Assessment of Wireless and IoT Security Awareness: A Case Study

Burak ÖZÇAKMAK^{*,1}, Ahmet KAPKİÇ^{*,2}, Beyza BAĞIRÖZ^{*,3}, Abdulkadir KOÇ^{*,4}, Uraz YAVANOĞLU^{*,5}

Gazi University, Computer Engineering Dept, Maltepe 06570, Ankara, Turkey
[1] burakozcakmak@gmail.com, [2] ahmetkapkic@gmail.com, [3] ahmetkapkic@gmail.com,
[4] abdulkadir0916@gmail.com, [5] uraz@gazi.edu.tr,

***Abstract*—This paper analyses wireless and IoT device security awareness among users over wireless and IoT device usage data in the capital of Turkey, Ankara and examines the focus needed to given to increasing security awareness based on the broadband and IoT device availability. In this context, district based wireless and IoT device data gathering is realized with the aid of Warwalking and Wardriving methods. Within the field of study, 53664 wireless and IoT device metadata have been collected in districts of Çankaya, Gölbaşı, Yenimahalle, Sincan, Etimesgut, Altındağ and Mamak. Study shows that while the security awareness in Ankara is calculated as 54/100 and this number is increasing slowly, the IoT device and broadband availability, thus the need for increasing the awareness is increasing faster. It has been considered that this study will provide other researchers a criterion to calculate wireless device awareness and increase security awareness.**

Keywords—Wireless; IoT; Awareness; Security; Information Security

I. INTRODUCTION

This study is the continuation of the work done by Yavanoglu and his colleagues in 2015 and it is aimed to investigate the changes in the understanding of the security of the country and the society of this study which was made 3 years after the writing of the article.

Although the concept of cyber security has been discussed in different circles almost every day and many academic studies have been done on it, the notion of awareness which is the basis of cyber security has not yet been adopted by the public at the necessary level. One of the most important reasons for this is it can not be perceived by individuals. The security dilemma that arises from individuals who have no knowledge and / or do not care about the consequences of the confiscation of personal information by others is one of the biggest instruments used by cyber attackers today.

Rapid and seamless transfer of information is one of the factors that cause the technology to develop very quickly. This technological development brings about many security vulnerabilities. With the creation of the IOT concept and the introduction of our life, we have access to the internet through almost any component of the wireless network infrastructure, from smart home systems, security camera systems, washing machines to toothbrushes. With the introduction of the IoT concept to our life, access to the internet is available through most IoT devices that we make use of, from intelligent home systems, camera systems, washing machines to toothbrushes [1-3]. These innovations, which are aimed to make life easier, also invite hackers to our homes at the same time. As a matter of fact, the largest DDOS (Denial-of-service) attacks of 2016 were carried out via IOT systems [1]. Washing machine, transportation machine, etc. b. Persons who are involved in the attack by means of devices included in the IOT system have been used by attackers because of the lack of cyber security awareness [2,3]. The IoT approach is increasingly used in everyday life in todays hospitals, in many areas of the industry, with the spread of concepts such as intelligent home, smart cities. Including more than 50 million devices will be expressed in a few years in IoT approaches, security vulnerabilities can also be found in many different areas. These vulnerabilities in IoT approaches can be on either hardware or software level. This situation, it is important to inform users and gain awareness times more emphasized. In the last 10 years, many studies have been carried out in Turkey under the "National Cyber security strategy and 2013-2014 action plans" document in order to improve the awareness of the cyber security [4]. However, the security gaps created by the devices included in the IoT system are still a very new concept in our country. Devices with IoT approach and complex the level of awareness for users is very low [5] although structures have begun to be used quickly. The most basic examples are the weaknesses caused by the devices used in the IoT approach are the vulnerabilities caused by the wireless network structure, the threats caused by the encryption infrastructure used in the communication between the sensors and the devices, and the problems that can occur during the authorization and verification steps. Because the architecture used has multiple engineering disciplines together, security threats can be compared to other systems it should be more. As the devices used in the IoT approaches have a lot of personal information in them, security is the most important factor in IoT systems.

