Economics of Cybersecurity Block 4
Telnet scans

Calvin Hendriks - c.hendriks@student.utwente.nl
Christiaan van den Bogaard - c.h.m.vandenbogaard@student.utwente.nl
Sander Bakkum - s.bakkum@student.utwente.nl
Riccardo Colombo - r.colombo@student.utwente.nl

October 21, 2019

1 Introduction

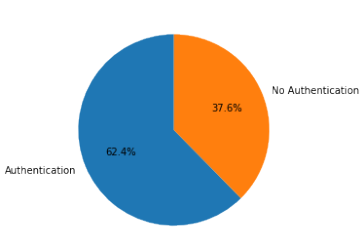
In previous assignments, we discussed the security issue behind telnet scans, the creation of IoT botnets and the DDoS attacks launched from them.

In this assignment, we aim at understanding the factors influencing the variance in security performance in relation to a metric. We will investigate the underlying reasons behind the existence of variances in a metric.

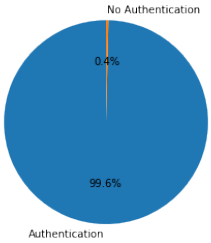
1.1 Metric: vulnerability per ISP

1.1.1 Authentication per hostname

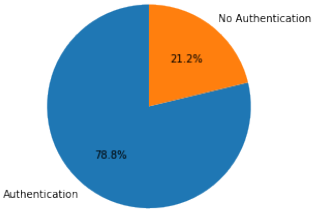
This metric gives insight in the percentage of devices that require authentication when a telnet connection were previously established [1][2]. This means, that these devices are *possibly* vulnerable to Mirai, as it used a dictionary attack[3]. In the devices that do not have authentication, we do not know what is the case. In most cases its either a rejected connection or a whitelist. In the previous assignment, it was the aggregated result over al hosts. This now is separated and the top 5 hosts are shown. It is separated by parsing the hostname and stripping the domains, while keeping the top level domain and second level domain e.g. kpn.nl.



