

Contents

- 1 Introduction 1
 - 1.1 Hardware Support for Network Security 4
 - 1.2 Platforms for Hardware-Based Networking 5
 - 1.3 High-Level Compilation of Networking Hardware 7
 - 1.4 Thesis Contributions 8
 - 1.5 Thesis Structure 11

- 2 Reconfigurable Hardware 13
 - 2.1 Field Programmable Gate Array (FPGA) 13
 - 2.1.1 Architecture 14
 - 2.1.2 Development Process 15
 - 2.1.3 Partial Reconfiguration 17
 - 2.1.4 Special FPGA architectures 18
 - 2.2 Hardware Development Boards 20
 - 2.2.1 BeeCube BEE3 20
 - 2.2.2 NetFPGA 10G 22

- 3 Prior and Related Work 25
 - 3.1 Hardware Support for Network Security 25
 - 3.1.1 Packet Classification 27
 - 3.1.2 Pattern Matching 29
 - 3.1.3 Anomaly Detection 30
 - 3.1.4 High-Level Applications 31
 - 3.1.5 Communication Stacks 32
 - 3.2 Hardware-Based Network Platforms 34
 - 3.2.1 FPGA Development Platforms 34
 - 3.2.2 Network Processors 36
 - 3.3 Custom architectures 38
 - 3.4 High-Level Hardware Compilation 40
 - 3.4.1 General Purpose Languages 40
 - 3.4.2 Domain-Specific Languages 42
 - 3.4.3 Micro-programmable and customized Hardware 44

3.5	Honeypots	45
3.5.1	Honeypot Systems	46
3.5.2	Hardware Honeypots	47
4	NetStage Core Architecture	49
4.1	Platform Design	50
4.2	Platform Architecture	52
4.2.1	Message-based Communication	54
4.2.2	Buffer Design	55
4.2.3	Reconfigurable Handler Slots	58
4.2.4	Core-to-Handler Shared Bus	60
4.2.5	Routing Service	61
4.2.6	Global Application State Service	66
4.2.7	Notification Timer Service	68
4.3	NetStage Communication Core	70
4.3.1	Core Architecture	71
4.3.2	Stage 1 - Ethernet Layer	72
4.3.3	Stage 2 - ARP and IP Layer	74
4.3.4	Stage 3 - UDP/TCP Layer	78
4.3.5	Stage 4: Routing Layer	82
4.4	Lightweight TCP Implementation	84
4.4.1	Lightweight TCP Connection Establishment	84
4.4.2	TCP Data Transmission	85
4.4.3	Window Sizing	87
4.4.4	Segmentation	88
4.4.5	Closing Connections	88
4.4.6	Comparison with other network communication cores	88
4.5	Chapter Summary	90
5	NetStage Platform and Application Support	93
5.1	Application-Specific Service Handlers	94
5.1.1	Handler Types	95
5.1.2	Handler Interface	97
5.2	Supporting Platform Services	101
5.2.1	Management Interface	101
5.2.2	Extended Statistics	103
5.2.3	Mirror Port Functionality	103
5.2.4	Simulation Environment	104

5.3	Dynamic Partial Reconfiguration	105
5.3.1	Architecture	106
5.3.2	Reconfiguration Controller	107
5.3.3	Reconfiguration Candidate Selection	109
5.3.4	Adaptation Engine Implementation	111
5.3.5	Discussion of Packet Routing	113
5.3.6	Transferring Bitstream Data	115
5.4	Chapter Summary	116
6	Malacoda: Compiling Honeygot Applications on NetStage	117
6.1	Domain Specific Languages	118
6.2	DSL Decision and Domain Analysis	120
6.2.1	Domain Analysis	121
6.3	Language Design	124
6.3.1	Syntax	124
6.3.2	User-Defined Variables	125
6.3.3	Expressions	127
6.3.4	Log Messages	127
6.3.5	Malacoda Examples	128
6.4	Compiler Implementation	129
6.4.1	Handler Microarchitecture	131
6.4.2	Compile Flow	133
6.4.3	Conditions	137
6.4.4	Regular Expression Matching	139
6.4.5	Variables	140
6.4.6	Response Packets	142
6.4.7	Log Packets	144
6.4.8	Optimizations	144
6.5	Chapter Summary	145
7	Experimental Results	147
7.1	Hardware Implementation	147
7.1.1	BEE3 Prototype	148
7.1.2	NetFPGA 10G Prototype	148
7.1.3	Buffer Management	149
7.2	Hardware Synthesis Results	151
7.2.1	Core Synthesis	151
7.2.2	Handler Synthesis	153

7.2.3	System results	158
7.2.4	Dynamic partial reconfiguration	159
7.3	Network Performance	161
7.3.1	Core Latency and Throughput	161
7.3.2	Handler Performance	163
7.4	MalCoBox Live Test	164
7.4.1	Network Statistics	165
7.4.2	Service Emulations	168
7.5	Chapter Summary	170
8	Conclusions and Future Work	171
8.1	Summary and Conclusions	172
8.1.1	Platform	172
8.1.2	Malacoda	174
8.1.3	Results	174
8.2	Future Work	175
8.2.1	Hardware	175
8.2.2	Compiler	177
	Bibliography	179