In the second section of this work, security systems of IoT devices and administrators' behaviors related to these systems, scientific explanations and explanations about deficiencies of IoT devices and approaches to these deficiencies are given. The methods and procedures followed during the work is given in the third section of the work. In the fourth section of the work, the field work results carried out accordingly to the methodology section are given and explained thoroughly. In the last part of the study, several findings were given to increase the IoT device safety awareness in the society, various evaluations were made and suggestions were presented.

II. LITERATURE STUDY

In a study conducted by Yavanoğlu and his team in 2015, the study of the safe internet usage awareness of people in Ankara and the relationship between social consciousness of the community and socioeconomic level were investigated. In the study, the measurement of security levels of wireless network devices was done using wardriving and warwalking methods. With the examination of the data, it was determined that the devices use WPA2 encryption method by 72%, SSID identity is changed by 64% and WPS standard by 43%, and the determined rates are 95,58% similar to the socioeconomic level of residents of Ankara, showing the effect of socioeconomic status on information security [5].

In the work carried out by Tabane and Zuva, it has been suggested that the IOT approach will directly affect by daily life in the near future . Authors said that, the IOT system is basically communicating between different sensors and smart but this system also spread quickly and get a place in our daily lives. IOT approaches have included many personal and sensitive prescriptive knowledge. Authors who emphasize the problems that may arise if this information is passed on to malicious people. in a short time they stated that security measures in IOT systems would be one of the most important issues.Also iot system which is the hardware structure of smart devices, the system creates the hardware of the communication with each other (smart devices, sensors, etc.), And the web forming the IOT approach is stressed that call forth security vulnerabilities of each layer, the statement would be one of the near future, the most important research topics of these problems they have.

Vashi and colleagues defined the IOT approach as smart home, smart city, smart architecture and smart world. The IoT structure that connects sensors, devices, hospitals, industry and customers to each other on the internet has a complex architecture because of the reasons such as connecting many devices, using multiple technologies together. The fact that many devices that meet our needs in everyday life quickly move to the IOT approach show that, in the next decade the most important parameter in the intelligent world is IoT. According to the authors, although security measures are an important factor in every system and approach, it is certainly the most important field in IOT systems. In that work performed by Vashi and colleagues, one of the key safety areas of IOT is the identification and authorization of devices. In addition, cryptographic approaches used in the communication of devices, cryptographic techniques, security protocols are also mentioned as other important steps to work. They noted that the detection of unusual processes, the development of vulnerability detection approaches of intelligent systems are some of the important needs, and they have questioned, how aware we are of the risks associated with the ever increasing IOT approaches.

Ahemd, and Shah Wahid claim that, next few years, than 50 million devices will be part of iot system and the security of the IOT network is one of the top priorities. In their work, they have examined security vulnerabilities in four layers of the IOT system (Detection, Networking, Processing and Application layers) and improved security solutions between 2010 and 2016 against these vulnerabilities. The authors emphasized that the IOT approach will be one of the most important systems threatening personal information in the coming years, as it is a very fast-spreading and daily life-affecting approach. Authors who indicate that vulnerabilities in the layers of the IOT system and the communication between the sensors and devices used can be exploited. They also use different topics such as firewalls, anti-virus, anti-spyware, Access control Lists, have proposed solutions in their titles.

S.Sridhar and S.Smys stated that IoT systems may be attacks the hardware, software and network structure of devices due to the use of wireless network sensors. The authors have proposed the Intelligent Security Framework for IOT devices in their paper. They used Lattice-based cryptography as a method of end-to-end asymmetric cryptography to improve the security of IoT gateways and low-power sensors in architectures they proposed, as well as cloud protection and system malfunction protection. The keys created by the proposed architecture's asymmetric key cryptography approach in nodes and the message is used in the transmission DDOS attacks, carried out by listening to be protected from attacks and also attacks the quantum algorithm It was. The authors suggested that there is a unique identifier for each device in the proposed protocol, suggesting that this approach is quite successful at the authentication and verification stages.They noted that many attacks on the components of the IOT approach could take place and emphasized that the consequences of not taking the right security measures could be disastrous in terms of protecting personal information.