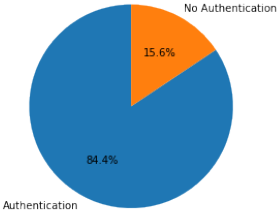
(a) kpn-gprs.nl



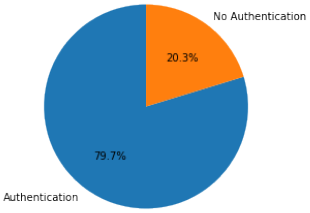
(b) versatel.nl



(c) kpn.nl

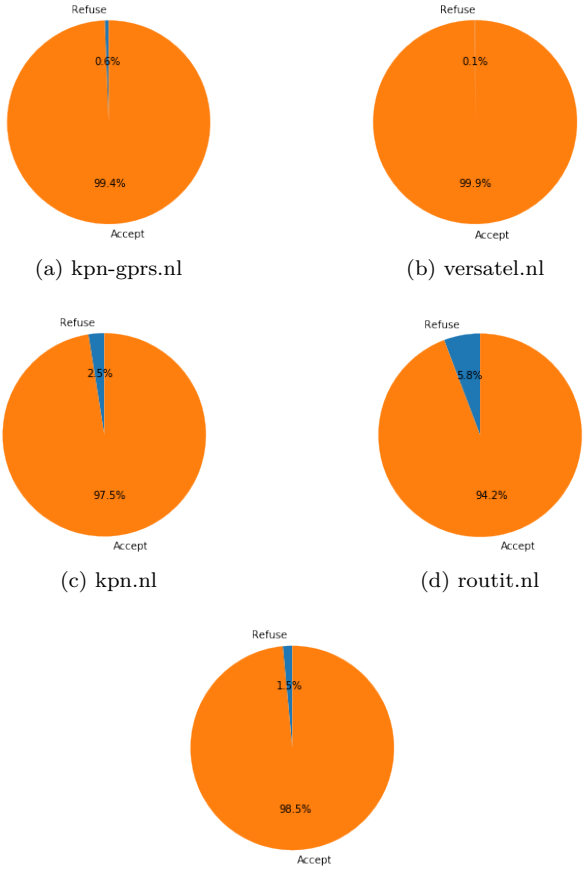


(d) routit.nl



(e) ziggo.nl

Figure 1: Fraction of devices requiring authentication for the top 5 hosts



(a) kpn-gprs.nl

(b) versatel.nl

(c) kpn.nl

(d) routit.nl

(e) ziggo.nl

Figure 2: Fraction of devices accepting the connection for the top 5 hosts

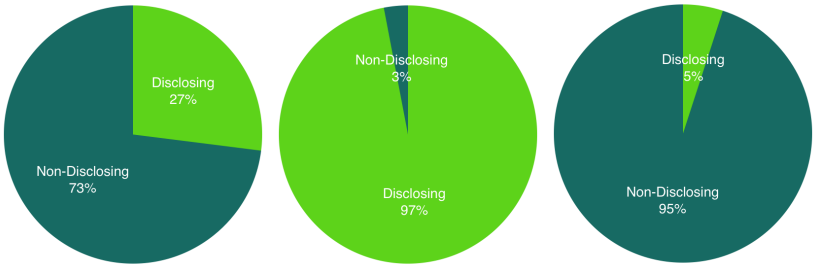
1.1.2 Refused connections per hostname

An important defense mechanism of these devices is whether the connection is rejected. If there is an extra layer of defense in place, such as a firewall, these devices can not be infected to be part of the botnet. Also, this metric was computed over the whole range of hosts, this now is split into the different hosts and the top 3 biggest hosts are shown.

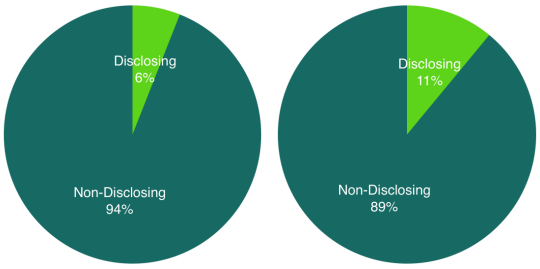
1.1.3 Information disclosure per hostname

Fingerprinting represents an important step in designing a strategy to victimize machines on the internet. Pieces of information such as the operating system and the service running on the host are of extreme importance to determine what vulnerabilities the device is prone to and what exploit tools could be

employed. The metric, as it was designed in the previous assignment, showed the overall percentage of the machines that disclose some kind of information about their running operating system/service. We have now rearranged it to show the percentage of disclosing machines for the top 5 hosts; the results are shown in fig. 3.



(a) kpn-gprs.nl (b) versatel.nl (c) kpn.nl



(d) routit.nl (e) ziggo.nl

Figure 3: Fraction of disclosing IPs for the top 5 hosts

2 Actors involved in the security issue

In this section, several of the actors involved in our security issue are analyzed. We expand upon a possible countermeasure, the costs and benefits involved and the presence of externalities with the proposed countermeasure.

2.1 End users of IoT devices

The end users of the devices are the largest group of actors which do not directly suffer from the security issue. However, with a solid countermeasure this security issue can be mitigated completely. If there are no insecure IoT devices, then no botnet of IoT devices can be created.

2.1.1 Countermeasure: configuring a firewall

The main problem with publicly accessible IoT devices is that they are not behind a firewall. In most cases, customer routers have a built-in firewall but this not correctly used. For example, when UPnP is enabled or ports are forwarded, the IoT devices still are publicly accessible. If this firewall is not present or simply not working, a new customer router should be provided.

2.1.2 Costs, benefits and incentives

The first solution, disabling UPnP will have no direct cost. The main problem however, is that most consumers do not know how to do this or even that they have to do this. The incentive to do this is not present, so this will need to be done by the ISP as the consumer routers are mostly supplied by their ISP. If there is no firewall present, a new consumer router should be requested from the ISP which also does not have direct costs for the consumer. In both cases, there are no direct costs for the consumer. The main issue is that the incentive to request or configure the firewall is not present.

2.1.3 Externalities

A positive externality is that the costs for ISPs for the prevention of DDoS attacks such as IDSs are less as the botnet sizes are shrinking due to better protected devices due to Firewalls. Furthermore, the costs for target companies are less as the DDoS attacks are gradually smaller.

A negative externality is that the costs for ISPs are increasing thus indirectly increasing costs for consumers. The ISPs will possibly need to supply new routers for consumers.

2.2 Internet Service Providers

Internet Service Providers can play a role in the mitigation of DDoS attacks against its customers. Internet Service Providers that offer bandwidth capacities to their customers that are large enough to be able to for example stream high-quality videos have to have a large amount of total bandwidth available (to be divided among their customers). However, while an ISP might have a large total bandwidth capacity, this capacity is tiered down to cities, areas and even blocks of streets. When a customer's home connection is attacked by a sufficiently large DDoS attack, this might affect other home connections on the same street or in the same area as well.

