Journal of Engineering and Applied Sciences 13 (9): 2668-2671, 2018
ISSN: 1816-949X

Internet of Things-Proactive Security Approach

Ali Shawket Thiab, Abdul Samad Bin Shibghatullah and Zeratul Izzah Mohd Yusoh
Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Abstract: The proposed solution in this study is to use a proactive WPA/WPA2 approach in order to secure the access link side of the IoT. The proactive approach is controlled by a DDWRT router which changes the password proactively after a specific time interval after instructing the connected devices to do so as well. The solution uses an IPsec security on the end routers to ensure the data security on the public internet side of the connection. This simple solution allows using a simple Wi-Fi setup or even better to use the current Wi-Fi infrastructure which is available in almost every enterprise or home environment where the IoT is needed. A separate Wi-Fi network will be created for the IoT devices, so that, the current normal users experience will not change. The solution proved to be secure by evaluating the three security pillars: confidentiality, integrity and availability.

Key words: Security, Wi-Fi, internet of things, SSL, solution, confidentiality, integrity

INTRODUCTION

Today's world was not so a couple of decades ago. A substantial technology leap happened when the Internet became public in the 1980's allowing people to surf the web, send emails and share les. It is always exciting to look back and see how much the world has advanced and how the internet helped in this process (Evans, 2011). It is a fact that the internet continues to evolve shaping our everyday life in the process. The internet of things is thought to be the next evolution of the internet (Evans, 2011) as it is going to provide a networking infrastructure allowing trillions of devices to collect data and communicate with each other and with other devices to make processed smart decisions. The devices can be any object or anything embedded with the needed hardware and software that are required for processing and networking capabilities. In other words, IoT will be a network of the currently existing rather powerful internet devices like smart phones, personal computers and servers with addition of new less complex devices like heart or brain activity monitoring sensors, automobile motion or brake sensors or any environmental sensors (Chase, 2013). Therefore, the IoT will allow a new era of data exchange and decision making. That is why in 2008, the US National Intelligence Council (NIC) reported that by 2025 internet nodes may reside in everyday things, food packages, furniture,study documents and more (Fingar, 2009; Palattella *et al*., 2013; Reiter, 2014).

Developments point to future opportunities and risks that will arise when people can remotely control, locate and monitor even the most mundane devices and articles. Internet of Things networks need to be connected on daily basis, a need for flexibility and adaptive configuration arises depending on the complexity, physical environment, available power and security requirements (Kurose and Ross, 2013). In the majority of the cases, the wireless solution is more suitable for the internet of things networks than the wired one as it is easier to set up in tricky physical situations and cheaper to install and maintain. However, a care should be taken when choosing the right wireless technology that is adequate for the present circumstances (Babar, 2015; Singh, 2000; Kahn, 1974; Raza, 2013; Bontu *et al*., 2014).

Internet of things networks are currently being implemented in many enterprise and home environments. The opinions about the Internet of Things burst are vacillating and there is still no confidence in the available security solutions (Kamoona and El-Sharkawy, 2015). Some surveys like show multiple security aws that are deleterious to the development of the internet of things. There are currently numerous implemented and proposed solutions to secure the internet of things. Many of them are rather complicated or do not provide a robust solution for low power devices that use Wi-Fi connectivity. This emergence of the internet of things will be hindered without finding an easy, simple and feasible solution that facilitates the ubiquity of such networks in every environment with minimum efforts (Fingar, 2009).

The aim of this study is to propose a new feasible easy-to-implement solution that uses the current infrastructure of the Wi-Fi networks to form a paradigm

Corresponding Author: Ali Shawket Thiab, Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

that proves secure and saves bandwidth, delay and energy consumption which are the main pillars for the internet of things applications.

MATERIALS AND METHODS

The IoT is the natural evolution of the internet. Its fast growing nature and being an integral part in daily sensitive services like industrial, enterprise, home networking and education raises some security concerns. While the IoT connectivity can be any of the wired or unlicensed wireless technologies like Bluetooth, Bluetooth Low Energy (BLE), ZigBee and Wi-Fi, the target of this thesis is to find a security solution for the pervasive wireless technology, the Wi-Fi.

The proposed solution uses a DD-WRT router to manage the PWPA and IPsec security, a Thingspeak server on a Linux machine as a cloud application and multiple Freescale K64f embedded systems to simulate a typical internet of things scenario. It is important to note that it is assumed in this research that the adversary does not have physical access to the routers in which they can log in to the router or simply disconnect the connectivity or unplug it to remove the service as such actions will easily be noticed by the administrator.

System design: The hardware system design is very simple as no explicit extra hardware needs to be added unless the router does not support DD-WRT Software in which an embedded system is needed. To get connected for the first time, users can simply enter the current password or use an NFC to get authenticated and connected. Then the router generates a predefined length strong random password that incorporates multiple techniques for strong passwords generation like mandating the choice of some special characters and different upper and lower case letters. Each of the connected users then opens a TCP connection to the listening server which provides the new password and a timeout for the current password expiration. The router can be set to accept connections to as many users in the network so that no TCP SYN connection initiation request will be rejected. The router and clients operate normally after that until the timeout occurs. When the timeout occurs, the DD-WRT router applies the new distributed password and all the clients apply the new one as well. All the operations are seamless and in case any of the devices gets disconnected, it will try to connect with the newly advertised password from now on. The above explanation shows that except for the first time connection everything else is done automatically by the code on the DD-WRT router and the connected clients and no user intervention is required.