Z. Ling and colleagues focused on the security and privacy issues of the IOT system in their paper and examined the IOT approach with two different studies. The authors first proposed a viewpoint based on risk analysis using ten simple functional structures in the IOT system. they offer, the software forms the IOT systems, network and cloud system big data in terms of providing end-to-end security that creates a logical expression analysis perspective It has. In addition, the authors of the Edimax IP camera systems that they perform vulnerability analysis, exploit the system and claimed that the whole control was taken over by themselves. Authors can identify attacks like those they do in the real world and identify potential security vulnerabilities the results show that the alarm level continuously increases in the IOT approach.

Atkinson et al can be estimated in this study that, they can guess many personal data during wireless network usage in via mobile devices. The work they have conducted demonstrates that, when a mobile device is using which is connected to the Internet with wireless network has broadcast many personal information. Atkinson and colleagues have tried to obtain personal information about individuals using some of the applications. They are gathering data remotely in the air. After get all internet traffic, they are tring to analyze this data [6]. They can just make sense time and frame size because of encryption between mobile devices and wireless network. Authors indicated that they get %99 success rate with "Random Forest classifier" methods in the observing set. They found that when they tried to get traffic generated by more than one device and try to observe in real time, the success rate decreased to 84% in the controlled environment and 67% in the environment when simulating real life. With this study, Atkinson and his colleagues stated that a mobile device which is connected to the wireless network by internet, can be detect many personal data by using a remote identification mechanism. Also this work point out that the changes that can be made to cover the vulnerabilities and can be the basis for future wireless network protocols can be revealed by working on wireless networks in large areas.

AG Finogeev and AA Finogeev investigated problems in the detection of SCADA systems' attacks on wireless network structures (WSN) by examining the data transmission in the automated process control systems (APCS) and SCADA systems with an information security perspective [7]. As a result of the classification performed by the authors examining the attack detection studies on the sensor networks and attacks from outside the SCADA system can be detected by the attackers. The authors emphasized that most of the attacks in the SCADA systems in the articles were staffed by working personnel. In order to solve the problems arising from personnel, it is proposed to provide necessary education in the field of information security, to provide the basis of trained and competent personnel, to define the necessary rules in the internal system and to keep them under supervision. Also, in the works performed on 128 bit AES encryption key used for wireless network construction, no solution can be produced despite using "ZigBee Pro Feature Set specification" system. In the case of SCADA systems, the routing table that can be used on the wireless network structure is proposed to use hybrid switching. This approach give opportunity to protect system from attack. Authors thinking that for further work, the approach to hiding data into the data (steganography) methot can be use for security. Syncing value and time value can be hidden in data value which is used in wireless network (session key), so it may take a safer state of the communication of PLC with SCADA systems over a wireless network statement they have.

P. Jindal and B. Singh have performed extensive experimental work on the security level of network structure with various scenarios in the WLAN architecture working in the IEEE 802.11 b / g / n stand [8]. The authors intended to measure the security level and determine the performance of the network structure using experimental data such as correct data transmission, response time to request, encryption structure, data loss, delay in packet. The authors have tested the WEB, WPA, WPA2, AES and TKIP encryption approaches on WLAN in accordance with protocols on many different combinations. As a result of the experiments performed, the security level increases and the functional network performance decreases as the IEEE standard 1 rule structure (SSID) goes to the 9th rule structure. As a result of the experimental observations, WPA / AES, WPA2 / AES encryption performance is better than WPA / TKIP and WPA2 / TKIP encryption. In conclusion, this article gives experimental results and superiorities against each other in detail for different security protocols. How to use the protocols for the applications to be used or the infrastructure to be installed can be easily performed by examining the results in the article.

