

Platform Agnostic, Scalable, and Unobtrusive FPGA Network Processor Design of Moving Target Defense over IPv6 (MT6D) over IEEE 802.3 Ethernet

Joseph Sagisi, Joseph Tront, and Randy Marchany
Bradley Department of Electrical Engineering and Computer Engineering
Virginia Tech Blacksburg, USA
Email: {jsagisi, jgtront, marchany}@vt.edu

Abstract—This work presents the proof of concept implementation for the first hardware-based design of Moving Target Defense over IPv6 (MT6D) in full Register Transfer Level (RTL) logic, with future sights on an embedded Application-Specified Integrated Circuit (ASIC) implementation. Contributions are an IEEE 802.3 Ethernet stream-based in-line network packet processor with a specialized Complex Instruction Set Computer (CISC) instruction set architecture, RTL-based Network Time Protocol v4 synchronization, and a modular crypto engine. Traditional static network addressing allows attackers the incredible advantage of taking time to plan and execute attacks against a network. To counter, MT6D provides a network host obfuscation technique that offers network-based keyed access to specific hosts without altering existing network infrastructure and is an excellent technique for protecting the Internet of Things, IPv6 over Low Power Wireless Personal Area Networks, and high value globally routable IPv6 interfaces. This is done by cryptographically altering IPv6 network addresses every few seconds in a synchronous manner at all endpoints. A border gateway device can be used to intercept select packets to unobtrusively perform this action. Software driven implementations have posed many challenges, namely, constant code maintenance to remain compliant with all library and kernel dependencies, the need for a host computing platform, and less than optimal throughput. This work seeks to overcome these challenges in a lightweight system to be developed for practical wide deployment.

Index Terms—IPv6, Moving Target Defense, Network Processor, FPGA.