Notice and Invitation
Oral Defense of Master's Thesis
The Volgenau School of Engineering, George Mason University

Matthew Ryan Carter
Bachelor of Science, University of Virginia

Enabling a Control System Approach to Side-Channel and Fault Attacks

Wednesday, December 5, 2018, 3:00pm
Engineering Building, Room 3507
All are invited to attend.

Committee
Dr. Jens-Peter Kaps, Thesis Director
Dr. Kris Gaj
Dr. Craig Lorie

Abstract

As the number of embedded devices continues to grow, attacks that require physical access to the device become more plausible. Two sub-classifications of these attacks, Side-Channel Attacks (SCA) and Fault attacks, necessitate the attacker to be familiar with the target implementation. Side-Channel Attacks exploit information leaked by the target device to discover secret cryptographic keys. Fault attacks act upon the system to induce error in device operation that may result in information leakage or improper execution. The error produced by the attack is dependent on the method used to inject the fault. This paper discusses some of the advances in SCAs and Fault Attacks and proposes a control system approach to these classes of attacks. The result of the research is a System on a Chip (SOC) for measuring power consumption, analyzing results, and refining measurement as a feedback loop.