FA Alaba and his colleagues have examined the security vulnerabilities in Internet of Things (IOT) which is one of the most studied areas in recent years. IoT is a technology based on the relationship between objects and sensors without human factor [9]. While many different industrial areas show that the IOT approaches have been developed rapidly because of reduce human errors and delays. it is reported that the emerging technology poses great threats to the security vulnerabilities it brings with it. The authors addressed two different areas as security weaknesses. One of them is IoT systems communication vulnerabilities. IoT system use various technology to send data each other. This necessity cause some vulnerabilities. Other weakness is hardware vulnerebility. IoT systems occur different component and each of them has different vulnerabilities. Because of that They preffer some control mechanism. Their suggestion include to generate control messages on this infrastructure to prevent attacks on the model that LLNs (low-power and lossy networks) network system. This system prevent the attack of smart cards and programmed objects from misleading the system by generating their own packets during communication. In addition, the presence of small memory areas on IoT devices, the provision of encrypted communications and frequency hopping are among other security measures taken. Datagram Transport Layer Security (DTLS) and Constrained Application Protocol (CoAP) protocols are also used for communication in Iot system. In the examinations carried out by the authors, IoT structure is reported to be composed of 3 different layers as application layer, detection layer and network layer. These layers are subdivided into different usage areas and system components, and each component has been described as having various security vulnerabilities originating from its intended use. The authors should be familiar with the protocols used for each layer (CEN, ETSI, etc.), the protocols used (DSRC), devices (smart devices, RFID, smart medical cards etc.), communication formats used for communication of devices (bluetooth, ZigBee Wi-fi etc.) and classified the threats to IOT systems as misuse, hacking and cyber attacks. The authors classify security holes that can be formed by a scenario involving many areas such as the health sector, mobile systems, home security systems, mobile game sector, where IOT systems are used extensively for different purposes, and superficially transmit the necessary measures against the attack. The scenarios classify attacks that can be performed against these threats by classifying the authentication and authorization systems, firewalls, threats based on smart applications, threats based on network architecture, data transmission and communication-related threats, and hardware threats. As a result, the authors have presented the network-based threats of each component and system used in IOT construction and have introduced the cyber attack approaches that can be implemented towards these areas. In the initial stage and stated that insufficient security measures in IoT that there are many security precautions to be developed in the article and that the precautions should be taken immediately in this area.

Pietro and his friends work ad-hoc wireless network. They said that coverage area, cheaper services, easily domain changed is extremely useful [10]. However, due to the fact that the system has a lot of domain, it can be easily accessed by attackers everywhere, security measures are inadequate, attackers have been able to make many attacks like Dos attacks, interception attacks, etc., is much easier than other wireless network approaches. The authors divided the ad-hoc wireless network structure into low-end network structure and high-end network structure. The low-end network structure is classified as the network structure resulting from the communication of the sensors, and the high-end network structure is classified as the traffic originating from the communication of the network devices. According to the authors, security vulnerabilities in the ad-hoc structure can be overcome by taking precautions in the data collection and encryption steps. Low-end structure to express a symmetric encryption High-end encryption with the future structure of the public-switched data transmission Is the case by the attackers made several attacks may fail It was.

Previous work on these issues has highlighted the importance of security awareness among users of IOT devices. In the methodology part of this study, a new method developed to compare the results obtained by Yavanoglu et al. in 2015 with IoT awareness is presented.

III. METHODOLOGY

In this section, the methodology of analyzing wireless security awareness of the selected regions is described, including the scans, data analysis, analysis and screening of wireless network devices as well as the methods to be followed.

Residential and workplace scans were conducted between 09:00 and 22:00 due to the scope of the scan. Several tests and applications have been carried out in order to be able to list wireless data devices in the surrounding districts and to obtain data. As a result of these tests and researches, it was decided to use the app Wifi-Collector, an application developed by Nirsoft, which provides the most comprehensive way to scan IoT and network devices that share over wireless access points and to process on smart devices in particular [11].

The selection of the region, the collection of data and the methods used to process the data are presented in Figure 1.

In the field selection section, which is the first step of the field study, provinces that the research should be done have been determined.

In the next step, mobile teams navigate the selected areas with the aid of GPS (Global Positioning System) and map applications, then gather the metadata of IoT and wireless network devices via Wi-fi Collector application.

The data processing step focuses on extraction and categorization of the metadata gathered in the previous step.

In data visualization, the processed data is visualized and prepared for the assessment step.

