# Economics of Cyber Security

Łoin, Michał Meijerink, Mart Man, Ka-Wing Tubbing, Rico

October 23, 2017

## 1 Introduction

DDoS attacks become bigger and bigger threat every day. In order to fully analyse the risks and possible impacts, one should pay a lot of attention to numerous factors. Actor analysis helps to understand how different characters can influence the security and how likely are they to do it. Evaluation of externalities can help to understand the complete set of effects.

In this paper we will analyse impact of factors that influence the security performance in case of a DDoS attack. In the first section, we will have a look at different actors and the countermeasures they can take, together with corresponding costs and benefits. Later we will see what are the incentives that would motivate actors to implement the solution. Finally, we will describe existing externalities connected to the DDoS attack. In the next section, we will perform statistical analysis of the data set, in order to discover what impact certain factors have on the metrics.

## 2 Analysis of actors

This section describes one concrete countermeasure for three different actors. The costs and benefits, incentives, and externalities involved are described per countermeasure.

The following actors were selected:

- Internet Service Provider
- Manufacturers
- IoT device owners

### 2.1 Countermeasures

In order to mitigate the problem of DDoS attacks, each of the actors described above can choose a different strategy. The main problem owner, that is the ISP whose customers are being attacked, has a possibility to perform traffic analysis and set up a mitigation service. Implementation of monitoring systems would enable packet inspection, which enables the ISP to filter malicious traffic after it determined patterns for legitimate packet flow. That way the suspicious packets can be analysed later and malicious ones dropped immediately.

In terms of protection against DDoS attacks the second actor, which is the manufacturers of IoT devices, should put most efforts on implementing proper security controls and protocols in the devices. Some of those technologies include firewalls, intrusion detection systems (IDSs) or load balancing protocols. By introducing some of the mentioned solutions, the manufacturer directly increases the security. Therefore, the attackers must increase the amount of resources necessary for the attack to succeed.

The last actor, the owners of IoT devices, can help to mitigate the security issue indirectly by demanding proper security standards. If the security standards are seen as a crucial part of any IT related product in the society, it would put some pressure on the manufacturers to increase them, in order to attract potential buyers. However, security stays a market for lemons [7] and therefore, it is difficult to assess the actual security of devices. For the average consumer this could even be viewed as almost impossible. Companies, however, have more influence. They can implement proper network security measures, which can help protect the IoT devices they buy. Even if they still might fall victim to attackers, all malicious traffic could be filtered by the company. This way, DDoS traffic could be stopped by the source, introducing the least possible impact.

### 2.2 Costs versus Benefits

In Table 1, the costs and benefits of the actors ISP, manufacturers and consumers are given.

### 2.3 Incentives

In this section we will analyse the incentives of the aforementioned actors. Incentives are important because it gives is insights into why a certain actor implements certain security controls and ignores others. The first actor that will be discussed is the ISP, which is followed by the manufactures and finally the IoT device owners.

| Actor | Costs | Benefits |
|---|---|---|
| ISP | Investment in traffic monitoring | Less revenue losses due to downtime by DDoS attacks |
| | Investments in mitigation techniques | Maintaining reputation due to less disruptions. |
| Manufacturers | Investment in security guidelines | Liability covered |
| | Investment in implementing controls | Selling points for tested product security |
| | Investment in penetration tests | New security standards force the whole community to adapt and improve to reach them |
| Consumers | Investing resources to increase awareness | Not contributing to DDoS with their IoT devices. |
| | Spending time to learn about security and demand proper standards | Products not slowed down due to usage for DDoS attacks. |

Table 1: Costs versus benefits

#### 2.3.1 ISPs

The problem owner, the ISP, is able to most easily introduce countermeasures against DDoS attacks as the owner of the network. The biggest incentives for ISP's to actually take action, is to secure the resources of their network and to increase their reputation as customers experience less downtime of their internet connection.

When DDoS attacks are properly mitigated, the network bandwidth of the ISP will not be affected by DDoS traffic. Therefore, the network will be more stable and need less resources to maintain sufficient connection.

