Home > ETDS > THESES > 1054

Masters Theses 1896 - February 2014

Off-campus UMass Amherst users: To download campus access theses, please use the following link to log into our proxy server with your UMass Amherst user name and password.

Non-UMass Amherst users: Please talk to your librarian about requesting this thesis through interlibrary loan.

Theses that have an embargo placed on them will not be available to anyone until the embargo expires.

Protecting Network Processors with High Performance Logic Based Monitors

Download

SHARE

Harikrishnan Kumarapillai Chandrikakutty, University of Massachusetts - Amherst

Follow

Document Type
Open Access

Degree Program
Electrical & Computer Engineering

Degree Type
Master of Science (M.S.)

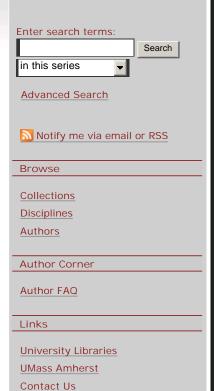**Year Degree Awarded**
2013

Month Degree Awarded
May

Keywords
Network Processors, Security Monitors, Hardware, Programmable, DE4 NetFPGA, Determinitic Finite Automaton

Abstract
Technological advancements have transformed the way people interact with the world. The Internet now forms a critical infrastructure that links different aspects of our life like personal communication, business transactions, social networking, and advertising. In order to cater to this ever increasing communication overhead there has been a fundamental shift in the network infrastructure. Modern network routers often employ software programmable network processors instead of ASIC-based technology for higher throughput performance and adaptability to changing resource requirements. This programmability makes networking infrastructure vulnerable to new class of network attacks by compromising the software on network processors. This issue has resulted in the need for security systems which can monitor the behavior of network processors at run time. This thesis describes an FPGA-based security

Notify me via email or RSS

Browse

Collections

Disciplines

Authors

Author Corner

Author FAQ

Links

University Libraries

UMass Amherst

Contact Us

monitoring system for multi-core network processors. The implemented security monitor improves upon previous hardware monitoring schemes. We demonstrate a state machine based hardware programmable monitor which can track program execution flow at run time. Applications are analyzed offline and a hash of the instructions is generated to form a state machine sequence. If the state machine deviates from expected behavior, an error flag is raised, forcing a network processor reset. For testing purposes, the monitoring logic along with the multi-core network processor system is implemented in FPGA logic. In this research, we modify the network processor memory architecture to improve security monitor functionality. The efficiency of this approach is validated using a diverse set of network benchmarks. Experiments are performed on the prototype system using known network attacks to test the performance of the monitoring subsystem. Experimental results demonstrate that out security monitor approach provides an efficient monitoring system in detecting and recovering from network attacks with minimum overhead while maintaining line rate packet forwarding. Additionally, our monitor is capable of defending against attacks on processor with a Harvard architecture, the dominant contemporary network processor organization. We demonstrate that our monitor architecture provides no network slowdown in the absence of an attack and provides the capability to drop packets without otherwise affecting regular network traffic when an attack occurs.

Advisor(s) or Committee Chair
Tessier, Russell G