Economics of Cyber Security
IOT Mirai Botnet Economics - Group 3

Sina Davanian, Oleksandr Shyvakov, Alpha Diallo, Tugce Arican

1. INTRODUCTION

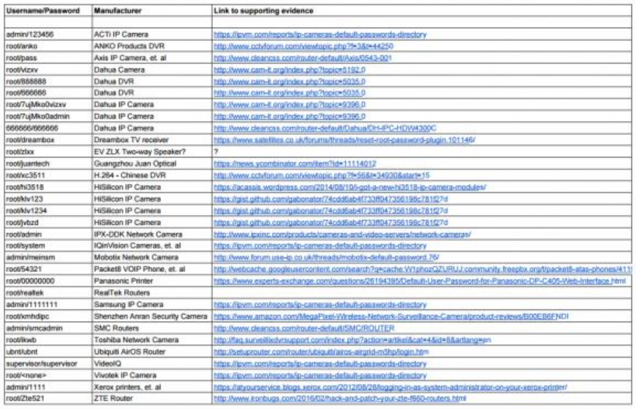
The innovation of IoT is still at a relatively early stage of development, and the development of IoT devices is mainly lead by start-ups and companies that have not been around for long. These companies often mainly depend on the success of one product or service. Especially in IT business, where young companies are willing to accept high risk to gain a market share as soon as possible [7]. Moreover, creating cyber security in IoT products or services might be costly, and this cost may be more than the cost of anything that may happen if the risk is left unattended. Therefore, vendors choose to accept the potential risks, and try to find a way in order to avoid secondary losses due to risk acceptance such as loss of reputation or losing competitor positions. That being said, our dataset shows bots (compromised devices) are from both startups and famous vendors who have been in the market for years. Our security performance analysis shows a meaningful difference between the security strategies of famous and unknown companies. In the rest of this paper we analyze the security performance and then correspondent security strategy of vendors. We then discuss the security strategy of other actors and what they can do based on the security strategy. Finally we analyze the case study of Dahua and their ROSI based on their new security strategy from two perspectives and we conclude the paper.

2. PROBLEM OWNER OF THE SECURITY ISSUE

The effect of the vulnerability of IoT devices goes beyond one stakeholder. Starting from the end-users this issue not only compromises the security of the device and the organization itself but also may legally make the organization responsible for being involved in a DoS attack. Lack of security harms the reputation of a vendor. This is acceptable as long as all vendors provide loose security but as soon as one vendor decides to provide security, other vendors profits may decrease. On the other hand victims of DoS attacks by a botnet of IoT devices clearly are hurting from this security issue. As mentioned by the developer of the botnet, ISPs bandwidth would be occupied as a result of the botnet communication and thus ISPs are the other stakeholders [3]. From a big picture it is also not hard to imagine that even state authorities may hurt from this problem. Assume that a state filters the traffic from outside the state to critical infrastructures because of a cyber war threat. A huge number of compromised IoT devices forming a botnet in a state can act as insiders and make a DoS attack against critical infrastructures possible. That being said we narrow down our focus on vendors. Vendors see strong incentives since now it is publicized that some vendor devices have been responsible for DoS attacks and this results in legal issues and also customer lost.

3. METRICS AND SECURITY PERFORMANCE DIFFERENCES

From our previous metrics we noticed that attackers are not focused on any specific vendors. They tend to attack a set of most used devices with default credentials with approximately the same frequency. As it can be seen from Figure 1 of the credentials used in the released Mirai source code, bots were using a list of 68 default credentials in order to attempt logins.



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Figure 1: List of default username/password pairs used by manufactures

Yet after release of the Mirai source code, most reviewers started blaming a vendor called "Dahua" because of several severe vulnerabilities that allowed this massive breach. However, our dataset shows just one instance of this device being compromised! This peculiar inconsistency motivated us to review our analysis of the dataset. Looking for an answer, we started learning about the Dahua devices banner. Further investigation revealed that Dahua business model is B2B and Dahua does not sell product to end customers. In other words, there is no Dahua device brand in the market that a user can order. Users have to buy the device from Dahua partners with names like "H.264 DVR". This is the reason that searching for "Dahua" in the banners does not lead to any meaningful result. In order to find the number of breaches for the most vulnerable devices we extracted the frequency of similar banners and from that we were able to find the banners that H.264 DVR and NETSurveillance WEB (two partners of Dahua) use. Numbers for these devices compromise are 173186 and 138108. For the rest of the analysis we use the sum of these two numbers as the number of Dahua products breaches.