2.2.1 Countermeasure: black hole routing

To mitigate the loss of internet connection for other customers, an ISP could implement a black hole routing mechanism. The ISP would need some kind of detection mechanism to determine that one of their customers (or even a range of customers) is under attack, after which the ISP could simply drop

all traffic with the detected maleficent characteristics to the target IP range until the attack volume decreases. Simply put: all access to a customer's self-hosted service that is under attack is blocked temporarily to protect the internet connection of other customers.

2.2.2 Costs, benefits and incentive

For the ISP, costs are relatively low compared to other DDoS mitigation strategies. A detection mechanism needs to be set up that can either notify a network administrator to approve certain routes to be blocked, or the detection mechanism can control the lower-tier routers automatically so minimal human oversight is needed. The ISP would only have to refund (part of) their fees to a single customer for their experienced downtime, instead of to a significantly larger part of their network. As a fully-automated system primarily requires a one-time investment to develop or purchase and does not require much maintenance, an ISP certainly has an incentive to implement such a system. They could not only significantly reduce refunds for downtime, but also relieve stress on their customer support department during attacks. When an ISP is large enough, the indirect costs related to a DDoS attack outweigh the direct costs of implementation of a black hole routing system.

The direct victim of the attacks is less well off. Their hosted service is blocked for the entirety of the attack duration, thus they would lose all expected revenue for their hosted service during this time period. The factors a potential attack victim would consider are the extra costs involved in hosting their service on an external server with more advanced DDoS protection, the expected profits they would make from their service, and potentially other (vital) services they are hosting from the same internet connection.

For all other customers however, internet access is not affected. They suffer no losses. Prospective customers have an incentive to become part of an ISP that implements a black hole routing mechanism. Firstly because their own connection is protected from attacks against the rest of the network. Also, because their ISP makes less overall costs, the monthly subscription fees to individual customers is kept relatively low.

2.2.3 Externalities

As other customers than the attack victim are not directly involved in the solution, the fact that their network connectivity is unaffected from a DDoS attack can be seen as a positive externality. They benefit from the ISP protecting themselves against DDoS attacks on other customers.

A negative externality that comes paired with a black hole routing system is that this method ultimately does exactly what the attackers intend: denial of service of the target service. If an attacker knows that an ISP implements such a system, they can be confident that their DDoS attack will succeed as long as the traffic volume is high enough.

2.3 Manufacturers

Manufacturers of IoT devices can play a role in the first line of defense against the growth of IoT botnets. As hardware and software flaws are one of the reasons these botnets can grow at all, their role would be to eliminate such flaws in their designs.

2.3.1 Countermeasure: hiring a security consultant

The proposed countermeasure for an IoT manufacturer is to hire a security consultant to analyze their devices for security flaws before these devices go to market. After analysis they would compile a report of their findings, which the developers of the manufacturer can use to secure their designs. Such a report could include security measures from setting random default passwords on a per-device basis, or for example updating software libraries to latest versions to close security holes.

2.3.2 Costs, benefits and incentives

Outside-company security consultants are not cheap to hire. However, with a limited set of devices and possible reuse of hardware and software designs, costs could be kept limited to mostly a one-time investment with some extra incurred costs for every new device brought to market. After a report is made, extra costs are induced by the requirement of extra development time.

Hardware manufacturers have some benefits in increasing the security of their devices. It is possible that securing their devices better reduces the amount of refunds on their products, as hacked devices might be rendered useless and returned to the store. Also, the reputation of a manufacturer can be damaged if their devices are hacked, which could result in a loss of revenue.

However, manufacturers might have a greater incentive to release their devices to market as quickly as possible and for a price that is as low as possible[4]. Depending on the intended market for their devices, IoT device manufacturers will weigh the benefits of the costs of their devices against what consumers will be willing to pay. An average consumer might consider the amount of device features more important than the security level it provides, while for example companies might keep the security level of devices in a higher regard.

2.3.3 Externalities

A positive externality of making IoT devices more secure is the improved conservation of privacy to society as a whole. One could imagine that when IoT-enabled camera systems become more secure, these cannot be inspected from anywhere and by anyone with an internet connection.

Another positive externality is the reduction in the size of IoT botnets globally, reducing the power of maleficent groups of individuals launching DDoS attacks. This reduces costs in DDoS protection needed by companies globally and reduces stress on the global internet infrastructure.

3 Influences on security performance

The actor whose security performance is visible in the metric defined in section 1.1 is the ISP, since most of the second-level domains seen in the data set belong to a ISP. As we can see in the results of that section, there is a noticeable difference in the security performance among the ISPs. In this section, we will define factors causing the variance in the metrics, collect data for said factors and perform a statistical analysis to explore the impact on the metrics.

