Economics of Cyber Security
Assignment Block 4 - Group 3

Sina Davanian, Oleksandr Shyvakov, Alpha Diallo, Tugce Arican

1. INTRODUCTION

Actors involved in the security issue follow different strategies to mitigate its impact. Security vulnerabilities in internet of things (IoT) devices affects multiple actors but in this paper the focus will be on vendors, Service providers (SPs), and victims of DDoS attacks done using IoT devices. This paper will look at the valid countermeasures that could be implemented by each of the noted actors to mitigate the security issue, and an analysis of the cost and benefits of the countermeasures will be done. The incentives of why the actors would want to implement the countermeasures is explored, and the role of externalities, both positive and negative, are looked at. Lastly, the security performance of vendors is analyzed based on previous metrics chosen.

2. COUNTERMEASURE IMPLEMENTATIONS TO MITIGATE SECURITY ISSUE

Vendors: From a security performance perspective, as discussed in the previous block, vendors are divided into two categories. The first category consists of the vendors that manufacture products without a critical authentication vulnerability but with default credentials. The second category includes vendors that have not invested in a security mitigation strategy. In the previous block we discussed the costs that the second category of vendors face now and we estimated their ROI. In this block we concentrate on the first category of vendors (comprised of all the vendors). The reason behind this choice is the severity of the issue. As a matter of fact, other actors will continue to hurt from externalities resulting from default credential vulnerabilities as long as vendors act irresponsibly in this regard.

The countermeasure for this subset of vendors are updates to firmware which would require unique username and passwords upon first use, and disabling settings by default and letting users turn them on if they want to, rather than having settings turned on by default and expecting users to turn them off.

Service Providers (SP): Service providers themselves can be targeted in DDoS attacks. The most recent Mirai attack targeted a service provider called Dyn. In this attack, the top level DNS server was attacked and as a result famous clients of this DNS server such as Amazon, Paypal and Twitter were taken down, although only temporarily.

A SP in our definition may be a critical server that plays a part in routing internet traffic like a DNS server or an ISP or even a data center. SPs can follow several countermeasures. In a combined effort with the vendors they may track the devices with the default credentials and notify the users to change the credential. Another more preferred approach would be planting sensor nodes in their network to track DDoS attacks. This approach would be based on anomaly detection and SP blocking the DDoS traffic.

DDoS victims: DDoS protection solutions to prevent interruption in business activity have been around for more than a decade. The primary solutions were in the form of pure appliance. The high cost and maintenance effort have derived service-based business models. Recent security providers offer cloud services with DDoS protection for a recurring cost. These DDoS protection programs are countermeasures that victims of DDoS attacks can implement to mitigate the same issue from occurring again in the future.

3. DISTRIBUTION OF COSTS AND BENEFITS OF COUNTERMEASURES AMONG THE DIFFERENT ACTORS

Vendors: Vendors have to invest in writing the code for the vulnerability fixes and firmware update. Moreover the vendors have to enforce updates of the old devices in case they want to fix the problem in a short run. Benefits firstly include more secure devices. More investment in update enforcement would infer more secure devices. Currently due to information asymmetry the vendors cannot maneuver on the decrease on the number of vulnerable devices. However, the recent attacks including Dyn DDoS, that resulted in takedown of famous websites like Twitter and Amazon [10], would probably start off some obligations like publishing the number of devices with default credentials. It is not also unlikely that a service emerges to identify the number of vulnerable IoT devices to default passwords and measures the security of different vendors. In presence of such information symmetry, the aforementioned investment of the vendors could garner more customers. On the other hand vendors' investment in the security of IoT devices has a positive externality effect for all the DDoS victims. It goes unsaid that as more vendors invest, the rest of the vendors are also motivated to invest. This is because as the population of vulnerable IoT vendors decreases, it becomes easier to point fingers to specific vendors. The benefit of vendor investment for ISPs is unclear since the decrease of vulnerable IoT devices may not significantly decrease bandwidth congestion of ISPs.