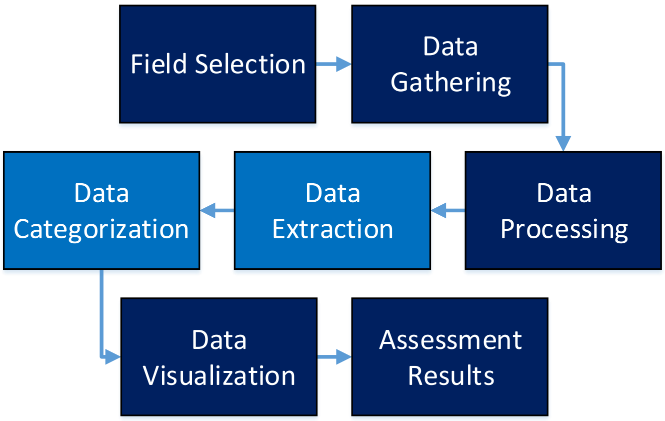


Figure 1. Methodology of the work

A. Field Selection

The region was selected in such a way that all the counties of Ankara were considered. All of the districts regardless of any criteria have been included in the project.

B. Data collecting

In the data collection step, Warwalking and Wardriving methods are used to obtain data on the devices in the selected zone boundaries. Said methods can be used to scan the selected region for the wireless network devices in the area with a vehicle or by foot. The data obtained are as such:

- Wireless device name (SSID),
- Brand of device,
- Signal level,
- Security standard,
- WPS support,
- Scan date and
- GPS coordinates.

In this study, IoT devices are identified using Wardriving and Warwalking methods in the field, with the aid of GPS and geolocation applications. The recorded data and visited regions are examined in the data processing module.

C. Data Processing

At this stage, the same data are first distinguished by deleting them in order and sorting them according to the metadata disclosed in the data collection section. The obtained data are divided into categories after they are edited, thus providing a more accurate way to analyze the data. After editing the data, they are categorized according to their area, WPS characteristics, encryption types and frequency they are broadcasting. A variety of tables and graphics have been created to provide insight into the content of the data.

D. Data Visualization

After the data categorization step, the data is visualized to further understand and analyze. Additionally, a map is created using the geolocation info collected in the data gathering step.

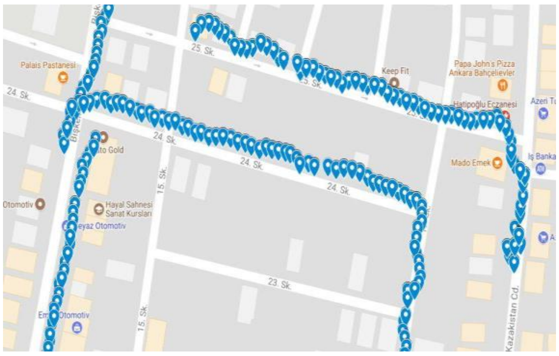


Figure 2. A map visualization of the site survey.

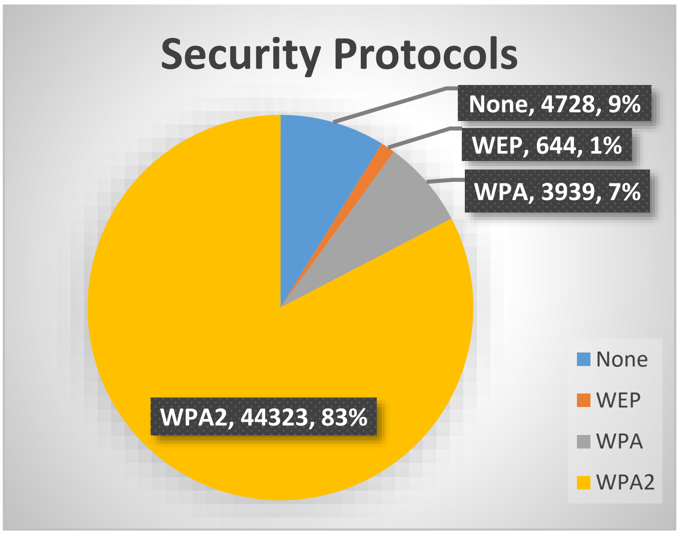
E. Assessment Results

The data that are interpreted by being extracted, categorized and visualized are compared with similar data in other regions and studies. In addition to this comparison, the relationship between the IoT device awareness and the regional data is analyzed using the broadband access status and device availability status data of TUIK.

IV. EXPERIMENTAL RESULTS

The field survey is conducted according to the methods specified in methodology section and the results are given in this section.