3.1 Factors

3.1.1 Installed security measures

A factor that could cause variance in metrics could be the presence of other security measures. That is, an ISP is probably more likely to install a security measure when other security measures have already been installed. Therefore, we investigate the internal relationship of the security measures by correlating the metric values.

3.1.2 Location of devices

Another factor that could cause the variance in the metrics is the location of the devices. Some regions have a higher security awareness than others, which could explain why some SLDs have a higher perc

3.2 Data

The data for both factors is extracted from our data set. For each SLD, we calculate the % of devices that require authentication, refuse the connection and disclose sensitive information, just like we did in section 1.1 but now for all the SLDs. An example for the top 5 biggest SLDs can be found in section 3.2. These percentages will later be used as a rank to calculate Spearman's coefficient. Furthermore, we calculate for each SLD the percentage of devices that is in one of the 13 provinces.

Table 1: Metrics comparison per top 5 second level domains

	SLD				
Metric	kpn-gprs.nl	versatel.nl	kpn.net	routit.net	ziggo.nl
% requiring authentication	62.4%	99.6%	78.8%	84.4%	79.7%
% of connections refused	0.6%	0.1%	2.5%	5.8%	1.5%
% disclosing sensitive info	27%	97%	5%	6%	11%

3.3 Statistical analysis

Based on the factors described above, we have set up a number of hypothesis which we are going to explore using Spearman's rank-order correlation, which

measures the strength and direction of association between two ranked variables. Assuming a significance level of 1%, we reject the null hypothesis if $pvalue < 0.01$.

We interpret the correlation coefficient according to the following table [5]:

Table 2: The strength of a correlation

Value of Coefficient	**Meaning**
0.00 to 0.19	A very weak correlation
0.20 to 0.39	A weak correlation
0.40 to 0.69	A moderate correlation
0.70 to 0.89	A strong correlation
0.90 to 1	A very strong correlation

3.3.1 Installed security measures

This section is meant to analyze the correlation between the factors that have been discussed in section 3.1.1.

- Firstly, we investigate whether a correlation between the percentage of devices that require authentication and the percentage of devices that refuses the connection attempt is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices that require authentication and the percentage of devices that refuse the connection.
  - H_1 There is a significant relationship between the percentage of devices that require authentication and the percentage of devices that refuse the connection.

  When computing Spearman's rank-order correlation we obtained the following: $r_s = -0.3020$, $pvalue = 3.9066\text{e}{-38}$. Therefore we can conclude that a weak correlation is present between the percentage of devices that require authentication and the percentage of devices that refuses the connection attempt. Furthermore, such a small p-value is strong evidence against the null-hypothesis.

- Secondly, we investigate whether a correlation between percentage of devices that require authentication and percentage of devices disclose information is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices that require authentication and the percentage of devices disclosing information.
  - H_1 There is a significant relationship between the percentage of devices that require authentication and the percentage of devices disclosing information.

Computing Spearman's rank-order correlation revealed the following results: $r_s = -0.2307$, $pvalue = 1.6129\text{e}{-22}$. The results suggest the presence of a weak correlation between the percentage of devices that require authentication and the percentage of devices that refuses the connection attempt. Moreover, the little entity of the p-value firmly supports evidence against the null-hypothesis.

- Lastly, we investigate whether a correlation between percentage of devices that refuse the connection and percentage of devices disclosing information is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices that refuse the connection and the percentage of devices disclosing information.
  - H_1 There is a significant relationship between the percentage of devices that refuse the connection and the percentage of devices disclosing information.

  The computation of Spearman's rank-order correlation yielded the following results: $r_s = -0.1517$, $pvalue = 1.8541\text{e}{-10}$. We can therefore conclude that a very weak correlation is present between the percentage of devices that refuse the connection and the percentage of devices disclosing information. Furthermore, the little extent of the p-value represents strong evidence against the null-hypothesis.

3.3.2 Location of devices

This section analyzes whether a correlation between the factors that have been discussed in section 3.1.2 is present.

- Firstly, we investigate whether a correlation between the percentage of devices located in province X and the percentage of devices requiring authentication is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices located in province X and the percentage of devices requiring authentication.
  - H_1 There is a significant relationship between the percentage of devices located in province X and the percentage of devices requiring authentication.

