Final Report for Intel Research Council Award: Efficient Intrusion Detection and Response Systems

Wu-chang Feng
Portland State University
wuchang@cs.pdx.edu

1 Research

The award has supported a diverse set of projects on areas Intel is interested. Note that for all of the publications and software listed below, Intel is acknowledged for enabling the work. In addition, all material generated as a result of this award can be downloaded from `http://www.thefengs.com/wuchang/work/ixp`.

1.1 Packet classification research using the IXP

The initial thrust of the project was to do deep packet inspection for intrusion detection systems. However, the memory limitations of the initial boards made it difficult to do anything beyond packet classification using header fields. As a result, the major contributions of this project are related to packet classification. In particular, the project obtained results in analyzing organization of packet classification caches [1], examining a new approach for packet classification based on approximate caches [2, 3, 4, 5], and understanding how to map packet classification algorithms onto the IXP [6]. In addition, as part of this effort, we also built an open-source packet classification simulator [7] and an open-source traffic replay tool called TCPivo [8, 9] which has been used by Aaron Kunze at Intel and by other researchers.

1.2 On-line Games

Our project also examined a issues involving on-line games in order to determine the feasibility of using the IXP network processor to accelerate them. The work initially focused on the traffic analysis of game servers [10, 11, 12, 13, 14]. Since network processing consumes a minimal amount of resources compared to the rest of the application, we have been refocusing our efforts to determine how other aspects of gaming. The result of this has been an invited talk at SC'05 MasterWorks [15] on high-performance computing in next generation games and an on-going collaboration with Erik Johnson looking at ways for securing online games against cheating via trusted platforms.

1.3 Network Puzzles

This project examined the use of client puzzles to thwart denial of service attacks and other forms of undesirable communication. The end goal is force those initiating malicious traffic to pay a computational tax on sending such traffic. This is an on-going project and has generated several publications and a source-code release [16, 17, 18, 19].

2 Education and Outreach

2.1 IXP Networking Practicum course

While at OGI, I established an IXP networking practicum course (CSE 580) which was based around

the IXP1200 network processor. The course was offered twice. The first offering had 17 students (12 Intel employees) and received a 3.4/4.0 rating. The second offering had 12 students (6 Intel employees) and received a perfect 4.0/4.0 rating. The curriculum developed is freely available and the slides and laboratories were used by several other institutions including Portland State University (prior to my arrival) [20].

2.2 Talks and Workshops

Throughout the four years of the project, I have attempted to transfer the ideas and the results of our work to Intel. In particular, I participated in the Intel IXA workshops in 2002, 2003, and 2004 and gave talks at the first two. In addition, I gave a colloquium talk in October 2003 on our work in network puzzles. I am also arranging with Erik Johnson to give another colloquium talk on high-performance computing in on-line games.

3 Assessment

While the research deliverables on the project are of reasonable quality, I am still working to improve the level of direct interaction with Intel. With a more stable financial situation at PSU, a wider array of students to work with, and better working relationships with a variety of Intel employees, I plan on improving both the quality of the research being undertaken as well as the level of impact it has on Intel.

References

[1] K. Li, F. Chang, D. Berger, and W. Feng, "Architectures for Packet Classification Caching," in *IEEE International Conference on Networks (ICON)*, Sydney, Australia, September 2003.

[2] F. Chang, W. Feng, and K. Li, "Approximate Caches for Packet Classification," in *Poster session of ACM SIGCOMM*, August 2003.

[3] F. Chang, W. Feng, and K. Li, "Approximate Caches for Packet Classification," in *INFOCOM*, 2004.

[4] F. Chang, , W. Feng, W. Feng, and K. Li, "Efficient Packet Classification with Digest Caches," in *HPCA Workshop on Network Processors (NP3)*, 2004.

[5] F. Chang, W. Feng, W. Feng, and K. Li, "Chapter 3: Efficient Packet Classification with Digest Caches," in *Network Processor Design: Issues and Practices*. 2005, Morgan Kaufmann Publishers.

[6] D. Srinivasan and W. Feng, "Performance analysis of multi-dimensional packet classification on programmable network processors," in *IEEE LCN*, November 2004.

[7] PCCS developers, "PCCS: Packet Classification Cache Simulator," `http://pccs.sourceforge.net/`, 2003.

[8] W. Feng, A. Goel, A. Bezzaz, W. Feng, and J. Walpole, "TCPivo: A High-Performance Packet Replay Engine," in *ACM SIGCOMM Workshop on Models, Methods, and Tools for Reproducible Network Research (MoMeTools-03)*, Karlsruhe, Germany, August 2003.

[9] TCPivo developers, "TCPivo," `http://syn.cs.pdx.edu/projects/tcpivo`, August 2002.

[10] W. Feng, F. Chang, W. Feng, and J. Walpole, "Provisioning On-line Games: A Traffic Analysis of a Busy Counter-Strike Server," in *Proc. of*

the Internet Measurement Workshop, November 2002.

[11] F. Chang, W. Feng, W. Feng, and J. Walpole, "Provisioning On-line Games: A Traffic Analysis of a Busy Counter-Strike Server," in *Poster session of ACM SIGCOMM*, August 2002.

[12] F. Chang and W. Feng, "Modeling Player Session Times of On-line Games," in *NetGames 2003*, May 2003.

[13] W. Feng and W. Feng, "On the Geographic Distribution of On-line Game Servers and Players," in *NetGames 2003*, May 2003.

[14] W. Feng, F. Chang, W. Feng, and J. Walpole, "A Traffic Characterization of Popular On-line Games," *IEEE/ACM Transactions on Networking*, vol. 13, no. 3, June 2005.

[15] W. Feng, "Got MIPS? The Need for Speed in On-line Games," SC—05 MasterWorks invited talk.

[16] W. Feng, "The Case for TCP/IP Puzzles," in *ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA-03)*, Karlsruhe, Germany, August 2003.

[17] W. Feng, "PuzzleNet," `http://syn.cs.pdx.edu/projects/puzzles`, May 2003.

[18] W. Feng, E. Kaiser, W. Feng, and A. Luu, "The Design and Implementation of Network Puzzles," in *Proceedings of IEEE INFOCOM*, March 2005.

[19] E. Kaiser, W. Feng, W. Feng, and A. Luu, "Reducing Malicious Traffic with IP Puzzles," in *USENIX Security Symposium (poster session)*, August 2004.

[20] W. Feng, "CSE 580: Networking Practicum," `http://www.thefengs.com/wuchang/work/courses/cse58x_spring2003/`.