During the experiment, a fieldwork has been carried out for the province of Ankara, within the districts Gölbaşı, Yenimahalle, Sincan, Etimesgut, Altındağ and Mamak, for the purposes of collecting data regarding IoT and wireless devices. As a result of the field work, a total of 50855 IoT devices were collected. It has been found that upon processing the data and examining it, only 1787 of the 53664 devices are IoT devices; it is seen that 42027 of all devices are WPA2, 3939 are WPA, 644 are WEP and 4728 are not password-protected.



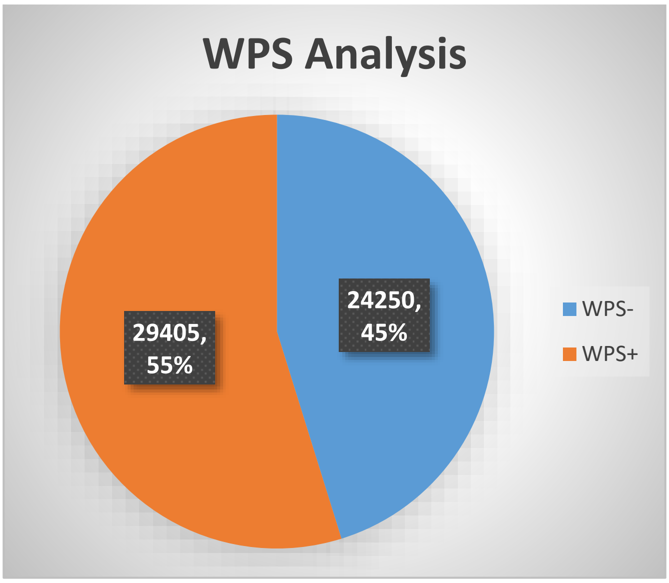
Graph 1. Encryption types used in IOT devices

Graph 1 compares the cryptographic methods of IOT devices collected from the fieldwork.

WPA2, which is currently the most advanced security device on the market, shows an increase in awareness among users when it comes to 83% of all devices and 72% of the work done in 2015.

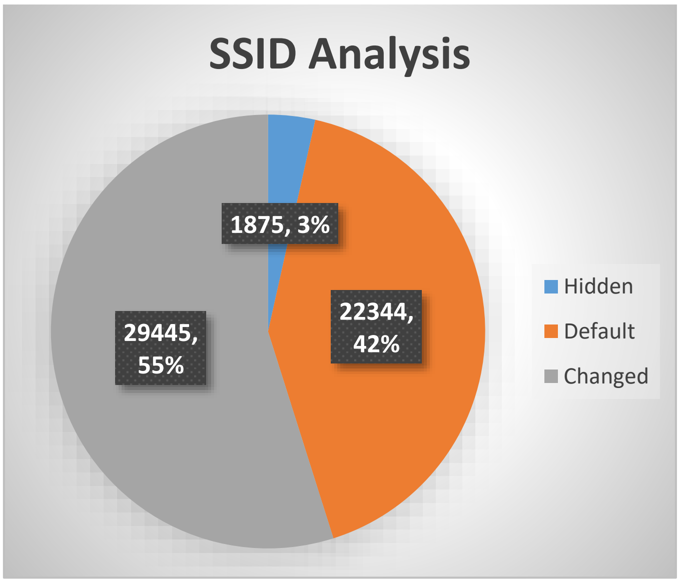
Wi-Fi Protected Setup (WPS) is an Internet security standard that allows users to connect to a wireless network without having to enter long passwords via a key. However, keeping the WPS open can make the wireless network devices vulnerable [12].

It shows that there is no specific change in awareness of the WPS when compared to the 55% rate quoted in the chart at 57% of the 2015 study.



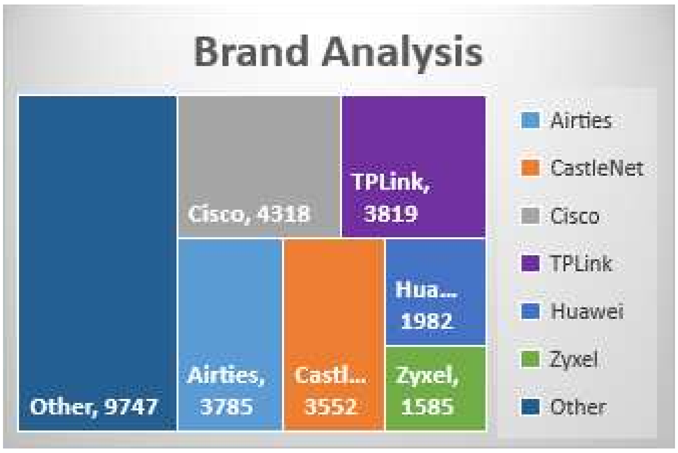
Graph 2. WPS analysis of IoT devices

Graph 3 compares the SSID names of network devices participating in the research.



