

Contents

1	Introduction	1
1.1	State of the art	1
1.1.1	Proxy	1
1.1.2	Encrypting proxy	2
1.1.3	Anonymity group	2
1.1.4	Mix	2
1.2	Motivation	3
1.2.1	Goals	3
1.2.2	Non-goals	3
2	Threat models and countermeasures	5
2.1	Remote adversary	6
2.1.1	Certainty	6
2.1.2	Complexity	6
2.1.3	Countermeasures	6
2.2	Local adversary	7
2.2.1	Certainty	7
2.2.2	Complexity	7
2.2.3	Countermeasures	7
2.3	Global adversary	8
2.3.1	Passive Attacks	8
2.3.2	Active Attacks	15
2.3.3	Message tampering	16
2.4	Third party	18

3	Evaluation of existing solutions	21
3.1	Proxy	21
3.2	Encrypting Proxy	22
3.3	Mix	22
3.3.1	Cypherpunk remailers	22
3.3.2	Tor (The Onion Router)	23
3.3.3	JAP (Java Anon Proxy)	23
4	Design of PGA	25
4.1	Overview	26
4.2	Client	27
4.2.1	Achieving platform independence	28
4.2.2	Achieving application independence	32
4.2.3	Achieving simplicity	36
4.3	HTTP proxy	38
4.3.1	Request Parsing	39
4.3.2	Response Parsing	48
4.3.3	Message parsing	51
4.3.4	Persistent connections	55
4.4	Server	57
4.4.1	Core	57
4.4.2	Remote Management	66
4.5	Certificate Authority	66
4.6	Tunnel protocol	67
4.6.1	Generic message format	67
4.6.2	Message syntax and semantic	69
4.6.3	Message tunneling	73
4.6.4	Flow control	85
4.6.5	Adaptive dummy traffic generation	100
4.7	Remote Management protocol	101
5	Java NIO Framework	107
5.1	Motivation	107
5.2	Introduction	107
5.3	Multiplexing Strategies	110

5.3.1	One Thread Per Socket	110
5.3.2	Readiness Selection	110
5.4	Java NIO Framework Design	112
5.4.1	Mapping the Reactor Design Pattern	112
5.4.2	Example	118
5.4.3	Parallelization	119
5.4.4	I/O Processing	121
5.4.5	Synchronization of Parallel I/O	124
5.5	Forwarders and Transformers	125
5.5.1	Atomic Forwarders	126
5.5.2	Composite Forwarders	130
5.6	SSL	135
5.7	Prevention of redundant copy operations	137
5.8	Usage	137
5.9	Conclusions	139
6	Implementation	141
6.1	Overview	141
6.2	Tunneling	141
6.2.1	I/O processing	141
6.2.2	Dummy traffic coordination	142
6.2.3	Message representation	143
6.2.4	Protection against bandwidth attacks	144
6.3	Target I/O handling	146
6.4	Server	147
6.4.1	Address resolution	147
6.4.2	CPU load detection	148
6.4.3	Remote file browsing	149
6.4.4	Anonymity group management	149
6.4.5	User management	150
6.4.6	Traffic accounting	150
6.4.7	Misuse discouragement	152
6.4.8	Testing	153
6.5	Remote Management	155
6.6	Client	156

6.6.1	Autostart	156
6.6.2	Automatic Proxy reconfiguration	162
6.6.3	Bandwidth charts	166
6.7	Certificate Authority	166
6.7.1	Initialization	166
6.7.2	Certificate request handling	169
6.7.3	Miscellaneous	170
7	Usage	171
7.1	Certificate Authority	171
7.1.1	Initialization	171
7.1.2	Certificate request handling	171
7.2	Server Core	172
7.3	Remote Management	174
7.4	Client	182
8	Conclusion	193
A	ProMeLa models	195
A.1	Message tunneling	195
A.2	XON/XOFF flow control	197