Peer review to Group 13 – Reviewed by Group 11

- **A summary of the assignment:**
  The security issue focused on in their paper is the use of exploited IoT devices for launching sophisticated DDoS attacks, from the viewpoint of the ISPs as problem owners (which they state their goal is to keep the network clean from 'DDoS-requests'). Their research dataset contained connections to a honeypot mimicking an IoT device, which they aim to use to measure the occurred incidents in order to determine which security controls are necessary to prevent future attacks. They state that it is therefore ideal for ISP to know which IP-addresses are used in botnets. Based on their dataset, they defined a metric that measures 'the number of connections made to any system (IP address), to which port, the source IPs and the commands the attackers are executing on the victim machines' (p.4). They define a system as more secure, when there are 'almost only known attacks, for which defences are in place' (p.4). They conclude with the statement that the focus of their investigated security issue lies on incidents and vulnerabilities. Quantitative support for these conclusions and recommendations for their problem owner regarding the security issue are missing.

- **Strengths of the assignment:**
  - Clear introduction and in particular a clear explanation of Honeypots.
  - Nice explanation of the security issue on several actors and clearly stating one problem owner in the end. It gives a more in-depth analysis of the issue.
  - Clear explanation of your dataset. You clearly explain what the data looked like.

- **The list of major issues:**
  - Your paper contains a lot of statements with no scientific support, no reference. Some examples:
    - "The goal of the ISP is to keep the network clean from 'DDoS-requests'" (p.3).
    - "Metrics are effective tools to measure the performance of the detection and mitigation of attacks from the victim's point of view, but can also be used to measure the performance of an attack from the attacks point of view" (p.3).
    - "For improving the security of any system, it is very useful to know what what type attackers to expect, what kind of attack methods are used and what the target(s) of those attackers would be" (p.1).
    - "However, each device that gets connected introduces new privacy and security issues" (p.1).
  - In your 'Ideal metric'-part you explain what ISPs would like to know, but you don't actually explain the metric. What are you measuring? What performance? Isn't what you're measuring a metric to address the issue of disclosing an entire home, instead of a measure for ISP to determine which controls are necessary to prevent future attacks? Would ISPs not also like to know what be solutions would be for them to solve the problem after tracing the specific IP-addresses?
  - In your part 'Metrics in practice' no sources and no explanations of these metrics were included.
  - In your part 'Designed metrics' an in-depth analysis and explanation of your metrics was missing.
  - We notice that the results of applying your metrics to the actual data are missing.
  - Also, a conclusion with a recap of the security issue and concrete recommendations for the problem owner was missing.
  - A discussion of the conducted study is missing.

- **The list of minor issues:**
  - The paper does not really follow the instructions of the assignment, it does not include an abstract, a methodology, a strong title, a reference list, page numbers and an APA-style reference-system.
  - “Metrics are effective tools to measure the performance of the detection and mitigation of attacks from the victim’s point of view, but can also be used to measure the performance of an attack from the attacks point of view” (p. 3). Why is this your introduction for the chapter Metrics as you just told to focus on the ISP point of view? Also, this statement isn’t supported by any scientific source. This is part of our observation that in your metrics you diverge from the perspective of the ISPs and also add measurements that are about understanding attackers' behaviour.
  - The last figure is missing a label, so it is not clear if it is your own figure, or one of the literature.