A Testbed for Reconfigurable Network Security Research and Experimentation_

Final Report

SUBMITTED TO

Air Force Office of Scientific Research
875 North Randolph Street
Suite 325, Room 3112
Arlington, VA 22203
Point of Contact: Dr. Robert L. Herklotz email- robert.herklotz@afosr.af.mil
(703) 696-6565 fax (703) 696-8450

Grant Number: FA9550-06-1-0249

Principle Investigator: Douglas H. Summerville
Co-Principle Investigator: Yu Chen

Research Foundation of SUNY
Binghamton University
Department of Electrical and Computer Engineering
Po Box 6000
Binghamton, NY 13902

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **19 OCT 2009**	2. REPORT TYPE	3. DATES COVERED **01-06-2008 to 31-05-2009**

4. TITLE AND SUBTITLE **A Testbed for Reconfigurable Network Security Research and Experimentation**	5a. CONTRACT NUMBER **FA9550-08-1-0267**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Research Foundation of SUNY,Binghamton University,Department of Electrical and Computer Engineering, Po Box 6000,Binghamton,NY,13902**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

Abstract

A novel reconfigurable network testbed has been developed, suitable for the implementation, testing and analysis of new and existing network-based defenses against various information attacks. The system is based on a cluster of reconfigurable networking nodes that can be configured to emulate an arbitrary network infrastructure. This novel testbed is the first of its kind to incorporate hardware reconfigurability at multiple network layers, integrating FPGA co-processing elements in both the network interface and routing infrastructure. The system supports emulation of combined hardware/software network-based defense mechanisms. The system has been built and is operational. To date, small test experiments have been performed to verify operation of the platform. Full-scale simulations are currently under development.

General description of the facility. A reconfigurable network tested has been constructed to support experimentation and testing of combined hardware/software network security defense mechanisms for gigabit networks and beyond. As modern networks become faster and more feature-laden, attacks against them become increasing sophisticated and prevalent. It is widely accepted that today's software-based defense mechanisms, which are embedded in routers and end-hosts, will be overwhelmed by the rate of traffic they will be required to process. It is also known that more sophisticated hardware-based defense mechanisms can be embedded within the network infrastructure to better secure it. While research has already started to address this need, evaluation of new security mechanisms is hindered by the hard-wired architecture of the current network infrastructure. Limited reconfiguration of networking components is possible in some instances through device hacking and firmware modification, but this approach is insufficient for practical analysis.

The developed reconfigurable network testbed facilitates analysis of hardware-based network defense mechanisms. The system is based on a cluster of networking components that can be quickly reconfigured to emulate a wide-range of network configurations. These components are reconfigurable in both hardware and software, allowing accurate high-speed network emulation. The architecture of the reconfigurable network testbed is illustrated in Figure 1.