The number of breaches is huge however it only makes sense when it is combined with the number of Dahua devices in the market and also in comparison with other vendors. Based on this we define the metric "Vendors breach probability" to measure the vulnerability level of a vendor. The security of a vendor is in negative correlation with this metric. In order to calculate this metric for each metric we define "Population size" of a vendor and we collect this data from Shodan. In addition we define frequency of breach based on the total count of a vendor bots from scan dataset. In summary:

$S(x) = Population\ size\ of\ vendor\ x$

$B(x) =\ Number\ of\ breaches\ for\ vendor\ x$

$PB(x) = Probability\ of\ breach\ for\ vendor\ x$

$$PB(x) = \frac{B(x)}{S(x)}$$

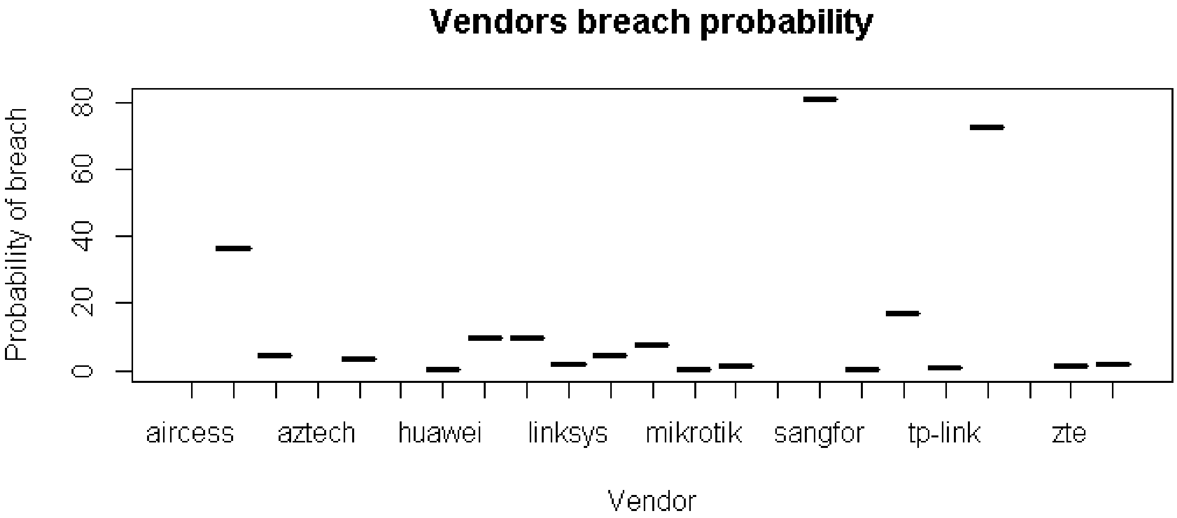


Figure 2: Security comparison of vendors based on probability

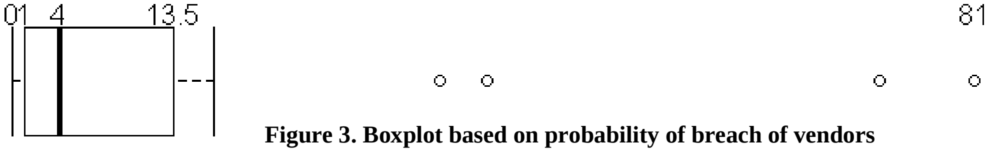


Figure 3. Boxplot based on probability of breach of vendors

Figure 2 shows different vendors probability of breach. The figure suggests low variance and relatively similar probability of breach for different vendors. In order to analyze more precisely we look at the boxplot shown in Figure 3.

From Figure 3, 3 sets of vendors can be observed. Vendors that are in first 2 quartiles and they have a PB of less than 4%, vendors that are scattered in the last 2 quartiles and out layers. Using Figure 2 we can see that vendors that are in the first 2 quartiles are actually famous companies like Linksys, huawei, microtic, tplink, asus, matrix and zyxel while vendors in the last 2 quartiles are mostly not famous. On the other hand closely examining out layers from Table 1 we see two types of vendors. Vendors with big market shares and high probability of breach and vendors with tremendously small market share.

Table 1. Outliers with high probability of breach

Vendor	Market size	breaches	PB
airties	14253	5172	36
Dahua	781227	311294	40
sangfor	280	226	81
upvel	391	284	73

Our analysis of the vendors breach probability shows meaningful difference among vendors. Firstly it confirms that famous companies (Dahua being an exception) have relatively better security probably because there has not been any severe vulnerability. Secondly, it shows that only a few vendors have extremely high probability of breach and out of these few only two vendors have a high share of the market. The high probability of breach is not by chance and Dahua products have several authentication vulnerabilities. Putting all the pieces together we can conclude:

- Companies' security are correlated by their reputation. Famous companies invest more on their security since lack of security can significantly hurt their brand name.
- Dahuas lack of security may be attributed to their Business model. Since they do not sell products to end customers, the customers do not know Dahua name and this may have led to company indifference attitude toward the security of product, transferring the problem to their business partner.

