Peer review group 13 by group 4

Summary

The security issue this paper focusses on is: DDoS attack performed by (infected) Internet of Things devices. The DDoS attack is usually performed by a botnet, who controls many IoT devices. Owners of infected IoT devices usually don't know that their device is being exploited and thus have no incentives to fix this. Another actor is the Internet Service Provider (ISP) since there network is misused, which results in slow connections for customers. This paper takes the perspective of the ISP.
The data that this paper uses is collected via a HoneyPot. It consists of records of date, source IP, destination IP, destination port and list of commands. According to the paper all the records have as destination port 23 and have commands to login to unprotected IP cameras and DVRs. After this, a few shell scripts are downloaded and executed, which probably create a connection with a botnot.
The goal of an ISP is the have zero DDoS attacks in their network. Unfortunately an ISP cannot block a single IP, because several other devices might use the same IP (because of NAT). With IPv6 every device can get an IP address and thus the ISP can block an IP address that is used to perform an DDoS attack. Therefore the ideal metric is the specific IP address that has been used.
Several existing metrics for IoT network are given but an explanation why these metrics are useful is not given.
Several metrics are given such as the number of connections made to a system. A system is considered secure if there are almost only known attacks (for which defences are in place), a system is considered insecure if there are a lot of unknown/uncategorized attacks.

Strength of the assignment

- Well explained security issue, leading to a good explanation of why to focus on the ISPs.
- Clear structure.

Major issues

- Several existing metrics for IoT network are given but an explanation why these metrics are useful is not given
- In the ideal metrics section, the metric proposed is the specific IP address that is by a botnet. But, as mentioned, this can only be done when in the IPv6 address space, however the IPv4 address space isn't going anywhere in the coming decades so this ideal metric is definitely not 'ideal' since it ignores an enormous amount of addresses.
- In 'Metrics we can design from the dataset' you say that we can 'measure' to which port an attack is done, but in the section 'Analysis of honeypot data' you state that every connection attempt is made to port 23. So this metric would be not useful.

- In ‘Metrics we can design from the dataset’, no way of measuring ‘commands the attackers are executing’ is given. One way of doing this might be first thinking of some categories and then mapping each command to a specific category.
- In ‘Metrics we can design from the dataset’ a system is considered insecure if a lot unknown attacks happen and secure if almost only known attacks (for which defences are in place) occur. But if almost no attacks happen then we can’t consider a secure or insecure.
- The metrics from ‘Metrics we can design from the dataset’ are not evaluated.

Minor issues

- In ‘Metrics we can design from the dataset’ it is stated that ‘If there are a lot of unknown and uncategorized attacks….’, but a lot is not quantifiable.