Service Providers (SP): Service providers, because of the nature of their critical role have to have powerful servers and large bandwidth. Nevertheless the concept of authenticated service for them is hard to define because most of the times they have to serve everybody. Therefore while causing a Denial of service for a service provider is hard to achieve (because of large capacity) it is harder to defend against a DDoS attack when the attacker has the resource to perpetrate one. For a service provider that has a specific server that needs to be protected, off-the-shelf protections such as Arbor APS or Corero SmartWall can be used. However, when it comes to the protection of a WAN network as is the case of an ISP, a protection would become much harder. To the best of authors' knowledge, a kind of protection that can help ISPs to defend their bandwidth against DDOS traffic is not realized yet. Yet there have been several researches and solutions that can be implemented in order to provide such protection. A protection solution for ISPs not only imposes a direct deployment and development cost but also an indirect cost. One element of this indirect cost is the network latency because a further analysis to identify DDoS attacks is required. Moreover a hypothetical solution based on anomaly detection would not be 100% accurate and human supervision would be required. The most obvious benefit for ISP however, is bandwidth optimization. However, it is not yet clear that such

optimization can incentivize ISPs for investment in the protection. That being said in this analysis we formulize the costs and benefits for a service provider that has a commitment to provide a limit of availability.

We assume the service provider (SP) owns a link of V capacity. Moreover we assume that the SP has C customers. We assume these C customers on average use B Megabytes of the SP bandwidth. Based on given parameters, on average U = C * B Megabytes of the SP bandwidth is consumed. In order to perform a DoS attack an attacker would guide E megabytes of traffic. In order to succeed E > V - U. If this condition holds then D=(E- (V-U))/B users will not receive service and the DoS attack harms them. In a real world scenario, the SP offers a P rate of uptime and service availability. If the SP does not meet the minimum rate then it has to compensate the users. For the sake of simplicity, we assume SP offers p=100%. In such case the SP has to compensate D users after a DoS attack. We assume this value for all users is the same it is equal to M. In total the SP loses D*M as a result of a DoS attack.

DDoS victims: The cost for an enterprise to defend against a DDoS attack will be in hiring a DDoS protection firm and retaining the solution. Buying a DDoS mitigation appliance would cost something like $65,000 for the 2Gbps version of Arbor APS up to $160,000 for the 10Gbps model [9]. Corero, another vendor, offers SmartWall TDL product for $250,000 [7]. Other options are cloud protections per server that would cost [$300-$900] monthly [8]. Benefits include protection from potentially damaging business interruptions such as outages of web services that a large group of users would visit.

4. INCENTIVES FOR IMPLEMENTATION OF COUNTERMEASURES

Vendors: We shall assume that information symmetry happens in the near future. As a result vendors benefit from their investment. We shall also assume that vendors rely on users to update their devices. In previous assignment an assumption was made that about 75% of users will apply vendor security patches. The Second assumption will be that it will take 12 month for all the users in this 75% portion to apply the security updates. By applying a normal distribution function the following trend can be seen. During the first 3 months early adopters will do the patch (25% from all users who will apply the patch), from the third to ninth month the general population will apply the patch (50% of the 75%) and during the 9-12 months the remaining 25% of users will do the update. However, we assumed before that only 75% of users will apply the patch. So we can assume that after 3 months 19% of users will apply the patch, after 9 months 56% will have their devices secured and after a year 75%. In order to analyze if the vendor invests we consider a vendor does not and the rest do. As a result we approximate the distribution of the probability of compromise according to users update and see what will happen if the vendor does not invest.

As it can be seen from the figure there are 4 outsiders, whose security posture is relatively weak. Let us see what happens when all vendors but Airties invest in patching security holes in their devices.