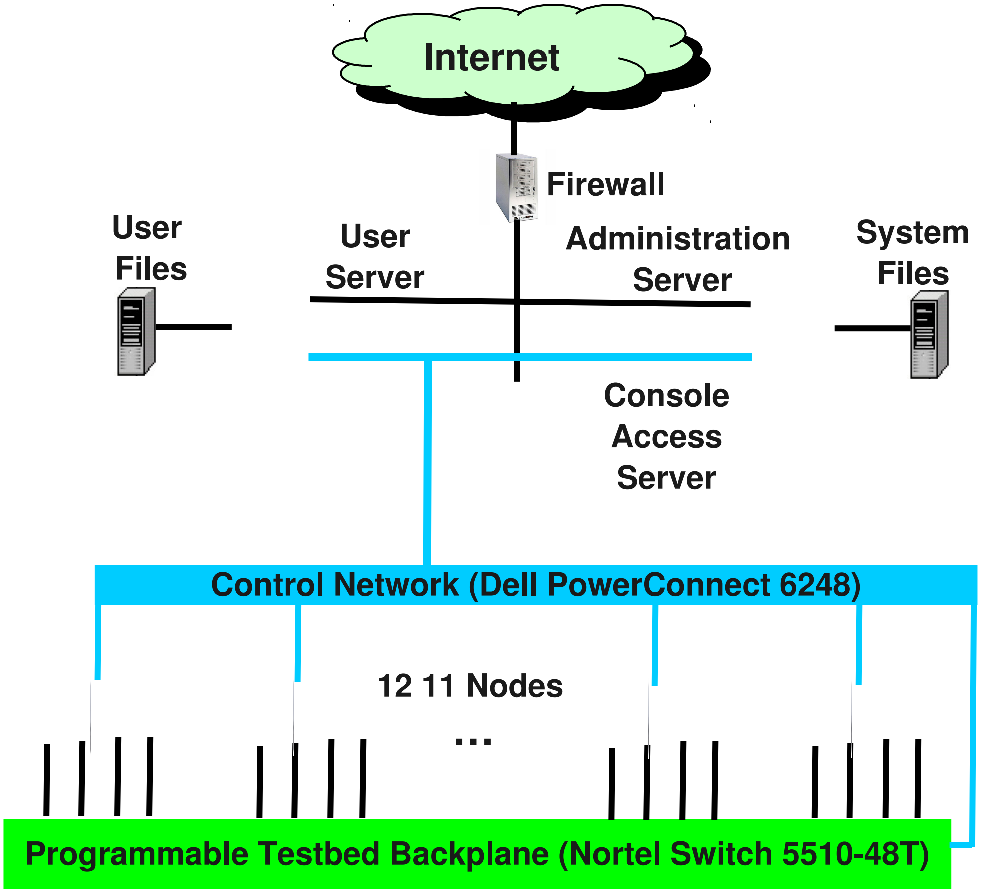

Figure 1. Architecture of the reconfigurable network testbed.

At the heart of the testbed are 11 reconfigurable networking nodes. Each node is based on an augmented XD2000 Development System from XtremeData, Inc. The development system consists of a linux PC tower with a dual Intel Xeon motherboard. One Xeon socket is populated with XtremeData's new XD2000 FPGA Coprocessor module, based on an Altera's Stratix II device. This coprocessor allows true FPGA coprocessing at the system processor level, which supports hardware acceleration of network processing at network layers 3 and above. The processor and co-processor each have 4GB of DDR SDRAM. Xtremedata's development system has been be augmented with a NetFPGA development board. The NetFPGA is an open platform reconfigurable development board that is used to build advanced network flow processing systems. On the board are a programmable Virtex II FPGA (with two PowerPC processors), SRAM, DRAM, and four 1Gbps Ethernet ports. The FPGA can be used to do low-level packet processing acceleration functions within the NIC. Aside from the kernel reconfigurable networks, there are 8 Dell 2950 servers that are also connected through the 6248 and 5510-48T switches. These servers not only provide the background traffic for the network security experiments, but also plays variant roles in the network architecture. In addition, when necessary, these Dell servers can be used as computing resources when computationally expensive operations are conducted.

This reconfigurable network testbed is the first of its kind to incorporate hardware reconfigurability at multiple network layers, integrating FPGA co-processing elements in both the network interface and routing infrastructure. Thus, the platform supports hardware accelerated network security approaches at all levels of the packet processing hierarchy.

The 48 network interfaces of the reconfigurable networking nodes are interconnected by the testbed's programmable testbed backplane, consisting of a Nortel Switch 5510-48T. The control network (PowerConnect 6248 Managed Switch) provides control access to monitoring the status of each test node. The remaining servers form the basic support infrastructure for the reconfigurable network testbed. These control user access, node configuration, and other administrative functions required.

The following highlights the main features of the facility:

- Gigabit per second packet processing capability; future upgradeable to 10GBps.
- Experimentation with hardware accelerated or pure hardware packet processing.
- Simultaneous testing of hardware-accelerated network processing in both the network interface and upper-level packet processing.
- Implementation and testing of defensive network mechanisms targeted at either end-host packet processing or Internet routing infrastructure defense.
- Real-time monitoring of network performance.
- A realistic and controlled reconfigurable Internet infrastructure allows for real-time simulation of Internet environment.
- Ability to inject any kind of network packet traces into a physical (not virtual) network environment to evaluate network defense mechanisms.

Research Projects Currently Supported by the Testbed

- **Server-Level Analysis of Network Operation Utilizing System Call Data**, a three-year, $600k project funded by the Air Force Office of Scientific Research (contract number FA9550-07-1-0453, PI: Douglas H. Summerville). This project began on May 1, 2007. The objective of this research is the development of a prototype system for the detection of multipartite malware and multistage attacks, which attack from multiple points *within* an information infrastructure, simultaneously (multipartite) or in sequential steps (multistage). This project is leveraging the hardware acceleration of the new testbed to perform network operation and server-level processing
- **Network Infrastructure Security** (PI: Chen, not yet funded) The DURIP supported testbed supports research at Binghamton University that addresses the compelling need to secure network infrastructure. Attacks against the fundamental Internet infrastructure lead to enormous destruction, as different infrastructure components of the Internet have implicit trust relationships with each other. A robust and intelligent infrastructure is vital to protect nation-wide interests. We propose to reinforce the network infrastructure by developing a reconfigurable, composable, and scalable network security system using distributed reconfigurable hardware devices. Moore's Law predicts that the number of