4. SECURITY ISSUE OWNER RISK STRATEGY

Based on the aforementioned conclusion we categorize the past security strategy of vendors based on their PB:

1. $PB(x) \leq 14\% \rightarrow$ $\textit{the company has had a mitigation security strategy}$
   - The company invests on security based on its budget and reputation
2. $PB(x) > 14\% \rightarrow$ $\textit{the company has had a transfer or acceptance strategy}$
   - Small companies probably accepted the risk with the hope that they penetrate mass market and later on they invest.
   - Big companies probably had transferred the risk. This especially seems plausible for Dahua since the user contact is their business partners and the vulnerability cannot directly be attributed to the Dahua name.

5. OTHER ACTORS WITH RESPECT TO SECURITY ISSUE

Other actors that can influence the security issue of authentication vulnerability are the consumers, governments, and ISPs. Consumers are the final users of the IoT devices made by the vendors and as such they integrate them into their networks relying on the fact that the devices are secure. If consumers decide that they do not want to buy devices that have no sort of authentication mechanism in them or if the authentication mechanisms are weak then the vendors will lose money from that, affecting their revenue. In this case the vendors will be forced to implement better authentication mechanisms so that they would not lose anymore revenue.

Governments can have an effect on the security issue by making legislation. The legislation could be one requiring that vendors implement authentication mechanisms in those devices that do not have any and unique credentials on the devices that do have authentication mechanisms but are not strong enough and are widely used in all the same devices.

ISPs can have an effect on the security issue as based on the recent DDoS attack on the krebsonsecurity.com site. The DDoS attack utilized IoT devices that were turned into botnets to attack the site. Since, the bandwidth usage by the botnets may affect traffic through the ISP, the ISPs can mainly take part by filtering the malicious traffic. This can be done either by filtering the botnet traffic based on an extracted signature or based on an unusual traffic flow. The former needs investment in human analysis and reactive reactions while the latter needs investment in behavioral based intrusion detection systems.

6. Risk Strategies

When it comes to the security strategies that can be employed by the problem owner and other actors affected by the security issue of authentication vulnerability on IoT devices there are four types of categories that the strategies can fall into. These categories are risk acceptance, risk reduction or mitigation, risk avoidance, and risk transfer. In risk acceptance the actor does not do anything about the risk and decides to accept whatever consequences occur from the risk. In risk mitigation the actors take steps to reduce the impact of the risk. In risk avoidance the actors do everything they can to avoid any exposure to the risk. In risk transfer the actors hand the risk off to a third party that is willing to accept the risk. Strategies in each category have their pros and cons which are explored below in relation to the actors choices.

6.1 Risk Acceptance

In risk acceptance the pro is that the actors do not have to spend any money at all unless the risk actually becomes a reality. In other words, the actor anticipates a loss value that is manageable and prefers to act permissively. The con is that once the risk does come about the losses could potentially be more than what was expected.

Based on security performance we discussed earlier it seems vendors accepted the risk of default password. Vendors can choose to accept the possible risks because of the severity of the risk. A default credential vulnerability may be considered high however its impact may be considered low. Default credentials vulnerability has been observed to be around for a while as evidenced by the research described in [6], which was conducted in 2012. Yet many vendors chose not to fix the vulnerability probably because of the perceived low impact of the default credential vulnerability. As discussed earlier the vendors exposed asset to device vulnerabilities is Reputation. Default credential vulnerability can be justified by user fault and it does not directly affect the vendor. Moreover, as our security performance suggests in case the device does not have another severe vulnerability and is well hardened the probability of breach is less than 1%. Considering all of these, default credential on IoT devices has been considered as low risk and has been accepted by vendors.

Consumers can choose to accept the risk that comes with their IoT devices having default or no credentials, but there are two kinds of consumers in this case; those who know they are accepting the risk and those who do not. Those who know have an idea of the potential consequences that the risk of having default or no credentials causes, which can range from their devices being used in DDoS attacks, to a disruption in their network if an attacker is able to get inside, and the scale of this ranges from small (home network) to large (enterprise networks). Those consumers who do not know that they are accepting this risk are the ones who think that having the default credential is enough or that it is strong enough, basically those who do not have any knowledge of security.