Figure 1. Probability of a vendor's device being compromised (PC)

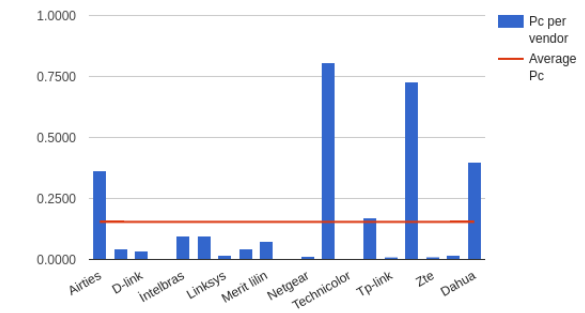


Figure 2. PC 3 month after all, but Airties secure their devices

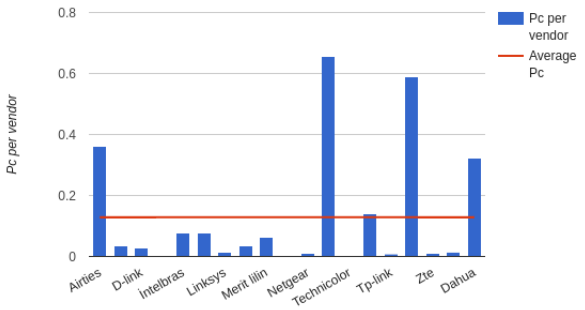


Figure 3. PC 9 month after all, but Airties secure their devices

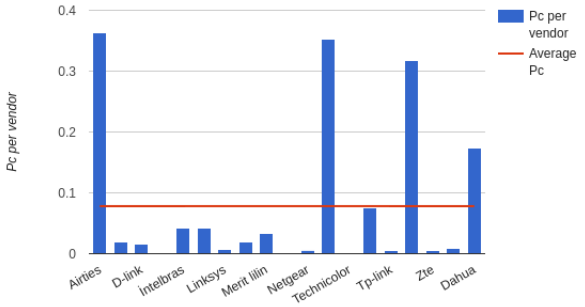


Figure 4. PC 12 month after all, but Airties secure their devices

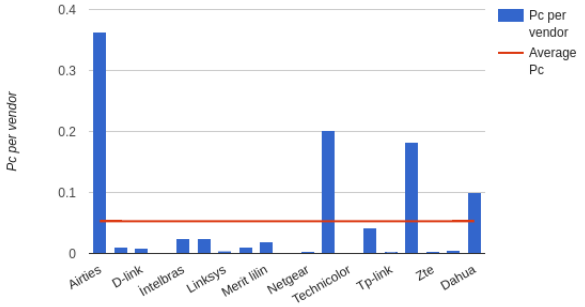


Table 1. Vendor security measures affecting the probability of compromise over time

Pc - probability of an exposed device produced by a particular vendor being compromised

Pc1- Pc 3 months after all the vendors but one secured their devices

Pc2 - Pc 9 months after all the vendors but one secured their devices

Pc2 - Pc 12 months after all the vendors but one secured their devices

vendor	frequency	breached	Pc	Pc1	Pc2	Pc3
Airties	14,253	5,172	0.3629	0.2948	0.1588	0.0907
Asus	63,789	2,698	0.0423	0.0344	0.0185	0.0106
D-link	91,443	3,204	0.0350	0.0285	0.0153	0.0088
Huawei	328,879	512	0.0016	0.0013	0.0007	0.0004
İntelbras	4,458	424	0.0951	0.0773	0.0416	0.0238
İnteno	5,759	558	0.0969	0.0787	0.0424	0.0242
Linksys	23,230	395	0.0170	0.0138	0.0074	0.0043
Matrix	5,000	213	0.0426	0.0346	0.0186	0.0107
Merit lilin	4,463	338	0.0757	0.0615	0.0331	0.0189
Mikrotik	1,320,256	1,192	0.0009	0.0007	0.0004	0.0002
Netgear	166,911	2,179	0.0131	0.0106	0.0057	0.0033
Sangfor	280	226	0.8071	0.6558	0.3531	0.2018
Technicolor	965,449	477	0.0005	0.0004	0.0002	0.0001
Totolink	3,496	599	0.1713	0.1392	0.0750	0.0428
Tp-link	333,116	3,443	0.0103	0.0084	0.0045	0.0026
Upvel	391	284	0.7263	0.5902	0.3178	0.1816
Zte	139,121	1,521	0.0109	0.0089	0.0048	0.0027
Zyxel	314,970	6,077	0.0193	0.0157	0.0084	0.0048
Dahua	781,227	311,294	0.3985	0.3238	0.1743	0.0996