#### 2.3.2 Manufacturers

Manufacturers of IoT devices will have the least incentive to invest in security measures. Their first objective is to deliver a working product which will win them market share. Implementing security measures costs labour, needs research, and does not contribute to the (observable) functionality for their customers. This is also the reason end users are not demanding the manufacturers implement protection techniques in their devices. However, when legislation is introduced, like the '*IoT Improvement Act*' [5], the manufacturers can be moved to take action. Adhering to the legislation will add an advantage to their product over their competitors.

#### 2.3.3 IoT device owners

Buyers of IoT devices are first of all focused on the product and with that the features they can observe. Security is not one of them. Therefore, the cyber security of an IoT device is less of an influencing factor when comparing devices. Also, (home) consumers have no direct monetary loss because of compromised devices. Focusing on companies, however, cyber security is more and more an issue which is taken into account. With that in mind, companies will become more interested in the security of devices they plug in to their network. Although, these incentives to demand better device security will be made with the integrity of the company network in mind, in which they do not want to introduce easily exploitable devices which might be used as a stepping stone to intrude in the network. Even though, the security issue of DDoS attacks is not addressed directly by these consumers, indirectly this also leads to less IoT devices which can be used in DDoS attacks. This is also the strategy of the US government, which introduced the '*IoT Improvement Act* [5]' to use the federal governments' buying power to increase standards in IoT device security in the hope that these standards will spread industry wide.

### 2.4 Externalities

Externalities in economics are the benefits or cost that occur for a party that occur by decisions of third parties [8]. For example, driving with unnecessary weight is a negative externality for the society since it pollutes the environment.

An actor that creates an externality for an ISP, which we call $A$, are other ISPs. If the ISPs have implemented controls to mitigate DDoS attacks, this can benefit ISP $A$ because it might be that less DDoS attacks now appear in $A$'s network due to controls of the other ISPs. Since the majority of the victims of DDoS attacks are users across networks [6], an ISP might be affected by IoT devices which are used to perform these attacks. This means that manufacturer of IoT devices are an externality, because they decided to neglect the security of these devices. Furthermore, consumers of these insecure devices are also an externality, because they introduce them in the network of the ISP.

When manufacturers increase the standard implemented security controls for all their devices, this has a clear benefit to all security issues involving botnets. Botnets will have more trouble growing and maintaining a big network of devices, due to the security controls. As stated in [2], "the capability of the bots can be reduced by the combined efforts of device manufacturers, legislators, regulators and end-users to implement and follow basic cybersecurity and cyber-hygiene guidelines".

Last, we consider the externalities introduced by the countermeasures of the consumers. When companies introduce proper network security, enabling them to detect and take out compromised IoT devices in their network or filtering malicious traffic, DDoS attack traffic will not reach its victim, or even the internet. Especially potential victims and their ISPs will benefit from this as less traffic will reach them. Widespread implementation of this countermeasure by many IoT device buyers will be needed for this externality to have a noticeable effect.

# 3 Data set analysis

In this section we will try to find factors which influence the security performance of an ISP, with these factors we will perform a statistical analysis on the impact of these factors on the security performance. In order to perform the statistical analysis, first the security performance of the ISP has to be measured. This can be measured with the following metrics:

- Number of attacks
- Duration of an attack
- Number of packets

The number of attacks can tell how well an ISP can detect if an event is a DDoS attack, while the duration and number of packets can tell how fast an ISP can mitigate these attacks. However, the duration and number of attacks depends as well on the attacker: if the attacker believes he has done enough damage, he stops the attack. Several other factors might affect the measurements as well.

## 3.1 External factors

As mentioned in the previous section, the metrics are influenced by several other factors than solely the security in controls in place from an ISP. In this section we will take a look at the external factors that influence the variance in the aforementioned metrics.

The first external factor is the popularity of IoT devices or the growth of the number of IoT devices. It is well-known that IoT devices are exploited and become part of botnets [3], which are used to perform DDoS attacks. As the number of IoT devices is growing, botnets are potentially growing as well. Larger botnets are able to perform bigger attackers in the form of number of packets or duration.