As can be seen in table 3, almost none of the p-values are smaller than our level of significance, meaning that that the null-hypothesis for that province cannot be rejected. Only for the province of Noord-Holland, the p-value is very small. However, the correlation coefficient is also very small, meaning that the correlation is extremely weak.

- Secondly, we investigate whether a correlation between the percentage of devices located in province X and percentage of devices disclosing sensitive information is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices located in province X and the percentage of devices disclosing sensitive information.
  - H_1 There is a significant relationship between the percentage of devices located in province X and the percentage of devices disclosing sensitive information.

The results for disclosing information are similar. As can be seen in table 5, for almost none of the provinces, the null hypothesis can be rejected. Only for Noord-Holland and Noord-Brabant, the p-values are small enough to say with high confidence that the results are not based on chance. Even then, the correlation coefficient is so small, that it is at the most a very weak one.

- Lastly, we investigate whether a correlation between the percentage of devices located in province X and percentage of devices refusing the connection is present. Therefore our hypothesis are:
  - H_0 There is no significant relationship between the percentage of devices located in province X and the percentage of devices refusing the connection.
  - H_1 There is a significant relationship between the percentage of devices located in province X and the percentage of devices refusing the connection.

Finally, the results in table 4 show that only for the provinces Flevoland and Noord-Holland, the null hypothesis can be rejected. Again, the corresponding correlation coefficient is very small, meaning that even though we can reject the null hypothesis that states there is no relationship, the found relationship is a very weak one.

Table 3: Authentication

Province	Correlation Coefficient	P-Value
FRIESLAND	0.077	0.001
GELDERLAND	0.056	0.02
NOORD-HOLLAND	-0.104	0.0
OVERIJSSEL	0.036	0.134
ZEELAND	-0.02	0.401
ZUID-HOLLAND	0.036	0.13
FLEVOLAND	0.021	0.377
UTRECHT	-0.009	0.699
DRENTHE	-0.013	0.596
NOORD-BRABANT	0.012	0.63
LIMBURG	-0.011	0.647
GRONINGEN	-0.035	0.147

Table 4: Refuse

Province	Correlation Coefficient	P-Value
FRIESLAND	-0.017	0.479
GELDERLAND	0.025	0.289
NOORD-HOLLAND	-0.088	0.0
OVERIJSSEL	0.047	0.051
ZEELAND	0.051	0.032
ZUID-HOLLAND	-0.047	0.051
FLEVOLAND	0.065	0.006
UTRECHT	0.011	0.645
DRENTHE	-0.01	0.674
NOORD-BRABANT	0.073	0.002
LIMBURG	0.015	0.541
GRONINGEN	0.002	0.94

Table 5: Disclosing

Province	Correlation Coefficient	P-Value
FRIESLAND	-0.004	0.866
GELDERLAND	-0.061	0.011
NOORD-HOLLAND	0.085	0.0
OVERIJSSEL	-0.048	0.045
ZEELAND	0.024	0.316
ZUID-HOLLAND	0.042	0.078
FLEVOLAND	-0.052	0.03
UTRECHT	0.001	0.973
DRENTHE	-0.003	0.899
NOORD-BRABANT	-0.069	0.004
LIMBURG	-0.026	0.278
GRONINGEN	0.024	0.311

4 Conclusion

We identified some of the actors involved in the security challenge of overcoming (IoT-based) botnets. We have shown that multiple actors can act on this problem in different ways, and that they have vastly different incentives to do so. It seems that while manufacturers and device owners do not have much incentive to get involved in the problem, they could play a role. On the other hand, ISPs have a larger financial stake in the prevention of DDoS attacks targeted towards and originating from their network.

Furthermore, we analyzed the statistical significance between factors we found in our dataset of telnet scans. Unfortunately, we did not find any strong correlations between any of these factors.

References

[1] C. Hendriks, C. van den Bogaard, S. Bakkum, and R. Colombo, "Economics of security block 2 telnet scans." [Online]. Available: https://github.com/thechib12/EOS_telnet/blob/master/reports/block_2/eos_assignment1_final.pdf

[2] ——, "Economics of security block 3 telnet scans." [Online]. Available: https://github.com/thechib12/EOS_telnet/blob/master/reports/block_3/Eos_Block_3_group2_final.pdf

[3] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17).*

Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[4] M. McFadden, S. Wood, R. Mangtani, and G. Forsyth. The economics of the security of consumer-grade iot products and servicesthe economics of the security of consumer-grade iot products and services. [Online]. Available: https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

[5] J. Fowler, L. Cohen, and P. Jarvis, *Practical statistics for field biology.* John Wiley & Sons, 2013.