As it can be seen from the Figure 2 to Figure 4, 3 months after vendors apply security controls, the situation for the one who did not invest in it, does not change a lot. However, after 9 months Airtiles Pc will be the highest and after 12 months its probability of compromise will be almost twice as high as the next most vulnerable vendor. So if the vendor does not invest in security it will make him an absolute outsider after a year; And as long as his devices are the most vulnerable, it will result in having more of his devices in botnets. That can result in some lawsuits, media buzz and as a result customers leaving this vendor. However, it is worth mentioning that this is not true for all the vendors. For instance, there are some vendors whose probability of compromise is lower than 10% (e.g. Linksys 1.7%) and even if such a vendor will not invest in security, when all others do it will not hurt them. Because after 12 months its Pc still will be below average and relatively low compared to others.

Service Providers: Based on the loss analysis we did in the previous section we can analyze whether a service provider implements a DDOS protection and how much they are ready to pay. According to [6] by 50% chance, an enterprise would face a DoS attack. Based on this, it is unlikely that a SP accepts the risk. They may invest in a DoS protection program that costs X. This does not remove the risk but reduces the probability of loss. On the other hand they may provide compensation insurance based on their free bandwidth capacity and the number of users that may experience outage. This is like gambling because in case the enterprise experiences a DOS attack, it would be 10 times per year [6] and the value of compensation shall be adjusted based on this. Taking all the factors into consideration, the SP must offer a reasonable P rate of uptime and a low M compensation value because most service providers do not handle small number of users and it is not predictable who will experience outage. In conclusion we believe the Dyn case encourages service providers to invest in DDoS protection because without it, victim investments will not be fully effective.

DDoS victims: DDoS victims have an incentive in implementing the countermeasures due to the losses that they may incur otherwise. The losses incurred by the DDoS victims could be from the revenue loss due to the business disruption such as website

being down, the loss of customers and reputation if the DDoS victim is a provider of an online service with multiple customers, employee productivity loss and payment costs, and decrease in stock market value. An example case of this would be Dyn [1], a Domain Name Service (DNS) provider, that suffered a DDoS attack that is believed to have been conducted using botnets created by the Mirai malware on October 21, 2016. The DDoS attack affected companies such as Spotify, Amazon, AirBnB, and Twitter. Monetary loss due to reputational damage and stock market value losses can be hard to ascertain and can vary greatly so only the losses to customers of Dyn and the internal losses of Dyn, consisting of employee pay and revenue generated, will be considered in the equation below. The customer loss is integrated into the calculation with the assumption that Dyn may be held liable since they were hired to perform a service and that service became disrupted.

$$Total\ Losses\ =\ P*T\ +\ E+\sum_{i=1}^{i} T*C_i$$

T = time offline (hours)

P = Revenue amount lost ($) per hour

C = customer loss ($) per hour

In a survey done in [2], of small and large companies, by Incapsula in 2014, it was found that 49% of the DDoS attacks surveyed lasted between 6-24 hours. In the case of Dyn a status update was provided in [3], stating that the DDoS incident started "at approximately 11:10 UTC and lasted until approximately 17:45 UTC". This fits the range of hours found in the survey. Making some assumptions on the average revenue lost by Dyn and the customer loss per hour, and the total lost from paying employees and contractors to fix the problem, a discrete sample number can be given to show the potential losses that can be incurred from a DDoS attack. The assumed averages for revenue loss by Dyn, customer loss, and total lost from employee and contractor pay are $20,000, $22,000, and $18,000 respectively. These values may be lower or higher, since in some cases like Amazon their losses when there is a disruption could be $31,000 per minute [4]; but from using these numbers along with a count of 1 customer, i=1, the total losses incurred by the DDoS attack is TL = ($20,000*6)+($18,000)+(6*$22,000) = $270,000, which is a generous estimate.

