

Contents

Chapter 1	Introduction.....	1
Chapter 2	Background.....	6
2.1	Application Layer Attacks	6
2.2	Secure Socket Layer Protocol.....	9
2.3	Attacks behind HTTPS.....	15
Chapter 3	The Framework of SSL Proxy Server.....	18
3.1	General Concept.....	18
3.2	Essential Framework.....	21
3.3	Aggregative Framework	25
3.4	Selectivity Content Framework.....	28
3.5	Implementation of SSL Proxy Server.....	31
Chapter 4	Experiments	34
4.1	Environment.....	34
4.2	Performance Evaluation	36
Chapter 5	Security Considerations	44
Chapter 6	Conclusions	47
Bibliography	51

List of Figures

Figure 1. The topology of “Defense In Depth”	2
Figure 2. The SSL protocol stack.....	10
Figure 3. SSL Record Protocol.....	11
Figure 4. SSL Full Handshake	13
Figure 5. SSL Resume Handshake	15
Figure 6. Attack is invisible under encryption	17
Figure 7. The concept of SSL Proxy Server.....	19
Figure 8. Practical deployment of SSL proxy server	20
Figure 9. SSL proxy server handles connections.....	22
Figure 10. The process of client’ s request	25
Figure 11. The process of response from server	25
Figure 12. Aggregative Framework	26
Figure 13. Check session table in order to use resume handshake.....	28
Figure 14. Selectivity Content Framework	31
Figure 15. User interface for monitoring the incoming requests.....	33
Figure 16. The comparison of connection rate	38
Figure 17. The comparison of the response time	43

List of Tables

Table 1. Request object type popularities	29
Table 2. Equipments of Testbed.....	35
Table 3(a). Connection rate of essential framework	36
Table 3(b). Connection rate of aggregative framework.....	37
Table 3(c). Connection rate of selectivity content framework	37
Table 4(a). Throughput of essential framework.....	39
Table 4(b). Throughput of aggregative framework.....	40
Table 4(c). Throughput of selectivity content framework	40
Table 5(a). Response time of essential framework	41
Table 5(b). Response time of aggregative framework.....	42
Table 5(c). Response time of selectivity content framework.....	42