Appendix A: Format of Report [for the victim to the policy manager]
ID of the report: XXXX
Victim Host Name: Trojan1
Victim Host IP: A.B.C.D
Attacker Host Name: YYYY
Attacker Host IP: E.F.G.H
Type of Attack: Ping-of-death
Time: 3:00:42 AM
Log in /etc/log/report

Appendix B: Format of Policy Update [for the policy manager to every host]
ID of the Policy Update: YYYY
ID of the receive report: XXXX
Destine Host Name: Trojan1 (Host to receive the policy update)
Destine Host IP: A.B.C.D
Attacker Host Name: YYYY
Attacker Host IP: E.F.G.H
Type of Attack: Ping-of-death
Time: 3:00:42 AM
Policy Manager Received Time: 3:00:43 AM.
Action Taken: Block IP E.F.G.H

Appendix C: Format of Status Report [for every host to the policy manager]
ID of the status report: ZZZZ
ID of the receive policy update: YYYY
Host Name: Trojan 1 (Host to submit its status report to policy manager)
Host IP: A.B.C.D
Action Taken: Block IP E.F.G.H
Status: Success
Time: 3:00:45 AM.

Please note that we give you one host to protected in the project (every host in the explanation = 1 host here). However, you will need to implement the table that is maintained by the policy manager and ready to hold large number of hosts. Policy manager will read this table and sent policy update to every host in the table. An example of the table is shown below.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Host Name</th>
<th>Host IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>USC Trojan</td>
<td>Trojan1</td>
<td>x.x.x.1</td>
</tr>
<tr>
<td>USC Trojan</td>
<td>Trojan2</td>
<td>x.x.x.2</td>
</tr>
</tbody>
</table>