While the amount calculated might not be much for a large company making billions in revenue per year, for a small company it can be damaging. The incentive for potential DDoS victims to implement the countermeasure is enabling business continuity should they be targeted, and the cost of the countermeasure will be minimal compared to the possible losses incurred from the DDoS attack.

5. ROLE OF EXTERNALITIES SURROUNDING SECURITY ISSUE

Positive Externality: Vendors investment in solving the security issues causes the first source of positive externality. On one hand, each new vendor who invests motivates others to invest because of competition. On the other hand, the vendors' investment leads to overall better security of both the end users and DDoS victims.

Service providers investment for security affects the whole internet. Depending on the role of service provider (DNS, Data center, backbone router) a number of stakeholders will be affected. Although their investment would be due to other incentives (mentioned in the previous section) their deduced security will defend the DDoS victims and also vendors' reputation. The former is due to the fact that even if DDoS victims invest in security but their service provider is vulnerable, they still hurt from a DDoS attack launched against a different target. The latter is due to popularization by the media after a massive DDoS attack happens. For instance in recent Dyn DDoS attack, the reputation of IoT vendors harmed more than Dyn itself since most critics pointed fingers to the vendors. As a result an investment by service providers would also protect the reputation of vendors.

Negative Externality: Vendors lack of security controls on the IoT devices they create would harm the owners of these IoT devices especially when we speak about targeted attacks. It takes one vulnerable IoT device to pass a very powerful firewall organization. This is because for instance a smart TV in an employee office may be connected through an internet modem. The employee may be connected to the TV with his laptop and the laptop may be connected to the company via a network cable. An attacker can easily access the corporate network through the smart TV and the laptop if these devices are vulnerable. Although this is possible most of the recent attack were not targeted attacks and the IoT devices were just abused to attack other victims. It is crystal clear that the defect in vendor devices has resulted in the final damage to DoS victims.

The negligence of the vendors to provide proper security controls can make governments get involved which could cause new regulations to come about that can stifle innovation being made by other IoT device vendors. These new regulations could also have an effect on users whose devices may get blocked since the regulation could make it so that ISPs can designate devices as unsecure and block them from making any connection to their networks [12]. The question in regulations such as this would be what unsecured devices are defined as. As well as what the process would be in blocking these unsecure devices; would the owner of the device be warned beforehand so they have the opportunity to fix the changes?

Another negative externality is the IoT owners' indifferent attitude toward their security and leaving the default credentials that have harmed other players. Up until now, default credentials for hardware and even software installation has been a common practice. Vendors always warn users and they count on user awareness to change the credentials. The recent attacks have harmed vendors' reputation mainly because the users of IoT devices are extensively unaware and indifferent about the risks. For instance a user may understand the risk of having a weak password for her laptop but cannot imagine the damage from leaving her smart tv credential intact. From her perspective, the TV still works even if somebody else has the credential and she accepts such risk. However, users' insecure behavior has resulted in the denial of the service of famous market players like Amazon. Due to this damage to big players such as Amazon now vendors have to pursue a mitigation plan for such risk.

Another negative externality is the increase in the sale of DDoS protection providers as the number of DDoS attacks grow. In other words, the more vendor devices vulnerable the higher enterprises invest in DDoS protections. The same goes for ISP lack of defense against DDoS. The less ISPs defend themselves against traffic congestion, the more other players have to invest.

6. SECURITY PERFORMANCE OF ACTOR VISIBLE IN THE METRIC(S)

The actor that we are working on is the vendor and we defined their performance based on the probability of compromise. We believe fame of the company derived the better security performance. Although fame is not a tangible asset to measure there are other factors that can help us indirectly measure the impact of the companys fame. A very simple factor is the age of a company. Although this is a simple factor it says much about the company. First longer age shows that the company is not a startup anymore and second it shows the number of years the brand had a chance to enrich the market. The second factor, that we believe is related, is the number of reported CVE vulnerabilities for a vendor e.g. number of vulnerabilities attributed to linksys. This factor supports our argument about the security performance in two forms. First the more a company has vulnerabilities, one may argue that the more security research investments made to find these vulnerabilities for the product. The more number of reported vulnerabilities not only induces better security in a way but also infers the vendor attractiveness and popularity.