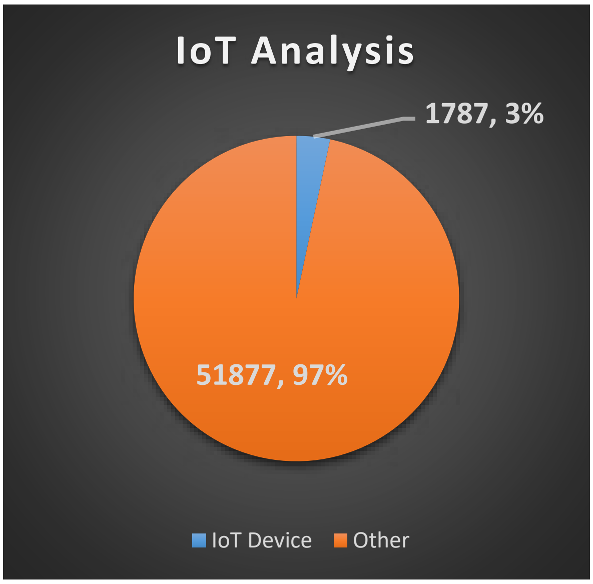
Graph 3. SSID analysis for IoT devices

SSIDs are the name used by the devices to identify themselves to users. SSIDs can consist of a maximum of 32 alphanumeric characters and can be changed or hidden according to the user's request. Leaving SSID as it is can make the modem vulnerable to various attacks [13]. In the study conducted in 2015, a proportional reduction in the SSID change is observed when 60% of the SSIDs are changed.



Graph 4. Brand analysis of IoT devices

In the brand analysis data, modems with only a valid brand name are handled, while in the other category, brands with a ratio of less than 2% are indicated. Compared to the research in 2015, it can be seen that Huawei has decreased while TPLink and Airties brands have increased and Cisco and CatleNet have entered the list.



Graph 5. The ratio of IoT devices to wireless network devices

When we look at the schematic, it can be seen that only 3% of the existing devices can be found as IoT devices. This rate covers only IoT devices with wireless access enabled and does not include IoT devices running on internal networks.

The gathered results are compared with TUIK IoT device and broadband usage data and the impact of IoT device awareness on these data are given in the conclucion section.

V. CONCLUSION

In the study made in 2015 by Yavanoglu et al., a criterion named KFP is given, aiming to calculate the wireless awareness of the residents living in an area using the wireless device data in the area. Upon gathering up all the results and comparing them to the 2015 results, which has found the KFP of Ankara as 58 over 100; current results show that the KFP as 61. This shows that the wireless awareness has increased since 2015 by 3.

Since 2015, some wireless standards have changed; thus there is a need for a more accurate way to represent IoT awareness.

WAP (Wireless Awareness Point), is a point system aiming to estimate wireless security awareness of IoT device users by the security protocol, SSID and WPS statuses while considering the latest available security standards at the province.

WAP is calculated by this formula:

$$\frac{\sum \frac{\%SPd * SPp}{SPa} + \sum \frac{\%SSIDd * SSIDp}{2} + \%WPS^{-}}{3}$$

Formula 1. Wireless Awareness Point formula

SPd represents currently used wireless security protocol of the IoT devices, namely “None”, WEP, WPA, WPA2 and newly added WPA3. SPp is the security level points according to security protocol, “None” and WEP has the SPp value of 0, since WEP is already known to be vulnerable more than its successors. WPA has the value of 1, WPA2 has the value of 2 and WPA3 has the value of 3. SPa is the SPp of the highest security protocol available in the region. SSIDd is the SSID status of the device while SSIDp is the SSID points for different SSID statuses. Default SSID’s have the value of 0, whilst changed ones have the value of 1 and hidden SSIDs having 2, being the most secure way. Lastly, $\%WPS^{-}$ represents the percentage of devices with WPS setting disabled.

