University of Victoria | Graduate Studies

Notice of the Final Oral Examination for the Degree of Doctor of Philosophy

of

SAMER MOEIN

MSc (Kuwait University, 2004)
BSc (Kuwait University, 2011)

“Systematic Analysis and Methodologies for Hardware Security”

Department of Electrical and Computer Engineering

Friday, December 4, 2015
1:00 P.M.
Engineering and Computer Science Building
Room 468

Supervisory Committee:
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, University of Victoria (Co-Supervisor)
Dr. T. Aaron Gulliver, Department of Electrical and Computer Engineering, UVic (Co-Supervisor)
Dr. Alex Thomo, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Ahmed E. Kamal, Department of Electrical and Computer Engineering, Iowa State University

Chair of Oral Examination:
Dr. Lincoln Shlensky, Department of English, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

With the increase in globalization of Integrated Circuit (IC) design and production, hardware trojans have become a serious threat to manufacturers as well as consumers. These trojans could be intensionally or accidentally embedded in ICs to make a system vulnerable to hardware attacks. The implementation of critical applications using ICs makes the effect of trojans an even more serious problem. Moreover, the presence of untrusted foundries and designs cannot be eliminated since the need for ICs is growing exponentially and the use of third party software tools to design the circuits is now common. In addition if a trusted foundry for fabrication has to be developed, it involves a huge investment. Therefore, hardware trojan detection techniques are essential. Very Large Scale Integration (VLSI) system designers must now consider the security of a system against internal and external hardware attacks. Many hardware attacks rely on system vulnerabilities. Moreover, an attacker may rely on deprocessing and reverse engineering to study the internal structure of a system to reveal the system functionality in order to steal secret keys or copy the system. Thus hardware security is a major challenge for the hardware industry. Many hardware attack mitigation techniques have been proposed to help system designers build secure systems that can resist hardware attacks during the design stage, while others protect the system against attacks during operation.

In this dissertation, the idea of quantifying hardware attacks, hardware trojans, and hardware trojan detection techniques is introduced. We analyze and classify hardware attacks into risk levels based on three dimensions Accessibility/Resources/Time ART). We propose a methodology and algorithms to aid the attacker/defender to select/predict the hardware attacks that could use/threaten the system based on the attacker/defender capabilities. Because many of these attacks depends on hardware trojans embedded in the system, we propose a comprehensive hardware trojan classification based on hardware trojan attributes divided into eight categories. An adjacency matrix is generated based on the internal relationship between the attributes within a category and external relationship between attributes in different categories. We propose a methodology to generate a trojan life-cycle based on attributes determined by an attacker/defender to build/investigate a trojan. Trojan identification and severity are studied to provide a systematic way to compare trojans. Trojan detection identification and coverage is also studied to provide a systematic way to compare detection techniques and measure their effectiveness related to trojan severity. We classify hardware attack mitigation techniques based on the hardware attack risk levels. Finally, we match these techniques to the attacks the could countermeasure to help defenders select appropriate techniques to protect their systems against potential hardware attacks.