Table 2 reports our measurements of the factors from CVE database[5] and company profiles. At the first glance it seems these factors have actually a correlation with their number of compromised devices. For instance companies like Sangfor and Dahua with the lowest number of reported vulnerabilities (0 to 6) are actually those with the highest probability of breach. The same holds for the companies with the lowest probability of breach.

Table 2. Factors involved in # of breaches

Vendor	Frequency	Breached	#Vulnerabilities	Age
Airties	14253	5172	3	12
Asus	63789	2698	28	27
D-link	91443	3204	77	22
Huawei	328879	512	148	29
İntelbras	4458	424	0	40
İnteno	5759	558	0	26
Linksys	23230	395	64	28
Matrix	5000	213	1	28
Merit lilin	4463	338	2	26
Mikrotik	1320256	1192	2	20
Netgear	166911	2179	59	20
Sangfor	280	226	0	16
Technicolor	965449	477	6	12
Totolink	3496	599	0	7
Tp-link	333116	3443	16	20
Upvel	391	284	0	6
Zte	139121	1521	18	31
Zyxel	314970	6077	58	27
Dahua	781227	311294	6	15

To investigate age and number of vulnerability factors, the data given above divided into two groups for each factor. For age division, 25 years has been chosen for division. Same division has been done for the second factor. Average number of vulnerabilities has been chosen. The result is shown in Table 3 and Table 4.

Table 3. Vendors grouped based on age

	Age<=25	Age>25	Total
Breached	328070	12736	340806
Non-breached	3348752	876933	4225685
Total	3676822	889669	4566491

Table 4. Vendors grouped based on vulnerability

	# of vuln.<35	# of vuln. >35	total
Breached	326348	12367	338715
Non-brached	3300326	913066	4123392
Total	3626674	925433	4552107

Odds ratio is defined as the odds of success given that a certain condition exists divided by the odds of success given that a different condition exists. If the ratio is 1, events have the same probability. While it is greater than 1, first event is more probable. Odds ratio is calculated according to following formula.

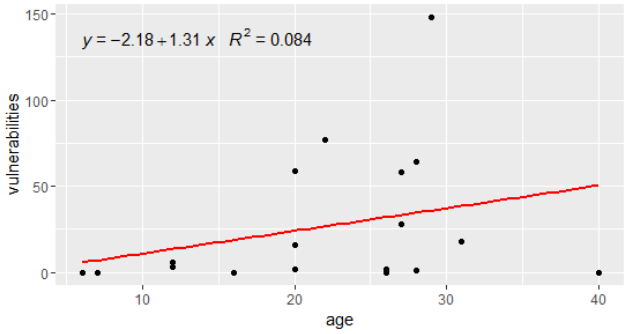
$$ODDS = P(Breached)/P(Non\text{-}Breached)$$

Odds ratio for each factor have been calculated, and the following results illustrates that the vendors younger than 25 years have higher breach probability than older ones. Same results can be seen for vulnerabilities factor.

$$ODDS_{age} = 6.92 \text{ , } ODDS_{vuln.} = 7.53$$

In order to investigate the relation among breach probability, number of vulnerabilities, and age, linear regression has been used. The plot below illustrates the regression between age and number of vulnerabilities factors.

Figure 5. Regression between Age and vulnerabilities



R^2 is a linear regression quantifier that defines the goodness of fit. If you put the same data into correlation, the square of correlation coefficient r might equal R^2 from regression[14]. Moreover, the slope of the regression line is used to test the significance of a linear relationship between x and y[15].

According to this information, correlation coefficient can roughly be calculated as the square root of R^2. Slope of regression line is easily calculated by taking the derivative of the equation given in the Figure 5 with respect to x.

