Alexa's Case: vulnerability issues in IoT devices in residential automation

Luiz Antonio de Sousa Ferreira[1], Leonardo Yvens Schwarzstein[2], Yuzo Iano[3], Camila Santana Domingues[4]

***Resumo*—With the advent of Internet-based technologies of Things, people's everyday lives have been invaded by connected devices, making it an important tool in consumer life, both in issues comfort, and receptivity in a world in which interactivity is one of the key issues for survival. In this study we present a history of vulnerability problems in residential automation systems, one of the devices to meet this new connected need. The focus of this study is on the Amazon Echo product developed by a leading electronics company, Amazon Technologies Company, which, because of configuration issues, has drawn consumers' attention to the risks that a potentially large system can bring to its routine, analyzing some solutions that the company adopted to overcome this type of problem, stressing the need for investment in the sector.**

***Index Terms*—vulnerability, security, iot, automation, tecnology**

I. Introduction

The first waves of things home automation and the internet of things (IoT) are becoming accessible to the general public. By definition, these devices are integrated into people's daily lives and are intended to facilitate and automate routine activities. What is called "Things"in IoT corresponds to a type of device, physical or virtual, that has an internet connection and is also capable of communicating with other devices, in addition to its user [6].

These devices are always connected on the Internet, often equipped with voice and video sensors, which are able to continuously capture information from the environment and communicate with services under the pretext of making their lives more convenient with their use. However, these capabilities have concerns about the privacy and security of users, since they are essentially devices requiring connection, they are subject to several types of security flaws, either in system development or configuration, common to any computer system.

With the emergence and popularization of such equipment, security problems stem from the large volume of use as well as the interest in invasion for data theft. The use of proprietary operating systems or services coupled with hardware characteristics may mean that conventional security schemes are not used in IoT devices, limited due to the need for miniaturization and reduced production costs [8].

In this article, we do a study of a real fact in which a child made the purchase of a toy without the knowledge of the parents, using Amazon Echo, a product of the Amazon Technologies Company, a fact that was aggravated by the transmission of the report in a local television news, where, exemplifying what happened, the reporter also caused the same vulnerability [9]. We then introduce the incidents, the vulnerabilities that caused them, and how these types of failure can be solved.

II. Incident

Devices like Amazon Echo have as one of the main features a personal assistant, in this case the so-called "Alexa", and one of its functions allows the user to make purchases only with voice commands. Unauthorized use of this functionality is a recurring problem, including cases where children accidentally send voice commands without parents' knowledge of functionality [2]. However, in this case the problem was exacerbated, because in a TV report about an incident of this type, the phrase *"I love the little girl, saying 'Alexa ordered me a dollhouse'"* was said to have triggered further attempts to buy quoted product without human intervention, since other Echo devices that were close to the viewers' TVs answered the reporter's voice command.

This does not necessarily result in the finalization of the request, because currently, to confirm the request it is necessary to say "*Yes*", however, it would suffice if there was any noise similar to the confirmation word, close to the device, for the request to be fulfilled.

It is evident that a vulnerability exists in this case, since authentication was not necessary to use the device, that is, any person or even another device that generates sound in the environment is able to control it, due to the fact that there is no recognition of the registered user's voice. An erroneous purchase order may seem like a mere inconvenience, but as these devices gain power to control all aspects of a home, such as the manipulation of lights, locks, appliances, among others, we realize how this type of vulnerability can become especially the physical safety of users. Such breach types can be discovered by malicious people who may also be known by programmers or system designers, but who, if not corrected

[1]L.A.S. Ferreira is with the Faculty of Electrical Engineering and Computation (FEEC), University of Campinas - UNICAMP, Brazil luizfer@decom.fee.unicamp.br

[2]L.Y. Schwarzstein is with Computer Institute (IC), University of Campinas - UNICAMP, Brazil leoyvens@gmail.com

[3]I. Yuzo is with the Faculty of Electrical Engineering and Computation (FEEC), University of Campinas - UNICAMP, Brazil yuzo@decom.fee.unicamp.br

[4]C.S. Domingues is with the Faculty of Electrical Engineering and Computation (FEEC), University of Campinas - UNICAMP, Brazil ca_santana_@hotmail.com

in future updates, can lead to a large-scale invasion with catastrophic proportions [6].

III. Causes

The main cause, acknowledged by the manufacturer itself [9] , consists in the misconfiguration of the devices which, if uncorrected, enables the device in question to be triggered by the same standard "*Alexa*"voice command, not requiring authentication for realization or for confirmation of purchase orders, provided that a credit card is registered in the device, which is requested during the initial configuration of the same.

The manufacturer presented a contour solution to this incident: it was informed that it was possible to switch off the voice purchase function or require an authorization code to make purchases [7]. However, by default, these settings are displayed on the least secure level possible, with voice purchase enabled and without authorization code. Another contour option would be to change the factory-set "*Alexa*"activation command to another customizing the user experience.

In addition to configuration issues, the vulnerability of the product in everyday use is notable because it does not consider a form of authentication that, in addition to an algorithm error, could expose important personal data of all local users of the device, such as credit cards, usage logs, personal data, passwords, etc.

