Research Report about IoT Security

Christos Beretas

Abstract: The purpose of the present research is to identify security holes in IoT in percentage, according to a research conducted from January 5, 2020 to January 26, 2020 involving a large number of people who are actively involving with IoT. These people wanted to share their fears and anxieties, expressing their views freely. The majority of participants expressed concerns about IoT security. This research clearly shows the phobias that exist as well as the lack of an IoT protection mechanism considering the restrictions that exist.

I. INTRODUCTION

There is a significant increase in the use of IoT in various sectors, the use of IoT has increased significantly in the last 5 years, taking into account the technological innovation of both electronics and Information Technology. According to research published in recent years, the use of IoT in the next decade is expected to increase by as much as **90%** as human needs grow and technology becomes more accessible.

Given recent forecasts for the use of IoT in the future, what concerns tech-savers is the lack of a security strategy that will be able to prevent IoT from being attacked by external cyber attacks or cyber attacks that began from the internal network. Some research that have been performed with a variety of prosthetic techniques have shown to be insufficient and do not provide the protection that is required.

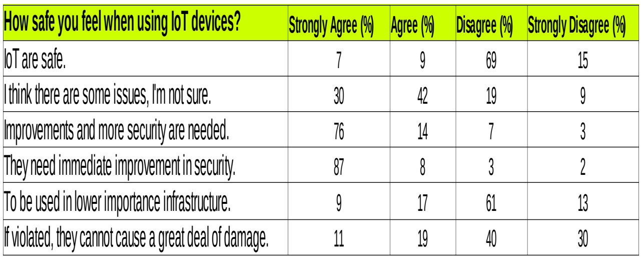
In order to create this research report, all the parameters were taken into account, incluiding the required evaluations, then the questionnaire sent to the participants after considering the possibility of misinterpretation.

II. METHOD

For the purpose of this research, one electronic questionnaire was used which was distributed to groups on social media. Participation was **anonymous** and **voluntary**. There was no personal data collection, the duration of this survey was **January 5, 2020** to **January 26, 2020** with a total duration of **22** days.

III. RESULTS

The participation rate in the questionnaire was **89%**. The following table presents in detail the research data which clearly shows that the issue of IoT security and privacy is a burning issue that will be of concern to all involved. In one or the other way with IoT.



How safe you feel when using IoT devices?	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)
IoT are safe.	7	9	69	15
I think there are some issues, I'm not sure.	30	42	19	9
Improvements and more security are needed.	76	14	7	3
They need immediate improvement in security.	87	8	3	2
To be used in lower importance infrastructure.	9	17	61	13
If violated, they cannot cause a great deal of damage.	11	19	40	30

From the analysis of the above table, may conclude the participants' clear concern about the security of Iot and its immediate improvement at **87%**.

IV. RESULT ANALYSIS

In **87%** of survey participants are deeply concerned about the security of IoT and requesting for its **immediate improvement**. This is followed by **76%** of those who believe that improvements and enhancements to security levels are needed. An **11%** believe that a breach of an IoT cannot affect the rest of the network. **9%** believe that deploying IoT in lower importance infrastructures would solve the security problem, thinking that breaching low importance information systems would not significantly affect organic information technology infrastructures. **7%** believe that IoT is secure, and finally **30%** believe there are security holes but they are not sure.

V. CONCLUSION

This research report has clearly raised users' concerns in the field of IoT security. It has highlighted the need to immediately improve **data security** and **network security policy**. The results showed some users in very small numbers who were not concerned about IoT security. The vast majority accept that there are problems and worries about personal data, and acknowledges the need to **immediately improve** and enhance IoT security.

REFERENCES

[1] D. A. H. Shehab and O. A. Batarfi, "RCR for preventing stack smashing attacks bypass stack canaries," 2017 Computing Conference, London, United Kingdom, 2017, pp. 795-800. doi: 10.1109/SAI.2017.8252186

[2] E. W. Netto, R. Vaslin, G. Gogniat and J. P. Diguet, "A Code Compression Method to Cope with Security Hardware Overheads," Computer Architecture and High Performance Computing, 2007. SBAC-PAD 2007. 19th International Symposium on, Rio Grande do Sul, 2007, pp. 185-192. doi: 10.1109/SBAC-PAD.2007.40

[3] F. Ye and Y. Qian, "A Security Architecture for Networked Internet of Things Devices," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6. doi:10.1109/GLOCOM.2017.8254021

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017. doi: 10.1109/JIOT.2017.2683200

[5] K. Liang, Y. Feng, J. Wei and W. Guo, "SecPage - A Lightweight Memory Protection Architecture," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 1917-1922. doi:

10.1109/TrustCom.2016.0293

[6] M. Ye, N. Hu and S. Wei, "Lightweight secure sensing using hardware isolation," 2016 IEEE SENSORS, Orlando, FL, 2016, pp. 1-3. doi: 10.1109/ICSENS.2016.7808904

[7] R. Jinnai, A. Inomata, I. Arai and K. Fujikawa, "Proposal of hardware device model for IoT endpoint security and its implementation," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 91-93.

[8] T. Thangam, G. Gayathri and T. Madhubala, "A novel logic locking technique for hardware security," 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), Karur, Tamilnadu, India, 2017, pp. 1-7. doi: 10.1109/ICEICE.2017.8192439

[9] Y. W. Lee and N. A. Touba, "Computing with obfuscated data in arbitrary logic circuits via noise insertion and cancellation," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 146-152.

Christos Beretas. PhD Candidate in Cyber Security at Innovative Knowledge Institute, Paris, France. Contact Details: 170 Rue Raymond Losserand 2, 75014 Paris, France. (+33) 173-491-442 | (+30) 693-890-947