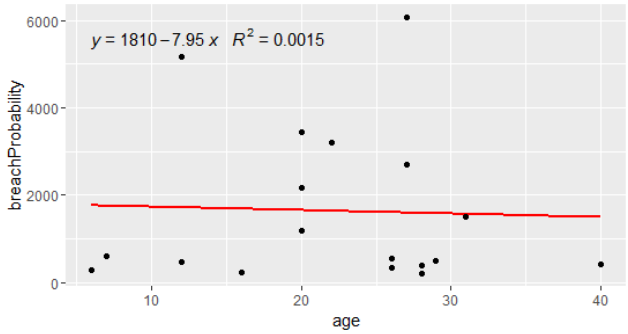
Correlation coefficient: $\sqrt{R^2} = r$

$\sqrt{0.084} = 0.29$

Slope of regression line: 1.31

The values show that age of a vendor and number of vulnerabilities, the vendor have, have a positive correlation with the correlation coefficient 0.29. Figure 6 shows the regression between age and breach probability of vendors.

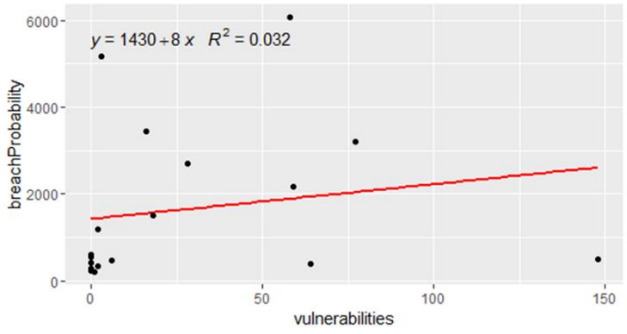
Figure 6. Regression between Age and Breach Probability



By using the equation and R^2 value, correlation coefficient has been calculated as 0.038. This means that there is almost no correlation between age and breach vulnerabilities. However, the slope of the regression line is negative. It says the breach probability of a vendor might tend to decrease while the age is increasing.

Figure 7 illustrates the regression between number of vulnerabilities and breach probability of vendors.

Figure 7. Regression between Number of Vulnerabilities and Breach Probability



According to definitions given before, correlation coefficient has been calculated as 0.17. The value represents quite small correlation between number of vulnerabilities and breach probability of a vendor. However, according to the regression line, breach probability tends to decrease while the age of vendor increases.

7. Conclusion

This paper looked at the valid countermeasures that could be implemented by vendors, service providers, and victims of DDoS attacks to mitigate the security issue, and an analysis of the cost and benefits of the countermeasures for each of the actors was given. The incentives of why the actors would want to implement the countermeasures was explored, and the role of externalities, both positive and negative, was reviewed. Lastly, the security performance of vendors was analyzed based on the vendors age and the number of reported CVE vulnerabilities for the vendor. A linear regression test was done based on the age and number of vulnerabilities for a vendor, the age of the vendor and the breach probability for the vendor, to see if there were any correlations between these variables.

8. REFERENCES

[1] http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_attack/

[2] https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

[3] https://www.dynstatus.com/

[4] http://www.forbes.com/sites/kellyclay/2013/08/19/amazon-com-goes-down-loses-66240-per-minute/#79e414c33c2a

[5] http://www.cvedetails.com/vendor-search.php

[6] Aberdeen Group. (2016, March). Quantifying the Risk of DDoS Attacks for the Traditional ... Retrieved October 24, 2016, from https://www.arbornetworks.com/images/documents/aberdeen-quantify-ddos-risk.pdf

[7] http://www.securityweek.com/corero-launches-new-ddos-protection-appliances-service-providers

[8] https://www.worldstream.nl/ddos-shield?gclid=Cj0KEQjwnKzABRDy2pb7nPSazdsBEiQAI4lZQGWi94kAUIC56bNF6qRHl8bsvTzocDS-j-NhZkHgH_IaAi728P8HAQ

[9] http://www.networkworld.com/article/2203027/network-security/data-center-anti-ddos-package-on-tap-from-arbor.html

[10] http://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html

[11] https://www.cvedetails.com/vendor/833/Linksys.html

[12] http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CD1BBB25-83E0-494D-B7E1-1C350A7CFCCA

[13] https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

[14] https://www.graphpad.com/support/faqid/1141/

[15] https://www.chegg.com/homework-help/definitions/slope-of-regression-line-31