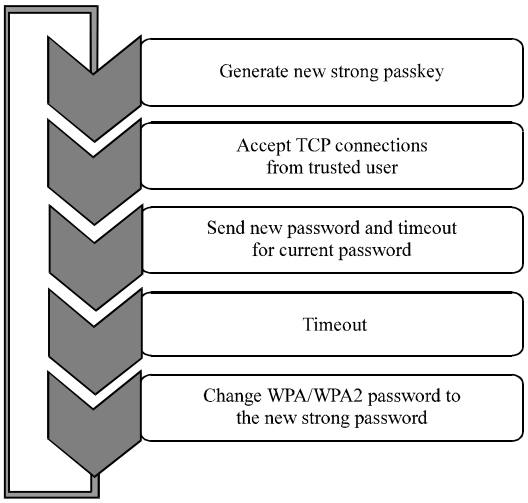

Fig. 1: DD-WRT router simplified flowchart

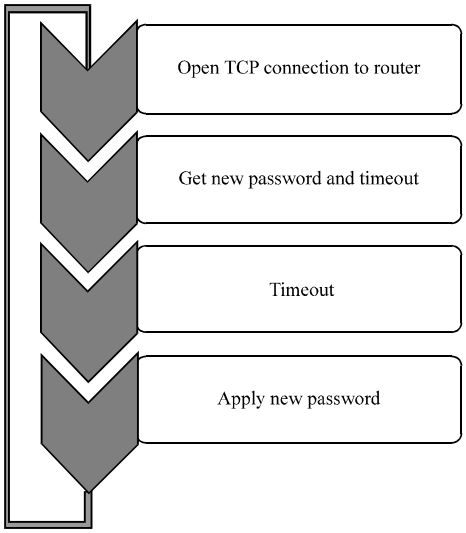

Fig. 2: Trusted client simplified flowchart

Wi-Fi networks: The aim of this research is to propose and implement a new algorithm that solves in a seamless way, the problem of WLAN WPA/WPA2 pre-shared key generation, distribution and administration by changing the passkey proactively and automatically with the trusted clients without any required intervention from the users using only the same DD-WRT access point that is used to provide the connectivity in the first place (Fig. 1).

Security: The proposed scheme is to use a proactive WPA/WPA2 approach (Fig. 2). The DD-WRT router generates a new fixed length random password every present time interval (2 h by default) then uses this strong password as the new pre-shared key. Before the password

change occurs, every connected user will automatically open a TCP connection over the same secured Wi-Fi link and fetch the new password and the time until the new password will be applied. In that case, when the timeout occurs, all the wireless devices in that network will seamlessly change the password and hence no need for any user intervention. For simplicity, the first time the users get connected to the router should use either a Bluetooth transceiver or a simple NFC then after that the proactive WPA/WPA2 scheme will take over to change the password in the router and all the trusted already connected devices, Fig. 1 and 2 show the flowchart of the router and a trusted connected client.

RESULTS AND DISCUSSION

Security analysis: Since, the proposed solution does not change the basics of the WPA/WPA2 personal model, it uses all the strength points of that model and adds to that some enhancements to target its weaknesses. The proactive approach for changing the password for the whole network eliminates the possibility of an attacker capturing a handshake messages exchange and trying to use online dictionary attacks to get the password. Taking into account the considerable amount of resources that requires an adversary to get the password by then our system had already generated and distributed a new strong password along with a new timeout and thus it would be meaningless for an attacker to perform online dictionary attacks.

WPA/WPA2 and IPsec: To provide an end to end internet of things security, an additional component which is IPsec is added. The Proactive Wi-Fi Protected Access (PWPA) was suggested as a counter measure to the weaknesses of the 802.11i standard to protect the wireless access network which means that the data on the rest of the public internet is still vulnerable.

The Internet Protocol security (IPsec) should be implemented between the two access routers to achieve end to end security. Depending on the application and the available bandwidth in the end to end network, either the Encapsulation Security Protocol (ESP) transport or tunnelling mode can be implemented to provide end-routers data security. Figure 3 shows the actual proposed IoT security solution.

PWPA configuration: To setup the IoT sensors and embedded systems for the first time, an Android application was developed and used to fetch the current WPA password and install it in the embedded system using the IR and BT interfaces. The security control is passed to the PWPA solution where the password change will take place between the AP and the connected devices in private channels using the WPA2 security model (Fig. 4).