The metrics could also be influenced by the government. If the government educates kids about the damage DDoS attacks, less attacks might occur. However, measuring the influence of this factor is hard with the current data set, as it only contains dates from 2013 till end of 2016.

Besides these two factors, attribution of people who are responsible for DDoS attacks can influence the metrics. A higher risk emerges if people can be brought to court, which thus might scare people off who are on the edge of performing a DDoS attack. However, this factor is hard to measure as DDoS attacks happen on a global level while jurisdiction happens on national level.

We will now focus on the number of IoT devices as this factor is the most trivial to measure. In [4], the author states that in 2013 there are around 9 billion IoT devices. In [1], the authors state that in 2013 there are around 11.2 billion devices, and in 1015 18.2 billion. We will use the data provided in [1] so that we can estimate the number of IoT devices that are in use in a specific month. Using the numbers we have of IoT devices per year, we can use Lagrange Interpolating Polynomial to create a function. This function can give us the estimated amount of IoT devices each month.Using an online tool that does the interpolation for us, this is the given formula for the estimation per month Equation 1.

$$\begin{aligned} f(x) = {} & 8.6904428904435900 * x^0 \\ & + 1.9175407925384214 * 10^{-1} * x^1 \\ & + 1.4639584952201602 * 10^{-3} * x^2 \\ & + 1.8447023655170587 * 10^{-5} * x^3 \\ & + -8.0094481135208151 * 10^{-8} * x^4 \end{aligned} \tag{1}$$

In Table 2 and Figure 1, you can find the estimated number of IoT devices per month. Note that we started from December 2012 and ended in July 2015 because that is the range of our dataset.

## 3.2 Statisical analysis

In Figure 2, you can find the linear regression of the estimated number of IoT devices vs the number of DDoS attacks found in the dataset.

# 4 Conclusion

The linear regression shows that there is somewhat a correlation between the number of IoT devices and the number of DDoS attacks. The more IoT devices there are,

| x | Month-year | Estimated amount of IoT devices | Amount of DDoS attacks |
|---|---|---|---|
| 11 | 12-12 | 11,00025707 | 67 |
| 12 | 01-13 | 11,23251748 | 173 |
| 13 | 02-13 | 11,46889544 | 191 |
| 14 | 03-13 | 11,70947759 | 112 |
| 15 | 04-13 | 11,95434866 | 167 |
| 16 | 05-13 | 12,20359147 | 851 |
| 17 | 06-13 | 12,4572869 | 189 |
| 18 | 07-13 | 12,71551391 | 794 |
| 19 | 08-13 | 12,97834956 | 694 |
| 20 | 09-13 | 13,24586895 | 2020 |
| 21 | 10-13 | 13,51814528 | 16768 |
| 22 | 11-13 | 13,79524984 | 20031 |
| 23 | 12-13 | 14,07725197 | 5735 |
| 24 | 01-14 | 14,36421911 | 34917 |
| 25 | 02-14 | 14,65621677 | 11746 |
| 26 | 03-14 | 14,95330853 | 14633 |
| 27 | 04-14 | 15,25555605 | 15375 |
| 28 | 05-14 | 15,56301908 | 38938 |
| 29 | 06-14 | 15,87575544 | 125793 |
| 30 | 07-14 | 16,19382102 | 293810 |
| 31 | 08-14 | 16,51726981 | 137913 |
| 32 | 09-14 | 16,84615385 | 49631 |
| 33 | 10-14 | 17,18052327 | 142153 |
| 34 | 11-14 | 17,52042628 | 170935 |
| 35 | 12-14 | 17,86590918 | 250782 |
| 36 | 01-15 | 18,21701632 | 449625 |
| 37 | 02-15 | 18,57379014 | 366205 |
| 38 | 03-15 | 18,93627117 | 361220 |
| 39 | 04-15 | 19,30449799 | 291052 |
| 40 | 05-15 | 19,6785073 | 284969 |
| 41 | 06-15 | 20,05833383 | 569185 |
| 42 | 07-15 | 20,44401042 | 247888 |

Table 2: Estimation of IoT devices per month

the more DDoS attacks are done. However, this correlation may be biased, because more honey pots were placed later in the researched and thus more DDoS attacks might be measured because of the increased amount of honey pots.