Governments have been accepting the risks associated with the security issue but mainly due to the fact that the technology is new and whenever there is a new technology legislation is slow to be implemented or changed. Even though governments have been accepting the risks, they have to start making changes due to the fact that more and more of these IoT devices are being integrated into infrastructure such as smart grid where Supervisory Control and Data Acquisition (SCADA) systems and IoT devices are integrated. The cost and consequences associated with accepting the risk for governments could be more than if governments used another strategy since people's lives have to be taken into consideration, since SCADA systems are used in oil and pipeline systems, water treatment, and other critical infrastructures.

6.2 Risk Mitigation

Vendors may choose Mitigation strategy especially when it comes to more severe risks. Most well-known companies have almost the same breach probability. This suggests that the reason for the compromise for these vendors is leaving default credentials by the users and not any other severe vulnerabilities. Comparing these companies Probability of Breach to that of Dahua shows a meaningful difference when the company does not follow risk mitigation for severe risks. As mentioned Dahua products have been exploited more because of a vulnerability in changing the default password. If the user changes the password from the web interface, the credential of telnet/ssh will not be updated. This is a severe vulnerability that is left unattended. As stated by Zach Wikholm from Flashpoint Intel:

> " The issue with these particular devices is that a user cannot feasibly change this password. The password is hardcoded into the firmware, and the tools necessary to disable it are not present. Even worse, the web interface is not aware that these credentials even exist." [2]

The pros of having a risk mitigation strategy is that it gets the organization to be more aware to the possible problems they could have, resources could be used more efficiently, and the eventual losses due to a risk coming true are greatly reduced. The con of risk mitigation is that although money may be spent to try to reduce the risk of something happening, the risk that is being mitigated for may never happen and instead a risk that was not being mitigated may occur.

One risk mitigation strategy vendors can use to mitigate the risks present in authentication vulnerability in IoT devices is to get rid of default credentials and require users to set up strong unique ones. As it can be noticed recently some vendors actually realized the need for exactly this security measure and started to demand users to create a unique password after the first login in order to use the device. This shift in mitigating this risk instead of accepting it can be attributed to the change in their prospective into the impact of the default credential vulnerability; the impact may be in future lawsuit cases.

With today's IoT device capabilities they can be easily used to attack a critical infrastructure; and the creation of botnets consisting of these devices will continue as long as attackers are able to leverage the default credentials of these devices to gain access to them. Governments can drastically mitigate the problem from the legislation prospective by issuing laws which will force manufacturers to ship devices with unique default credentials or to prohibit the usage of devices with unchanged factory passwords. Fines can be applied to the ones who are not following the rules. Some security experts think that government intervention that will force IoT vendors to take security more seriously is the only security measure that can solve the issue as is evident by Bruce Schneier's argument that "the universe of IoT will remain insecure and open to compromise unless and until government steps in and fixes the problem" [1].

Customers may only choose Risk mitigation only if they are aware of a meaningful risk and also they can mitigate the risk on their own. First of all consumers are not really concerned about security and do not want to spend some extra time on it. Second of all some devices just do not have a possibility to change the telnet password. The password is hardcoded into the firmware leaving users no solution but changing the device. This means customers cost for risk mitigation is dependent on the vendor. For vendor the customer can easily mitigate the risk by changing the credential while for another the only choice is to not expose their IoT devices to the outer internet unless it is really necessary by placing them against firewalls, and disabling remote managing ports (telnet and ssh). However, a lot of users are not technically skilled to do this.

IoT botnets create a huge problem for the modern world and ISPs are ones who suffer a lot from them. However, ISPs can take measures from their side in order to reduce the botnets size. Together with the Mirai malware code, its creator published some interesting info. "So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISPs been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping" [3]. As it can be seen after the record 620Gbps DDoS on Brian Krebs website some ISP started to take prevention measures. Which resulted in the reduction of the botnet herd from ~380k to ~300k. The attack on Brian Krebs website happened on the 20th of September and the source code was released on 30th of September. So it took about 10 days after the incident to reduce the botnet herd by 20%. Unfortunately, the data set that was in possession does not cover any dates after the 13th of September, so it was not possible to correlate ISP countermeasures data in the datasets. ISPs can look at which devices use default/no credentials and block their traffic.

6.3 Risk Transference

The pro of risk transference is that the actor is no longer responsible for dealing with the risk since the responsibilities of dealing with the risk would fall on a third party. This is especially useful for companies that may want to focus only on their main business rather than also worrying about dealing with security risks, in which they may not have any experience in. The con of this is that even if the risk is transferred, if the risk does come about it will still have an effect on the actor; since there will be a disruption in the business, such as websites being down, or dealing with insurance if the third party that accepted the risk was an insurance company.

