Review for group 4, from group 8

Summary

The paper analyses the risk and investment strategies of different actors involved in a DDoS attack. It explains the security issue as that of an ISP trying to mitigate DDoS attacks using its infrastructure and justifies that ISP is the main problem owner of such attacks. It also suggests risk reduction and transfer strategies for the manufacturers to prevent any damages to their reputation, especially considering the proliferation of IOT devices that they produce. Similar strategies are also suggested for the government. The differences in their strategies are explored, given the differences in their risks and risk appetites. The evolution in the legislations to face these attacks are also analysed, with the implemented laws in the Netherlands used as example. The probable peak losses incurred by organizations are are estimated using the data from various sources to compute likely timespan of an attack and the number of attacks.

Nice parts

- The probable peak hourly losses of the organizations are computed nicely using a number of data sources.
- Good to see a lot of references to sources backing up the claims that are made throughout the report
- Nice insights into the evolutions of IOT risk mitigation strategies

Major issues

- The ROSI is not calculated
- The losses shown are for the companies served by the ISP rather than by the ISP itself.
- It appears that you have note incorporated indirect costs in your ROSI calculation, only focussing on the downtime loss.

Minor issues

- The differences in metric performance between the strategies of the various actors could have been more extensive
- Other actors like the organizations under attack could have been explored
- In pointing out the risk strategies the problem owner can follow, you mention risk acceptance, transfer and reduction, but you are missing avoiding the risk altogether