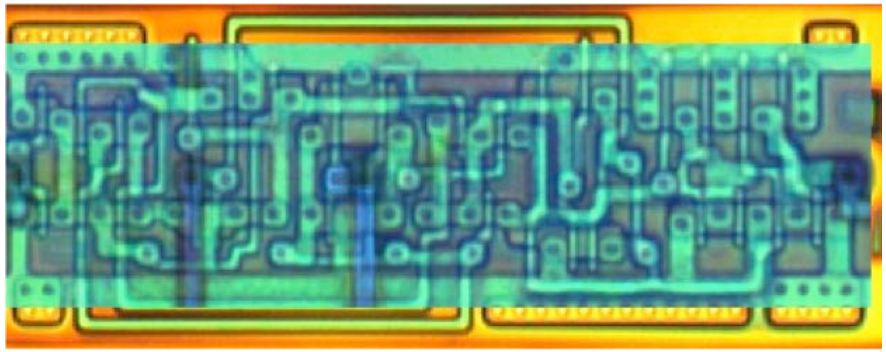

Our research group seeks to create systems that can be trusted even in the presence of malicious attackers and that empower individuals to control how their data are used. This involves many traditional areas, including security, software engineering, programming languages, cryptography, and networking. We are particularly interested in approaches that apply cryptography and diversity to provide security and privacy.

Security Research Group

www.jeffersonswheel.org

David Evans
Associate Professor
evans@virginia.edu
www.cs.virginia.edu/evans/

Department of Computer Science
University of Virginia
Charlottesville, VA

"Strengthening computer security and privacy while expanding the pool of the next generation of computer scientists through engaging classroom and research experiences."

UNIVERSITY of VIRGINIA
ENGINEERING

Privacy-Preserving Applications

The goal of secure computation is to enable two (or more) parties to perform a computation together without revealing their data. For example, we can use secure computation to enable a patient to compare their genome to genomes in a medical study, without revealing any actual private data, or to allow to people to find out any shared contacts they have without revealing anything about their other contacts. Although the theory behind secure multi-party computation goes back nearly three decades, deployed systems are rare due to both the implementation difficulty and heavy performance overhead. Our work seeks to improve our understanding of secure computation and to develop tools for making secure computation practical. We have developed techniques that improve the performance of the state-of-the-art privacy-preserving biometric protocols by more than a factor of 20, as well as that demonstrate that generic protocols can have performance comparable to the best custom protocols for private set intersection. We have also developed a general framework for secure computation using garbled circuits that we have used to build many applications, including private encryption and genome alignment.

Mobile and Web Security

Modern web applications and mobile devices raise a host of new privacy and security concerns. Our group explores methods for solving these problems drawing on techniques from programming languages, cryptography, and software engineering. The frequent and highly dynamic client-server communication that is characteristic of modern web applications leaves them vulnerable to side-channel leaks where an adversary can learn about the state of the application and visitor's choices, even over encrypted connections. We have developed a black-box tool for detecting side-channel vulnerabilities by analyzing network traffic over repeated crawls of a web application. Our tool quantifies the severity of side-channel leaks in a web application, and gives web application developers a measure of the risk of information leakage against different types of adversaries.

RECENT RESEARCH DEVELOPMENTS

- Developed a new framework for secure computation
- Protect private web content from embedded scripts
- Web application security framework

RECENT GRANTS

- NSF-Implementable Privacy and Security for Resource-Constrained Devices
- AFOSR/MURI-Hardware, Languages, and Architecture for Defense Against Hostile Operating Systems
- AFOSR-Designing for Measurable Security
- NSF-Practical Secure Two-Party Computation
- Google-Secure Multi-Party Computation on Smartphones

SEAS Research Information
Pamela M. Norris, Associate Dean
University of Virginia
Box 400242
Charlottesville, VA 22903
pamela@virginia.edu
434.243.7683

UNIVERSITY of VIRGINIA ENGINEERING