In the case of the authentication security issue in IoT devices, risk transfer applies only when there is a contract between the vendor and another party. For default credentials, vendors may have thought they transferred the risk instead of accepting it. If the vendor does not mitigate the risk, the users still can change the default credentials and this may be the vendor reasoning not to mitigate the risk. While it could be said that the vendors transferred the risk over to the customers, that would just be risk acceptance, since in the end if something happens the customers could go after the vendor. The only way that vendors could transfer the risk is having a term in the device usage terms mentioning that the user agrees to take responsibility for anything that might happen in case she does not change the default credential. Regarding Dahua authentication vulnerability, risk transfer would have been the case if Dahua had mentioned the risk in their contract with their business partners.

Consumers can transfer the risks, such as DDoS attacks and system intrusion, associated with the security issue to a third party that can help to prevent any of the possible consequences of the risk. The third party then becomes responsible for any possible losses that may occur, since the consumer will be paying for the services. This strategy will not work for single consumers though, so businesses (medium to large) are the ones likely to use this strategy.

Not all ISPs can transfer the risk, however, ISPs which are located closer to the victim of the DDoS attack can use anti DDoS cloud based providers. It is known as the first line of defense and can effectively filter out malicious traffic before redirecting it to ISP service. An example of a provider of this service for ISPs is Corero.

6.4 Risk Avoidance

The pro of risk avoidance is that the actor eliminates any potential exposure to a risk either by not going through with something that would bring about the risk. In some cases though it may not be possible to avoid the risk. The cons of risk avoidance are that the costs associated with the strategy are usually very high compared to other categories, since it may mean not going into a business. Also, although an actor may think that a risk has been avoided, things are always evolving and a risk that has been avoided before may come up in a different form.

For the vendors to be able to avoid any risks associated with default or no credential authentication mechanisms on IoT devices, they would have to drop out of the business. This is because although they may implement these authentication mechanisms on newer devices and send out firmware updates for older devices, there is no guarantee that all the users of those IoT devices will buy the new devices or upgrade the firmware of the old devices that they have. So, there is always the risk of someone managing to gain access to the vendors older devices and using it for malicious purposes.

Governments cannot avoid the risk unless they ban the usage of all IoT devices, which is not likely. Neither can ISPs, since there will always be the chance of some attackers using these IoT devices to generate large amounts of traffic to make things hard for the ISPs.

7. Return on Security Investment (ROSI)

7.1 Mitigation Strategy based on vulnerable device replacement

Out of all the risk strategies the one where vendors roll out the security firmware updates is chosen for this section. Up until now vendors have not had to worry much about implementing strict security authentication mechanisms on the IoT devices that they sold, even though they would say that security is of the utmost importance for them. Since, the DDoS attack on the krebsonsecurity site, and the release of devices that were part of the botnets there have been more talks of requiring regulations on IoT device security. Some vendors have started to mention about the improvements to the security of the IoT devices that they will implement. However a customer who owns a vulnerable device – and the device vulnerability cannot be fixed [5]– would switch to another device. If the vendor cannot incentivize the customer, it will lose the market quickly. Psychologically, the customer prefers to switch to another vendor even when the vendor provides a secure device with the same price of the rivals. This has led to vendors decisions to compensate the customers after the massive breach [4].

For instance Dahua company offers discounts to customers who want to exchange their vulnerable device. By analyzing the response of Dahua company, responsible for vulnerability of many devices, we strive to shed light on the ROSI of vendors who are shifting to Risk mitigation strategy by taking into consideration their recent decision. The Dahua vulnerability cannot be fixed by a simple update and the users have to change their device. In such a scenario, the vendor should not only invest on the security control cost but also on the cost to retain the users. Without the latter, the users would leave because they prefer to invest in another vendor who is not proved to be vulnerable. Dahua has not yet mentioned the percentage of discount. In the rest of this section we model ROSI based on the cost of vendors without taking any action that is the cost imposed on the vendor by the customers who leave (L) and with giving discount (D in %) and fixing the security issue (c). L is correlated by the number of users(u) who leave and the cost of devices(dev) that we assume it is a constant:

$$L = dev * u$$

After taking the actions vendors expect that the number of users who leave (u') reduce. We assume u' reduces to PU % of u. PU is correlated with D and c . This means the more the company invests, the more the users stay. Based on the defined parameters the expected loss for the vendor after applying discount and security control is:

$$L' = u' * dev + (u - u') * D * dev + c$$

Based L' and L we define ROSI as:

$$\text{ROSI} = L - L' = \frac{(1-PU)(1-D)(Dev * u) + c}{\Big(\big((1-PU) * D\big) + PU\big) * dev * u\Big) + c}$$

u can be maximum all the users of the company. We do not have the actual number but we can approximate it using Shodan result. If we assume the users act rationally without company countermeasures they all switch. In practice this is also expected. An IOT company with 300K customers talked to the authors of this paper and accounted bankruptcy as the cost of lack of security. Based on the Dahua devices identified by Shodan and the cost of $45 on average for DVRs (based on the price of H.264 DVR) we approximate L as 35 million dollars. We assume c does not exceed 350K dollars to fix the device vulnerability in new devices. Although such investment does not reduce the probability of breach for Dahua to that of vendors like Linksys it is a reasonable investment at this point in time. Over time the company may invest more to reduce the probability of defamation like this, however, now more investment does not incentivize the users to stay because they have no way to measure the security as a result. Also, as mentioned even with the same security, psychologically victims prefer to switch to other rivals product with the same price. This means Dahua should concentrate on the D value more instead of c. Based on this analysis we remove c from ROSI formula because it is less than 1% of the L and it is negligible compared to the other values. In addition if security investment is successful ROSI must be greater than 1. Given this, we get:

$$ROSI > 1 \rightarrow$$

$$\frac{(1-PU)(1-D)(Dev * u)}{\Big(\big((1-PU) * D\big) + PU\big) * dev * u\Big)} > 1$$

$$\rightarrow \frac{PU}{1-PU} < 1 - 2D$$

The formula gives us two insights. First, D can never be greater than 50% because otherwise the right side of equation becomes negative and the left side can never be negative (0≤PU≤1). Moreover, the relationship between PU and D is not linear and that in reality is also true. In other words even if more discount means more customer lock-in, the vendors are conservative in order not to lose money over the discount cost itself.

Figure 4. ROSI based on discount (D) and users leaving the vendor (PU)

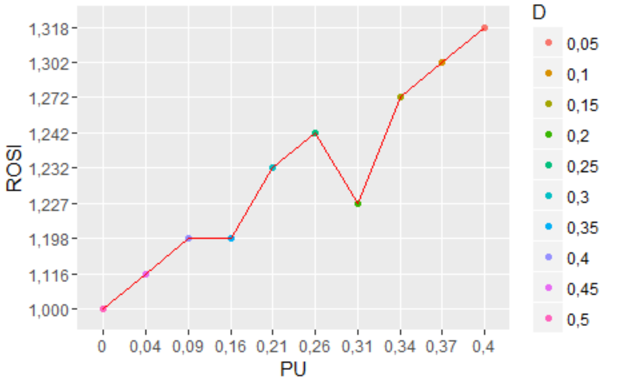


Figure 4 illustrates Dahua ROSI based on D and PU. As shown we only analyzed ROSI based on multiples of 5% up to 50%. We found argmax based on PU. This figure helps Dahua to choose the best amount of discount based on their expected PU value. For instance if company expects that 40% of its users leave even with a discount of around 10% then Dahua should only make the discount 5% because then they will have the maximum ROSI.

7.2 Mitigation strategy based on lawsuit cost analysis

Another problem is caused by the scale of the insecure IoT devices being used for malicious activities as it may result in class action lawsuits against vendors as evidenced by the following statement.

“ Also, in the past week I’ve heard from two different attorneys who are weighing whether to launch class-action lawsuits against IoT vendors who have been paying lip service to security over the years and have now created a massive security headache for the rest of the Internet.” [2]

These lawsuits may be absolutely disruptive for the business and lead to complete bankruptcy by the company. In order to calculate the ROSI some assumptions have to be made. Information security industry has seen lawsuits in which companies were losing billions of dollars due to different security incidents.[7]. However, suing the vendor for not taking security measures which lead to devices being compromised, used in botnets and for DDoS attacks in particular is something new.

