Economics of Cyber Security
Security and Risk Management - Group 3

Tugce Arican, Sina Davanian, Alpha Diallo, Oleksander Shyvakov

University of Twente

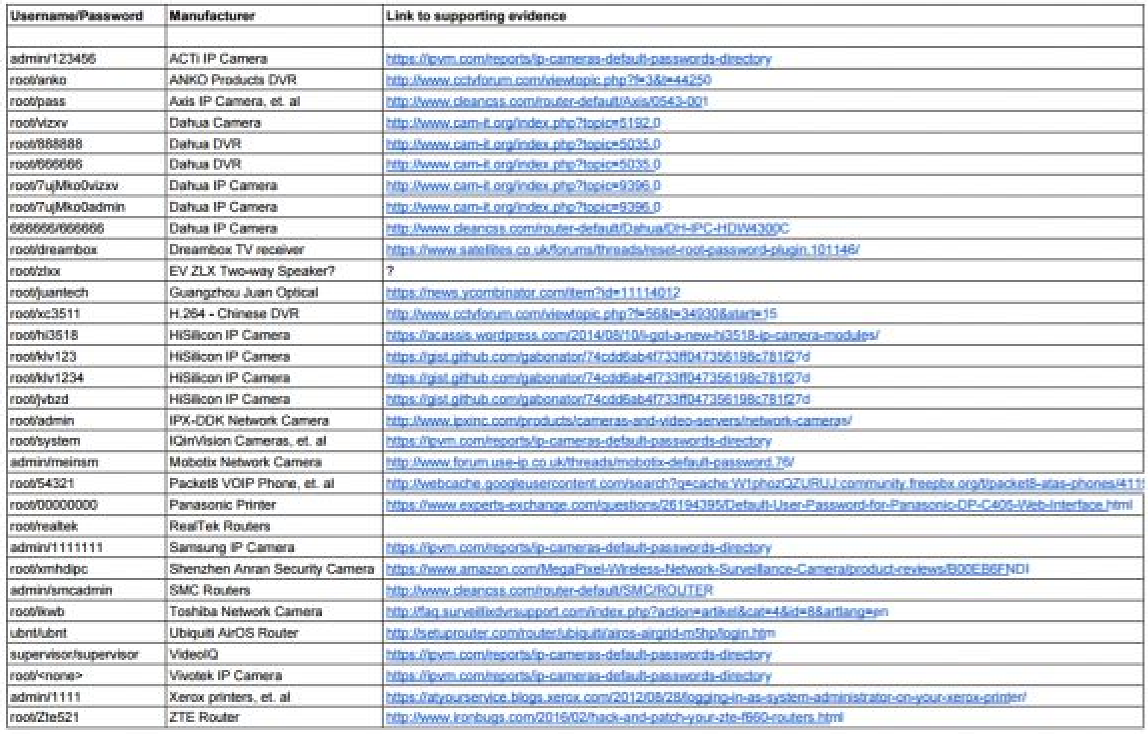
Problem Owner of the Security Issue

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. 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 outside the state to critical infrastructures because of threat of cyber wars. 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.

Metrics and Security Performance Differences

One interesting approach would be analyzing the security of two vendors with the same credential and the same frequency of attacks (this removes the uncertainty on the number of attacks performed against these specific devices) and compare the number of vendors we see in the scan dataset. We also need the number of devices from that vendor (exposures). Even if the credentials are not the same and the frequency of credential usage are negligibly different we can do the comparison. The analysis should also discuss the implementation of the default credential and analyze if the SSH/telnet credentials are default than the browser one.

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

Some login-password pairs were used more frequently than others, which can be described by the prevalence of some product over the other in the market.

Possible Risk Strategies for the Problem Owner

Vendors need 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. Vendors could also provide firmware updates to the devices that they know have no credentials or default credentials rather than asking users to change the credentials themselves. 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]

This is because although the users may change the credentials on the web interface provided, the devices can still be accessed through telnet or ssh, since the passwords are hardcoded into the firmware. Because many of the users may not know this they will think that by just changing the credentials through the web interfaces they are safe, which is the wrong assumption and vendors need to let the users using their devices know.

Other Actors with Respect to Security Issue

Other actors that can influence the security issue of default or no credentials 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 be buy devices that have no sort of authentication mechanism in them or if the authentication mechanism 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 mechanism so that they would not lose anymore revenue.

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

ISPs can have an affect 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 try to find the devices that have no authentication mechanism or that have default credentials and block them if they are using too much bandwidth.

Risk Strategies Regarding the Actors

The usage of IoT devices in botnets is growing really fast and very soon it can reach the governmental level. With today's 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].

The easiest and fastest way could have been for device owners to actually go and change their default passwords. However, there are some problems with that. First of all consumers are not really concerned about security and do not want to spend some extra time on it. And 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. Another choice consumers have 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 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 reducing of the bot herd from ~380k to ~300k. The attack on Brian Krebs website happened on the 20th of September and source code was released on 30th of September. So it took about 10 days after the incident to reduce the bot heard 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.

Calculate the Return on Security Investment (ROSI)

Out of all the risk strategies the one where vendors roll out the security firmware updates was chosen. 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. Some are offering discounts to their customers as stated in [4] on the press release by Dahua, after a security firm did research as stated in [5] and found that there were web authentication vulnerabilities present in the devices used in the DDoS attack.

Vendors providing firmware updates, that deal with the authentication credentials on their devices, to their customers do have a cost to deal with. The cost is mainly for writing the firmware updates. The cost of writing the firmware updates will be negligible when compared to the reputational damage the company may face, the cost of providing discounts to customers to get new devices, or completely replacing user devices at a later time.

If vendors do not follow any risk strategy and take the risk of ignoring any risks that may be present then they may face a loss in reputation. This loss of reputation will force them into spending money just to try to get back their loss reputation. 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.

“ 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 a complete bankruptcy by the company. In order to calculate the ROSI we need numbers that we do not posses. For instance the amount of money for the lawsuits or how reputation loss will have an effect on the company financial posture.

Conclusion

Vendors of IoT devices face a security issue in that the devices that they provide either only have default credentials for authentication purposes or have no authentication mechanisms whatsoever. This security issue affects not only the vendors, but also consumers of those devices, governments, and ISPs. Each affected party has their own strategy for dealing with the security issue, and when it comes to the vendors, one strategy is to provide firmware updates to their devices to require unique credentials on the devices. If the vendors do not take any steps to implement their strategies then they risk not only monetary losses but also a loss of their reputation, which in some cases can be worst then if they just lose some money. Although, the vendors will have costs in implementing their security strategies the losses that they accumulate in the implementation will be less than the losses they would accumulate otherwise.

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/