# References


[1] D. Airehrour, J. Gutierrez, and S. K. Ray. Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, 66(Supplement C):198 – 213, 2016.

[2] K. Angrishi. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. *CoRR*, February 2017.

[3] E. Bertino and N. Islam. Botnets and internet of things security. *Computer*, 50(2):76–79, Feb 2017.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645 – 1660, 2013. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond.

[5] B. Krebs. Krebs on security. `https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/`, August 2017.

[6] A. Noroozian, M. Korczyński, C. H. Gañan, D. Makita, K. Yoshioka, and M. van Eeten. *Who*

*Gets the Boot? Analyzing Victimization by DDoS-as-a-Service*, pages 368–389. Springer International Publishing, 2016.

[7] B. Schneier. A Security Market for Lemons. `https://www.schneier.com/blog/archives/2007/04/a_security_mark.html`, April 2007.

[8] B. Schneier. Information Security and Externalities. `https://www.schneier.com/blog/archives/2007/01/information_sec_1.html`, January 2007.

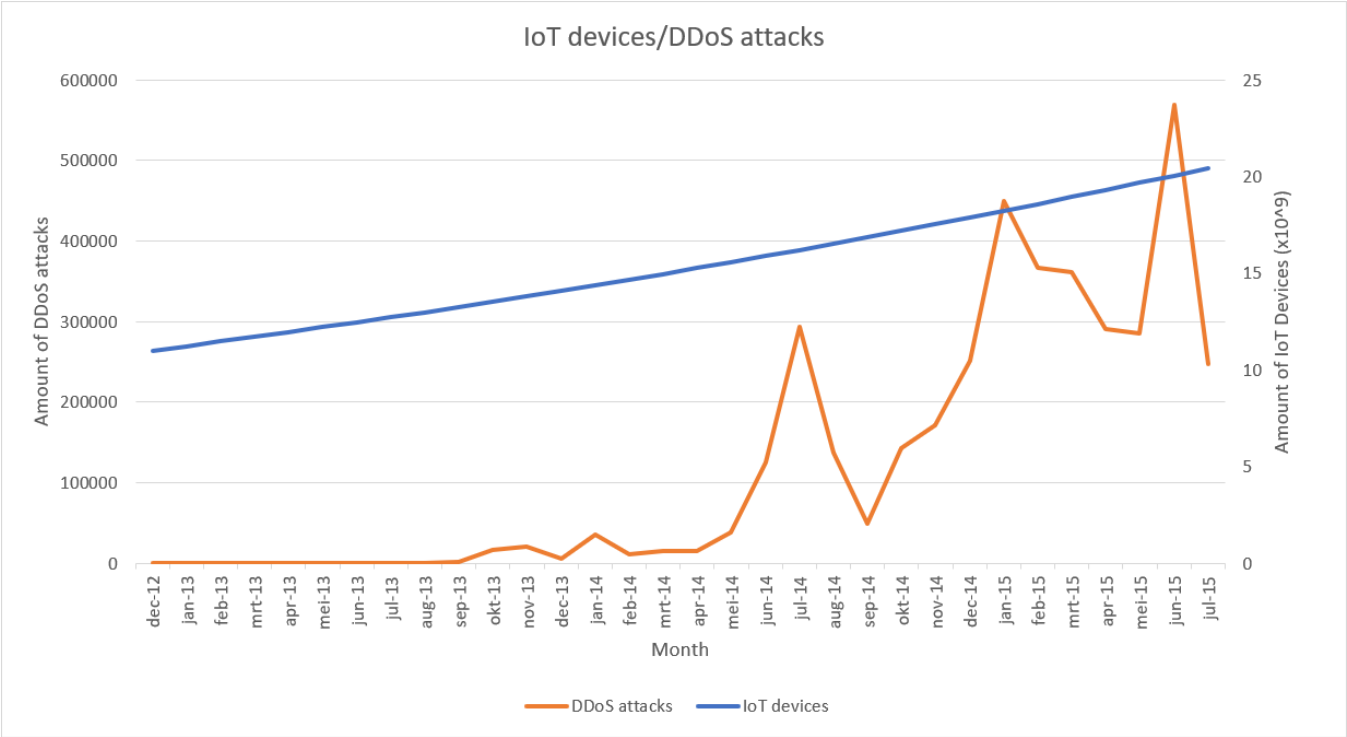


Figure 1: Estimated number of IoT devices per month and number of DDoS attacks

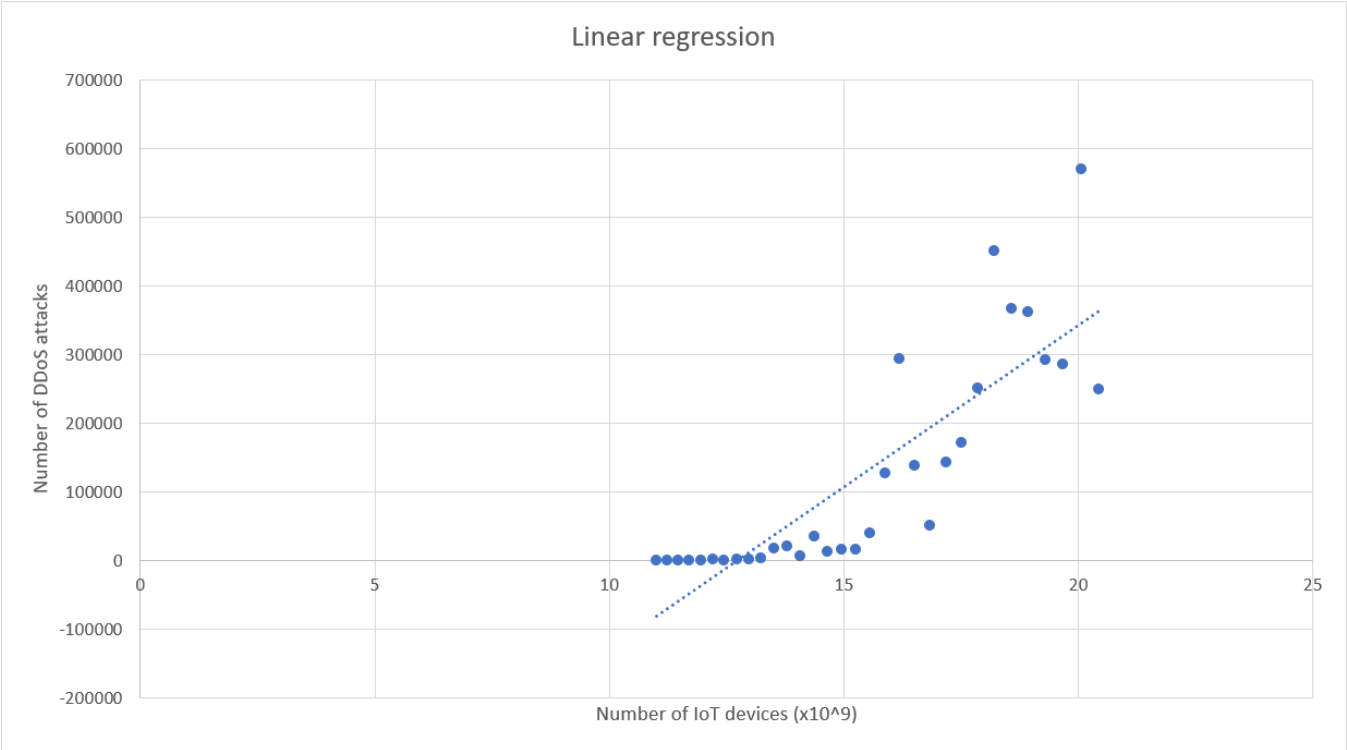


Figure 2: Linear regression of number of IoT devices vs number of DDoS attacks