For instance, anti-DDoS protection capable of dealing with a high volume IoT DDoS will cost about $200,000 a year and we will take it as a base number for lawsuit against the company From our data set we know that there were 872342 unique devices attacking the honeypot out of them 311294 were produced by Dahua. So 36% of all the devices attacking the honeypot during the 2 month period were produced by Dahua and we will take it as a base number for number of Dahua devices in the IoT botnets. So from this point we can assume that whatever losses are caused by IoT botnets. Victims will be able to sue Dahua for approximately 36% of their loses in any particular attack. According to [10] anti-DDoS company Akamai witnessed 4,523 DDoS attacks and 19 with a capacity over 100 Gbps in the first quarter of 2016. So 18,000 DDoS attacks can be expected in 2016 and 80 attacks with a capacity of over 100 Gbps can be expected. With the public release of the Mirai source code we can assume that the number of IoT botnets will grow drastically, so will their share in DDoS attacks. We expect that approximately 30% of botnets are IoT botnets. In order to calculate Dahua losses we need to do some more assumptions. We assume that approximately 15% of victims will go to court and only about of 7% of lawsuits will be successful. This numbers are relatively low because most of the victims are small companies who might have not enough resources to defeat a big company like Dahua in the court. These numbers are mostly assumptions and cannot be discrete for this reason we applied standard deviation of 30% to all of them and for the final results 1000 iterations of Monte Carlo simulation were done.

We will calculate vendor loss by multiplying unitary impact with annual frequency

Unitary Impact will be equal to one lawsuit against the vendor = $VictL * VendS$

$VictL$ *= DDoS victim’s loss and* $VendS$ *= percentage of the vendor’s devices involved in the attack.*

Annual frequency will be $D * I * C * C'$

D *= number of DDoS attacks*

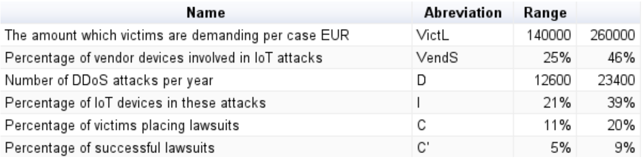
Ip *= percentage of attacks accomplished by IoT botnets*

C *= percentage of cases taken into the court*

C' *= percentage of satisfied lawsuits against vendors.*

Vendors annual loss can be calculated by the following formula

$$ALE_0 = VictL * VendS * Dh * I * C * C'$$



Name	Abreviation	Range	
The amount which victims are demanding per case EUR	VictL	140000	260000
Percentage of vendor devices involved in IoT attacks	VendS	25%	46%
Number of DDoS attacks per year	D	12600	23400
Percentage of IoT devices in these attacks	I	21%	39%
Percentage of victims placing lawsuits	C	11%	20%
Percentage of successful lawsuits	C'	5%	9%

Figure 5: Ranges of used variables

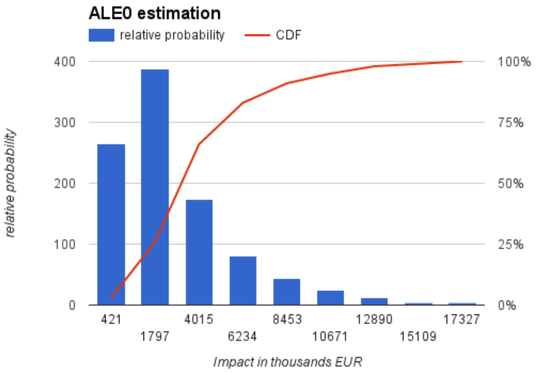


Figure 6: Annual loss estimation without applying any security measures

Figure 6 gives us an insight into the possible losses within the defined range of variables shown in Figure 5.

However, it is mentioned that Dahua has hardcoded passwords into the telnet binary and this is the primary reason passwords cannot be easily changed now. We believe that by putting some resources into development a custom way of replacing the weak binary with one that will have no hard coded values can be accomplished. During this process the user’s password can also be changed for a unique one by using a random number generator. According to the Gordon-Loeb rule Dahua vendor should not spend on security more than 37% of an expected loss. As it can be seen from the graph the likeliest outcome for the vendor will be $1.8M losses. However, we cannot hope that the chosen strategy will completely mitigate the problem. Because not all users might want to apply the fix or not all of them might be aware of the vulnerable device in the first place. So risk strategy will reduce the percentage of vendor devices involved in IoT attacks. Consequently, it will reduce the damage caused by these devices and the amount of possible lawsuits and their compensation. In order to calculate that we need to make an assumption about the percentage of devices on which users will not apply the patch. According to [11] in the first quarter of 2016 6.5% of users were running unpatched windows systems (vista, 7 ,8 or 10). However, such a low number seems unrealistic for IoT vendors. We can assume that 25% of users will not patch their devices. Standard deviation of 30% must be applied here too. This variable will be called Du with range 17.5% - 32.5%.