The manufacturer's effort to come up with a definitive solution is fundamental so that problems of this magnitude do not occur. In this sense, the company's commitment to investing in this type of solution can attest to its ability to work on future incidents. Consequently, the success of the product in the market can be tied to the user's confidence that, often, this information is used to measure the quality of services rendered [5].

IV. Impact

The problem of product vulnerability affected (i) the family of users of the device, which disposed of approximately 160 pounds for the toy, in addition to 4 pounds spent on cookies [3]; (ii) the viewers who accompanied the transmission of the report on TV, which, having devices with the same security flaw, were subject to the same problem of unauthorized purchase, caused by the repetition of the voice command by the reporter who reported the problem; and (iii) the product, which attracted the attention of the whole world through negative propagation by the media. The market itself is working to increase the popularity of such devices, bringing the virtual assistant of the study as the reference in products of the type, according to research released by eMarketer consultancy, where 70.6 percent of the North American market in a sphere estimated at 35.6 million users [4], with the main factor of adoption being the comfort of using such a tool on a day-to-day basis.

More than direct impact, this incident raises concerns about security in IoT devices, particularly the lack of authentication. This incident is an alert for the ease with which these devices can be controlled remotely even accidentally, without the need for technical knowledge, due to the simplicity of the failures.

V. Solutions

To get around the problem immediately, Amazon, the manufacturer of the device, expressed through the press and posts on its site dedicated to technical support, releasing guilt, while setting the responsibility of increasing security in the device itself. The user while clearly working on a definitive solution.

As a solution, after the reported incidents, as of the date of the publications in its technical support system, it has announced that physical purchases from the store may be returned and refunded, provided that the purchase date is less than one month. As this is a contouring solution, since the security flaw still persists and the affected user, besides the inconvenience generated by the accidental purchase, will have the wear and tear with the procedures for return and refund of the purchase.

It is also clear that after recognizing the problem, the company works on a definitive solution, however, it is still possible that an external voice can make purchase orders in several houses at once. Competitors of the Amazon Echo, which have a higher price, such as Google Home, have tools smarter than the molds of the product studied, among them, user recognition through voice [5].

One of the mechanisms used by the competitor would be a possible solution for the case studied, since it allows to register up to six different users in the same device, ensuring that only these users are able to use the voice functions, thus, the device is capable to recognize which user is performing the tasks [5].

VI. Conclusion

With the advent of domestic technologies and their insertion into the user's daily life, one must consider the increase of vulnerabilities in the same proportion as the devices become relevant in the market. This type of vulnerability leads to problems that may allow the misuse of technology, as well as causing inconvenience to users, who, through the generated dissatisfaction, may fail to consume or recommend the product in their relationship networks, a fact that can directly impact on sales of products or services.

Outline solutions demonstrate the company's intent to tune and recognize the problem, but only those are not enough to maintain the quality required and proposed by those systems. It is suggested to implement a universal security policy as effective as those present in a smartphone or personal computers, increasing investments in this sector.

It is considered, from the discussions listed in this article, that for the affirmation of these devices in the market, it is indispensable an extra dedication in aspects that can pass the confidence necessary for more users to use these devices in their day to day, facilitating, sometimes decisions that can be automated. Security is a key factor for the success of such devices, for manipulating personal data and personal information of each user.

Referências

[1] Help and Costumer Service. (2017, January) *About Placing Orders with Alexa* [Online]. Avaliable: https://www.amazon.com/gp/help/customer/display.html?nodeId=201807210

[2] The Verge. (2017, January 7). *"Amazon's Alexa started ordering people dollhouses after hearing its name on TV"*. Avaliable: https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse

[3] The Mirror (2017, January 8). *"Amazon Echo causes chaos when five simple words said innocently on TV news broadcast ends up costing viewers a lot of money"*. Avaliable: http://www.mirror.co.uk/news/world-news/five-simple-words-said-innocently-9583213

[4] IstoÉ Dinheiro (2017, May 8). *"Amazon lidera mercado americano de assistentes de voz, aponta pesquisa"*. Avaliable: http://www.istoedinheiro.com.br/amazon-lidera-mercado-americano-de-assistentes-de-voz-aponta-pesquisa/

[5] CNN (2017, April 20). *"Google Home now recognizes your individual voice"*. Avaliable: http://money.cnn.com/2017/04/20/technology/google-home-voice-recognition/index.html

[6] Z. K. Zhang,M. C. Y. Cho,C. W. Wang,C. W. Hsu,C. K. Chen,and S. Shieh,"IoT security: Ongoing challenges and research opportunities,"Proc. - IEEE 7th Int. Conf. Serv. Comput. Appl. SOCA 2014, pp.230-234, 2014.

[7] Amazon Help and Costumer Service (2017, January 7) *"Manage Voice Purchasing Settings"*. Avaliable: https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201952610

[8] M. M. Hossain, M. Fotouhi, and R.Hasan, *"Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things"*, 2015 IEEE World Congr. Serv.,pp.21-28, 2015.

[9] Fox News (2017, January 6) *"TV news report prompts viewers' Amazon Echo devices to order unwanted dollhouses"*. Avaliable: http://www.foxnews.com/tech/2017/01/06/tv-news-report-prompts-viewers-amazon-echo-devices-to-order-unwanted-dollhouses.html