Draper Cyber Research Interests

University Programs Point of Contact
Dr. Brenan McCarragher, CTO
617.692.0932
education@draper.com

Technical Point of Contact
Silviu Chiricescu
617.831 3883
silviu@draper.com

Introduction

Cyber-physical systems security is one of Draper's core capabilities. Draper's intimate knowledge of cyber vulnerabilities is used to inform design decision to holistically protect the entire compute stack. Draper's approach is comprehensive and relies on research from formal methods, system security, advance packaging, secure processors, and offensive cyber security.

About Draper Laboratory (www.draper.com)

Draper is an independent, not-for-profit corporation, chartered to work on problems in the national interest. Draper is seeking collaborative research partners from universities to further the state of the art in key technologies of mutual interest. Research Whitepapers describing Draper's technology interests and Technical Points of Contact can be found on the Draper Scholars webpage (Draper Scholar Program | Draper). The Draper Scholars Program funds thesis-bearing MS and PhD students at partner universities as one of the effective ways to progress the technology. Other means of collaborative research (e.g. joint proposals, sabbaticals, etc.) are also encouraged. Please contact education@draper.com if you have further questions.

Research Interests

Draper cyber-physical system security spans three broad, complimentary domains that use deep understanding of the hardware-software interface to develop solutions for some of our nation's premier, strategically important systems.

1. Computer system security

This research area covers security mechanisms, along with the associated compositional aspects, to protect the entire compute stack. We are dealing with strong, nation state adversaries, and our solutions must withstand the most sophisticated attacks. Thus, Draper is interested in collaborations the span a wide range of topics including:

- Secure processor design that includes methods to (formally) verify the (generated) hardware and its security properties (i.e., lack of side channel leakage, integrity and confidentiality of the computation, and reverse engineering and FI protections, etc.)
- Secure software stack design that includes secure operating systems and languages, property-based fuzzing, compiler transformations to enforce security policies, etc.

2. Formal methods

Draper applies a wide range of formal methods to understand and then modify programs (in source code or binary form). Our analyses include static, dynamic, and hybrid approaches. We are interested not only in scaling and extending existing approaches, but also creating languages and tool interfaces to make these analyses useful for others. Research topics of interest include:

- Specification composition/synthesis, proof automation (i.e., in Coq, Agda, etc.), counterexample guided inductive synthesis

- Secure compilation, sounds decomplilation, weakest precondition analysis, abduction inference, abstract interpretation
- Mathematical topics (e.g., type theory, homotopy, category theory, program logics), hyperproperties, datalog/e-graphs.

3. ***Offensive cyber security***

   This research domain covers a broad area of offensive techniques at both the hardware and software layers. Specific areas of collaboration include:

   - Compiler-based techniques including automatic generation of exploits based on X-oriented programming, transformations to increase diversity and obfuscation (i.e., static and dynamic opaque predicates, etc.), taint analysis, control follow analysis, etc.
   - Operating systems exploitation including via process injection, packer techniques, networking stack, etc.
   - Analog-based attacks (i.e., RF, acoustic, power, etc.) and physical attacks

We would be targeting PhD students for the development of novel approaches; and MS students for the application of existing approaches to specific problems of interest to Draper.