hardware security comes at a cost; Present issues in hardware security can be seen as the result of the players in the game of hardware security finding ways of avoiding

paying this cost. We formulate this idea into a doctrine of security, namely the Doctrine of Shared Burdens and analyze three case studies---Rowhammer, Spectre, and Meltdown---through the lens of this doctrine.

Following this we discuss a novel approach to incentivize vendors to include security in their products. Our approach, called open mandates, mandates that all vendors must dedicate some amount of resources (e.g. system speed, energy, design cost, etc.) towards security. Unlike the current state-of-the-art, "checklist security", open mandates do not prescribe specific controls that must be implemented. The goal of open mandates is to provide flexibility to vendors in implementing security controls that they see fit while requiring all vendors to commit to a certain level of security.

We quantitatively demonstrate that such open mandates can lead to measurable improvements, and then describe how open Mandates can be enforced with a case study on hardware support for software security. We will describe our prototype system (The proto-COMMAND system) and demonstrate its deployability.

11:40 Session Three: ***NIST Update on Recent C-SCRM-Related Work***

Speakers:
Angela Smith and Jon Boyens, NIST

11:55: ***Closing Remarks***

Brief Speaker Bios

Dr. Jeremy Bellay is a principal investigator in Battelle's Cyber Trust and Analytics division. He specializes in problems that require the synthesis of complex knowledge structures with sophisticated data driven approaches. Jeremy is particularly interested in an integrative approach to risk and assurance in cyber systems. He led the TAME Forum working group on Hardware Assurance, Weaknesses, Collaboration and Sharing, and is an active participant in the SAE G32 Hardware Assurance effort.

Adam Hastings is a fourth-year PhD student in Computer Science at Columbia University advised by Prof. Simha Sethumadhavan. Adam's research interests focus on hardware security and mechanism design. Prior to joining Columbia, Adam received an MS in Electrical & Computer Engineering and a BS in Computer Engineering, both from Brigham Young University. Outside of research, Adam enjoys climbing mountains and making music. https://www.cs.columbia.edu/~hastings/; https://www.linkedin.com/in/a-hastings/

Dr. Simha Sethumadhavan is a Professor of Computer Science at Columbia University, and founder of Chip Scan Inc., a hardware security company. Simha's research work at Columbia is focused on finding practical solutions to problems in the area of cybersecurity and computer architecture. He is a recipient of an Alfred P. Sloan Research Fellowship and the

NSF CAREER award. His work has received nine best paper awards for his work on computer security and computer architecture, and his team has successfully taped out three novel computing chips on shoestring budgets. Further his team's work on identifying security vulnerabilities and formulating security defenses have resulted in fixes to major products such as processors and web browsers used by millions of users, and his work on hardware security is actively considered by standards organizations. He has served on the Federal Communications Commission Downloadable Security Technical Advisory Committee. He founded Chip Scan Inc. to transition technology developed at Columbia and the company has products that find and mitigate hardware backdoors, and hardware solutions built on Zero Trust principles. Simha obtained his PhD from UT Austin in 2007. He tweets at @TheSimha, is also on Linkedin is: https://www.linkedin.com/in/simha/. Research papers can be found here: https://www.cs.columbia.edu/~simha