transistors that are integrated on a chip double every 18 months. As the transistor count is directly related to computing power, this law implies that computing power doubles every 18 months. This exponential gain is not sufficient to keep pace with advances in communication technology. Gilder's Law of Telecom predicts that bandwidth needs will grow at least three times faster than computing power. It is reasonable to expect that the gap between network bandwidth and computing power will continue to widen. Under such pressure on performance, reconfigurable hardware based security solutions become an ideal candidate. The network testbed will facilitate new security solution prototyping using FPGA devices and verification of performance.

- **In-Network Packet Level Intrusion Detection** (PI: Summerville, not yet funded) As network speeds increase and attacks against the network infrastructure become more sophisticated, more responsibility for protecting the network infrastructure against attack must be offloaded to the network. Detecting attacks in the network will become a necessity. Such detection will require advanced hardware-based packet filtering and detection approaches. A real-time packet-level anomaly detection system for network intrusion detection has been proposed that addresses this need. The approach is based on modeling normal traffic using a fully-automatic unsupervised machine learning approach. Network connections are characterized using a novel technique that maps packet-level payloads onto a set of counters using bit-pattern hash functions, which are no more complicated to implement in hardware than simple logic operations. Machine learning is accomplished by mapping the unlabelled training data onto a set of two-dimensional grids and forming a set of bitmaps that identify anomalous and normal regions. These bitmaps are used as the classifiers for real-time detection. The proposed method is extremely efficient in both the offline machine learning and real-time detection components and has the potential to provide accurate detection performance due to the ability of the bitmaps to capture nearly arbitrary shaped regions in the feature space. Features are programmable, providing flexibility to accommodate normal changes in network usage over time. The approach was developed with high-speed hardware implementation in mind. Results of a preliminary study demonstrate the great potential of the proposed technique. A hardware prototype will be developed on the testbed to demonstrate the practicality of the approach for detecting attacks in a high-speed network environment.
- **Detection of Covertly Embedded Hardware** (PI: Summerville, not yet funded)The objective of this research is to develop methods to detect active attempts to embed malicious functionality within digital circuits and investigate secure circuit design techniques that reduce or eliminate an attacker's ability to exploit this emerging form of stealthy attack. Tampering is detected near the end of the design cycle and does not rely on secure design facilities or tools. As a result, this approach enables full access to the latest COTS design technologies, including open source cores and cell libraries. In addition, because the approach does not rely on validation with respect to a clean circuit, the threat from insider

attack is eliminated. The impact of this research will be secure circuit design approaches and tampering detection methods that raise the bar for the attacker, making the level of security for hardware design commensurate with the state of the art in software protection. The proposed techniques are based on the observation that standard design methodologies leave structural artifacts within the unused state space of digital circuits. These artifacts cannot be observed through traditional testing and verification. Active attempts to embed covert functionality alter these structural artifacts, forming an accurate basis for detection. A study of modern digital circuit design techniques will provide a more complete understanding of these artifacts for use in developing subsequent detection approaches. This understanding will further be used to evaluate digital circuit design techniques that are inherently tamper resistant. The anticipated outcome of this research will be a set of techniques for the detection of covertly embedded malicious circuits, suitable for incorporation into modern CAD tool chains. Prototypes of these tools will be developed and tested against standard benchmarks. In addition, recommendations for circuit design techniques that resist the embedding of covert functionality will be provided.

Academics Currently Supported by the Testbed

The Department of Electrical and Computer Engineering (ECE) Course modules are being developed to be included into EECE658, Hardware-based Security. This PhD level graduate course focuses on security aspects of hardware systems. The testbed is enabling new courses in the area of reconfigurable network security, a growing area of need as network speeds increase and attacks become increasingly sophisticated. Hardware-accelerated networking approached will be needed to counter future threats to our national infrastructure. Graduates having the combined hardware, software, and security education will be needed to counter such threats. Most security professionals are primarily software specialists. It is necessary to train hardware engineers in the principles of security. A graduate course has been facilitated by the DURIP funded testbed, which will provide an experimentation platform and valuable research data that is to be introduced into the classroom.