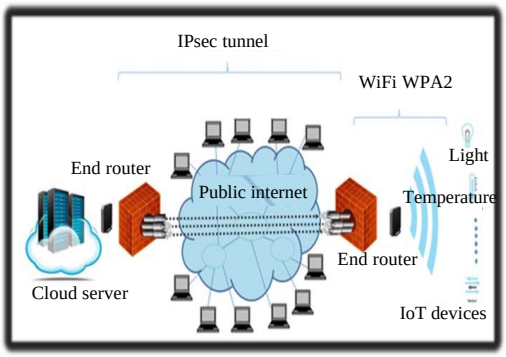

Fig. 3: Proposed security implementation solution

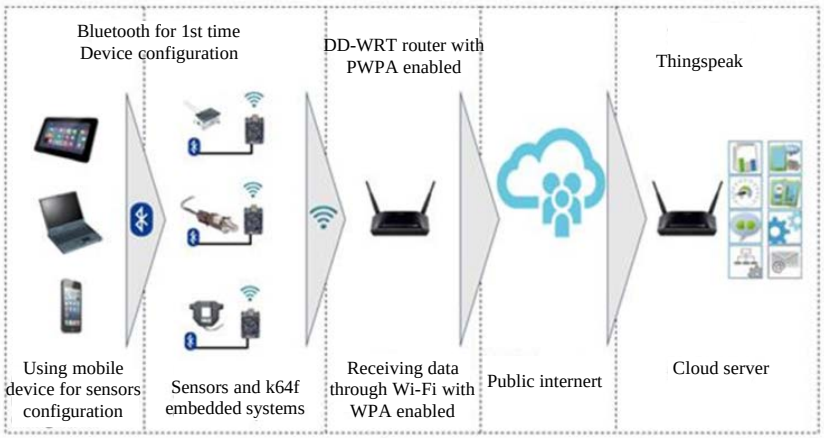

Fig. 4: PWPA solution IoT connectivity

CONCLUSION

This simple solution allows using a simple Wi-Fi setup or even better to use the current Wi-Fi infrastructure which is available in almost every enterprise or home environment where the internet of Things is needed. A separate Wi-Fi network will be created for the internet of things devices, so that, the current normal users experience will not change. The solution proved to be secure by evaluating the three security pillars: confidentiality, integrity and availability. More even, the solution improved the overall network performance by reducing the amount of delay experienced and increasing the bandwidth efficiency when compared to the end to end security solution using SSL. By shifting most of the encryption processing from the low power IoT devices to the router which is connected to the mains, the solution reduced the amount of processing done by those devices and thus greatly increases their battery life which is a major concern in the internet of things industry.

RECOMMENDATIONS

The proposed solution in this study used the proactive WPA/WPA2 to protect the access link and IPsec security to secure the data on the internet side. A possible future research can target the availability aspect of the WPA/WPA2 access networks. While the 802.11i standard has strong measures for both confidentiality and data integrity but very little research targeted the defense against DoS attacks. Although, some intrusion detection systems or other solutions can be implemented but an integral solution that is part of the Wi-Fi standard should exist.

REFERENCES

Babar, S.D., 2015. Security framework and jamming detection for internet of things. Master Thesis, Department of Electronic Systems, Aalborg University, Aalborg, Denmark.

Bontu, C.S., S. Periyalwar and M. Pecen, 2014. Wireless wide-area networks for internet of things: An air interface protocol for IoT and a simultaneous access channel for uplink IoT communication. IEEE Veh. Technol. Mag., 9: 54-63.

Chase, J., 2013. The evolution of the internet of things. Texas Instruments, Dallas, Texas, USA.

Clarke, R.Y., 2013. Smart cities and the internet of everything: The foundation for delivering next-generation citizen services. Tech Support, Alexandria, Louisiana.

Evans, D., 2011. The internet of things: How the next evolution of the internet is changing everything. CISCO. IBSG., 1: 1-11.

Fingar, C.T., 2009. Global Trends 2025: A Transformed World. DIANE Publishing, Collingdale, Pennsylvania, ISBN:978-0-16-081834-9, Pages: 99.

Kahn, D., 1976. The Codebreakers. Sphere, London, England, UK., ISBN:9780722151495, Pages: 476.

Kamoona, M. and M. El-Sharkawy, 2015. Flexiwi-fi security manager using freescale embedded system. Proceedings of the 2015 2nd International Conference on Information Science and Security (ICISS), December 14-16, 2015, IEEE, Seoul, South Korea, ISBN:978-1-4673-8611-1, pp: 1-4.

Kurose, J.F. and K.W. Ross, 2013. Computer Networking: A Top-down Approach. 6th Edn., Pearson Education, USA., ISBN-13: 9780132856201, Pages: 862.

Palattella, M.R., N. Accettura, X. Vilajosana, T. Watteyne and L.A. Grieco *et al*., 2013. Standardized protocol stack for the internet of (important) things. IEEE. Commun. Surv. Tutorials, 15: 1389-1406.

Raza, S., 2013. Lightweight security solutions for the internet of things. Ph.D Thesis, Malardalen University College, Vasteras, Sweden.

Reiter, G., 2014. Wireless connectivity for the internet of things. White Paper. Texas Instruments Inc., USA., June 2014.

Singh, S., 2000. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Industries Inc., Vanderburgh County, Indiana.