So our formula for ALEs = VictL * VendS’ * Dh * I * C * C’

VendS' = percentage of the vendor's devices involved in the attack (devices that are still unpatched)

VendS' = VendS * Du
ALEs = VictL * VendS * Dh * I * C * C' * Du = ALE0 * Du
EBISs = ALE0 - ALEs = ALE0 - ALE0 * Du >> EBISs = ALE0 * (1 - Du)

From this formula an interesting insight can be observed. As long as security measures cost less than 67.5%-82.5% of an annual loss the return on security investment will be positive. After another 1000 iterations of Monte Carlo simulation we have the following expected benefits of an investment in information security.

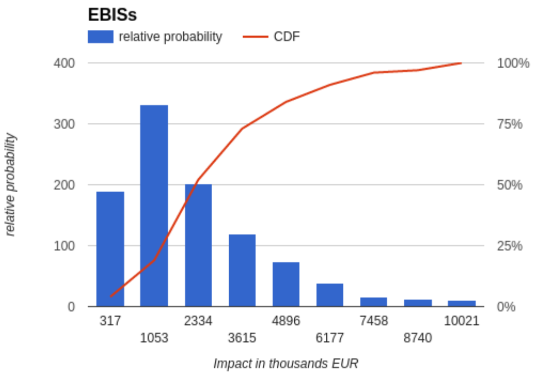


Figure 7: Expected benefits of an investment in information security

Lawsuits are a serious problem for every business. Recent decade has proven that security related lawsuits can cause a huge amount of harm for any business or even completely destroy it; And it can be one of the ways to make vendors take security more seriously. According to our analysis Dahua can expect the loss of millions of Euros annually. So it should definitely take measures in order to prevent it.

8. CONCLUSION

The security strategy of vendors before the recent massive Mirai compromise seems to be highly related to the companys fame. This is understandable because the compromise of customer device does not directly harm vendor assets but through reputation. While all the vendors seem to have the same risk acceptance or risk transfer strategy regarding default credentials, they tend to differ regarding other authentication risks. Again this is reasonable by the impact of other vulnerabilities to the company reputation. While a default credential can be traced back to the user awareness, an authentication vulnerability such as Dahua's greatly affects the company reputation and may lead to their bankruptcy. Dahuas different strategy may be justified by their business model that is B2B and the fact that their name is not known by the end user. This obviously has been a miscalculation because a DoS attack would start lawsuits.

9. REFERENCES

[1] B. Schneier, "We Need to Save the Internet from the Internet of Things," MOTHERBOARD, 6 October 2016. [Online]. Available: https://motherboard.vice.com/read/we-need-to-save-the-internet-from-the-internet-of-things

[2] B. Krebs, "Europe to Push New Security Rules Amid IoT Mess," KrebsonSecurity, 8 October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/europe-to-push-new-security-rules-amid-iot-mess/#more-36602

[3] B. Krebs, "Source Code for IoT Botnet 'Mirai' Released," KrebsonSecurity, 1 October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[4] CEPro, "Dahua Addresses Recent Report Regarding DDoS Attack," 6 October 2016. [Online]. Available: http://www.cepro.com/article/dahua_addresses_recent_report_regarding_ddos_attack

[5] Z. Wikholm, "When Vulnerabilities Travel Downstream," FlashPoint, 7 October 2016. [Online]. Available: https://www.flashpoint-intel.com/when-vulnerabilities-travel-downstream/

[6] Internet Census 2012, "Port Scanning /0 Using Insecure Embedded Devices - Carna Botnet," 2012. [Online]. Available: http://internetcensus2012.bitbucket.org/paper.html

[7] The Internet of Things is already here, but who bears the risks? A model to explain coverage disputes in a world of interconnected, autonomous devices, Andreas Haas, Markus Haas, Markus Weidner

[8] Olivia L. Eckerson, "Data breach lawsuits indicate a troubling trend for enterprises", TechTarget, February 2016. [Online]. Available: http://searchsecurity.techtarget.com/news/4500273340/Data-breach-lawsuits-indicate-a-troubling-trend-for-enterprises

[9] B. Krebs, "The Democratization of Censorship" KrebsonSecurity, 25 September 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/

[10] Steven J. Vaughan-Nichols, "DDoS attacks increase over 125 percent year over year", Zdnet, 8 June 2016. [Online]. Avialable: http://www.zdnet.com/article/ddos-attacks-increase-over-125-percent-year-over-year/

[11] "US PC Users Making Some Progress in Patching Software Vulnerabilities, But Significant Challenges Remain", Flexera software. [Online]. Available: http://www.flexerasoftware.com/enterprise/company/news-center/press-releases/US-PC-Users-Making-Progress-Patching-Software-Vulnerabilities-But-Challenges-Remain.html