SaTC: TTP: Medium: Collaborative: Deployment-quality and Accessible Solutions for Cryptography Code Development

Submitted by Barton Miller on Mon, 07/06/2020 - 12:12pm

Project Details

Lead PI

Barton Miller

Performance Period

Oct 01, 2019 - Sep 20, 2023

Institution(s)

University of Wisconsin-Madison

Sponsor(s)

National Science Foundation

Award Number

1929739

Ranked 562 out of 2290 Group Projects.
103 related hits.

Vulnerabilities in cryptographic implementations seriously reduce the security guarantees of algorithms in practice and lead to attacks. An effective fix to the vulnerable code problem is automatic code checking. However, existing code verification tools cannot adequately cover cryptographic properties due to deficiencies in both accuracy, in terms of missed detection and false alarms, and scalability, in terms of complexity and runtime. The technology in this transition-to-practice project is to help secure cryptographic implementations, which are the foundation of many advanced systems. By making relevant research solutions deployment-grade, this effort can substantially improve the cryptographic coding practice and benefit software developers in all professions.

The project's objective is to transition multiple secure cryptographic coding research solutions to practice and make it convenient and accessible to automatically screen programs against a wide range of cryptographic implementation vulnerabilities or misuses. The main technical enabler is a high precision and high throughput approach based on specialized program analysis techniques called CryptoGuard. CryptoGuard can detect a wide range of cryptographic misuses with ultra-low false alarm rates when used on complex and large-scale Java programs. The project leverages multiple popular software development and software security platforms, including the Software Assurance Marketplace, to make these tools effective in production environments. The systematic benchmark and measurement work is designed to advance the science of security and substantially raises the standard and quality of cryptographic code screening.

Barton Miller

Related Artifacts

No related artifacts found.

TTP Medium Collaborative Division of Computer and Network Systems (CNS)