Upon calculating the wireless awareness point using the WAP method, we find the wireless awareness of Ankara as 54 over 100 points.

TABLE I. COMPARISON OF RESEARCH DATA AND AWARENESS CRITERION IN PERCENTAGE

Feature	**Category**	**Ankara-2015**	**Ankara-2018**	**Change**
SSID	***Default***	36	42	+6
	Changed	60	55	-5
	Hidden	4	3	-1
Security standard	***None***	7	9	+2
	WEP	3	1	-2
	WPA	18	7	-11
	WPA2	72	83	+11
	WPA3	0	0	0
WPS	***Enabled***	57	55	-2
	Disabled	43	45	+2
Awareness criterion	***KFP***	58	61	+3
	WAP	52	54	+2

This work aims to analyze the relationship between IoT security awareness and broadband data and IoT device usage. Wardriving and Warwalking methods described in previous sections are used for this study. In selecting these methods, consideration is given to the effectiveness of the method and its compatibility with the work to be done later, and a multiple-step-methodology of field study is proposed in the methodology section. During the work, 53664 active wireless devices including IoT devices are analysed, which percentages are shown on Table I. It can be observed that while WEP is the least used security standard, WPA2 is the most widely used. Since WPA3 is relatively new and currently there are no WPA3 supporting wireless routers, there are not enough data to comment on its impact on user awareness. As of 2017, every 28 in 100 households in Turkey have at least one IoT device except modems [14] and every 78 in 100 households have a way of broadband access [15]. Compared to these stats, it is assumed that there is an increasing need to improve IoT and wireless security awareness in Ankara.

VI. References

[1] Hashem, I.A.T., Chang, V., Anuar, N.B., Adewole, K., Yaqoob, I., Gani, A., Chiroma, H., The role of big data in smart city, October 2016, Pages 748-758

[2] Domenico Raguseo, (2016 December 16) “2016: The Year of the DDoS Attack” [Online]. Available: https://securityintelligence.com/2016-the-year-of-the-ddos-attack/

[3] DAVID BISSON, (2016 November 29) “The 5 Most Significant DDoS Attacks of 2016” [Online]. Available: https://securityintelligence.com/2016-the-year-of-the-ddos-attack/

[4] Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı – BTK, 2014.

[5] Yavanoğlu, U., Kapkiç, A., Yağcı, S.T., Aktepe, C., Tunçer, G., Kablosuz Ağ Cihazı Erişim Güvenliği ve Farkındalık Analizi: Ankara Örneği, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:1, No:1, S:11-19, 2015

[6] John S. Atkinson, John E. Mitchell, Miguel Rio and George Matich, “Your WiFi is leaking: What do your mobile apps gossip about you?”, Future Generation Computer Systems, 2016, Elsevier.

[7] Alexey G. Finogeev, Anton A. F inogeev, “Information attacks and security in wireless sensor networks of industrial SCADA systems”, Journal of Industrial Information Integration 5, 2017, Elsevier, 6–16

[8] Poonam Jindal *, Brahmjit Singh, “Quantitative analysis of the security performance in wireless LANs”, Journal of King Saud University – Computer and Information Sciences (2017) 29, 246–268

[9] Fadele Ayotunde Alabaa, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, “Internet of Things security: A survey” , Journal of Network and Computer Applications 88, 2017, pages10–28

[10] R. Di Pietro, S. Guarino, N.V. Verde, J. Domingo-Ferrer, “Security in wireless ad-hoc networks – A survey”, Computer Communications 51 (2014) 1–20

[11] Nirsoft, Wifi-Collector. [Online]. Nir Sofer, 2014.

[12] Viehböck, Stefan. (2011-12-26) "Brute forcing Wi-Fi Protected Setup" [PDF]. Available: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[13] Susan Young, Dave Aitel, The Hacker’s Handbook: The Strategy Behind Breaking into and Defending Networks, 2003, pp. 588-589.

[14] Türkiye İstatistik Kurumu, Availability of devices in households, 2004-2017.

[15] Türkiye İstatistik Kurumu, Percentage of households with broadband access by Classification of Statistical Regions (SR) Level-1, 2011-2017.