VR Training for Security Awareness in Industrial IoT

Vasiliki Liagkou, Chrysostomos Stylios

VR Training for Security Awareness in Industrial IoT

Vasiliki Liagkou and Chysostomos Stylios

Department of Informatics and Telecommunications, University of Ioannina, Kostakioi Arta, GR 47100, Greece. liagkou@kic.uoi.gr, stylios@uoi.gr

Abstract. Virtual Reality technology provides new solutions and more efficient opportunities for a revolutionary new manufacturing training environment. This work focus on presenting a VR training environment on a new and promising IoT communication protocol, the Low-Power Wide-Area Networks (LPWAN). The LP-WAN have recently emerged as a standard IoT communication system that satisfies the challenges of industrial networks by enhancing their reliability and efficiency. The LPWAN is a promising response to the limitations showed by current IoT technologies. Here are exploited the possibilities of the 3D virtual world technology to create experiential learning simulations, which address IoT users' real needs for privacy and security awareness. To this aim, a 3D role playing game is introduced and a group of master students have evaluated its ability to help them for handling the security features of LPWAN.

Keywords: Virtual Reality, VR Training, Industry 4.0, E-learning, Internet of Things, LPWAN.

1 Introduction

Nowadays Virtual Reality (VR) is a new pillar for developing training and learning environment for Industry 4.0. VR is able to provide an integrated training environment where users are able to design, test and perform various manufacturing process activities like being on a real workspace. VR has many abilities that make it suitable for a novel manufacturing training environment ([1]). Virtual reality applications for training and learning propose have attracted great interest from the research community ([2]-[3]). VR have proposed to develop various training scenarios mainly based on 3D role playing games. But, only a few VR scenarios are focused on security issues ([4] - [5]). The majority of simulations and games have been developed in role based use case scenarios and they use two dimensional graphical representations. In this work, we present a 3D training environment on privacy and security issues for an IoT industrial environment.

Collaboration networks ([6]) can help Industry 4.0 to support several collaboration environments but this collaborative link between enterprises, customers, employees, and systems is vulnerable to cyber-attacks [7]. The security challenge is a crucial requirement for industry 4.0 to realize a reliable, trustful and seamless cooperation between enterprises, employees and customers. The new communication technologies

include various security mechanisms that can reduce security risks but enterprises and employees hesitate to use them due to their lack of skills and awareness.

To this direction our work tries to investigate the capabilities of Virtual Reality (VR) technology for familiarizing users with the functionalities of a promising Internet of Things communication system suitable for industrial networks... The authors introduce a VR training scheme that help users to investigate the security mechanisms in Low-Power Wide-Area Networks ([8]). The scope of the proposed VR training scheme is to increase user security awareness by helping users to identify the risks and vulnerabilities that they should have in mind when they use an IoT protocol.

The Internet of Things (IoT) is a basic component of the fourth industrial revolution: Industry 4.0. On the other hand, Low-Power Wide-Area Networks (LPWANs) are becoming one promising IoT communication protocol for the Industrial IoT (IoT) ecosystem since it can provide long-range communication at very low speed to an industrial IoT network. The current implementations could replace 2G/3G/4G/5G cellular networks because LPWAN can also increase the transmission range of devices by trading-off data transmission rate while preserving at the same time power consumption at low levels [8]. The Low-Power Wide Area Networks (LPWANs) exploit the abilities of low frequency signals to transmit over any obstacle or using multipath propagation. They are widely used because of their robustness and reliability [9]. LPWAN technology has becoming promising and widely adopted for IoT networks because it supports the connection of IoT devices at a distance. LPWANs main characteristics include energy autonomy for the IoT devices along with low cost, great coverage capabilities that are requirements of the Industry 4.0 applications [10].

1.1 Outline

Our work focus on a new and promising IoT communication protocol, the Low-Power Wide-Area Networks (LPWAN) and it uses a VR training environment for helping users to explore its security mechanisms. The LP-WAN have recently emerged as a hopeful IoT communication system that can satisfy the challenges of industrial networks by enhancing their reliability and efficiency [11]. The LPWAN can be a solution to the limitations showed by current IoT applied approaches, but their implementations were recently introduced, so it will be necessary users to acquaint their self with the provided security services and increase their awareness.
Our envision is that Virtual Reality can help potential users of Industry 4.0 to understand how the security mechanisms that are provided by LPWAN can be integrated through the whole industrial chain.

2 Security Challenge in Industrial IoT

Industrial IoT systems require an interconnected ecosystem that supports on-line access to interdependent and real-sensing data between enterprises in different

geographic places, thus these systems are not designed to be protected against a hostile unsecured internet environment. Security is a critical issue for novel Industrial IoT systems because the transmitted real-time data is confidential and its disclosure could cause huge financial loss for the industry. Nowadays, industrial competitors invest on "Industrial Espionage" in order to gain a completive advance e.g. by finding the design of a new product. Unfortunately, several companies spend a lot of effort to gather competitor's critical knowledge about its manufacturing processes, construction techniques, research plans or pricing/binding deals. If a competitor manages to gather any critical inside information, he could also have access to the enterprise's critical know-how and this fact will cause huge loss of enterprise's intellectual property.

In an IoT industrial system there is a horizontal interaction through the whole value chain from users and partners to customers thus huge amounts of data are being transmitted, audited, aggregated, annotated, stored and processed. If a competitor succeeds to gather a part of these collected data he can use it for creating a competitive advantage and he can also violate company's and customers' privacy ([12]- [13]). An IoT system must fulfill the security requirements for preserving data's confidentiality, integrity and privacy. Moreover, it is essential to extend the traditional security requirements in order to guarantee the confidentiality of the aggregated data from smart devices, especially when these devises are distributed in open and uncontrolled environments. Inherently, IoT environment is considered as a vulnerable link in an industrial network since they can be attacked by external devices for compromising their data and disrupting their operation. There are several efficient security solutions for IoT environment in the recent literature and the majority of them try to address resources constraints and scalability issues. The authors in [14] present an extended review of the most recent proposed security and privacy solutions in IoT systems.

Here we explore a new IoT communication protocol, the Low-Power Wide-Area Networks (LPWAN). Nevertheless the security remains a challenge that must also be considered in LPWAN ([15]-[17]). The authors in [18] present a set of security issues of LPWAN server that must be solved. An alternative key management scheme suitable for LPWAN is presented in [19]. Here we take a different direction and we try to increase users' security awareness in LPWAN by helping them to exploit the provided security mechanisms.

3 The VR training Scheme

In this work, we present a Virtual Reality (VR) scheme for training users to the basic security tools of LPWAN. The provided VR scheme help users to exploit the security issues and tools in IoT protocols and to better understand new risks and vulnerabilities that they should consider and address when they use IoT protocol.

Our VR training environment is decomposed in the following four phases that are implemented in VR 3D role based game scenario (see Figure 1). The user must

execute specific actions in order to successfully complete each phase and then he can proceed to the next one.

- *Introduction section* includes VR presentations and 3D visualization of the basic architecture and interactions in LPWAN.
- *Connection section* includes specific visualizations and steps so that the user to be able to understand how he can connect various devices in LPWAN. The user thought navigation is able to understand how the LPWAN authenticates his device by using a set of keys. Moreover here the user can select two types of IoT devices by following two distinct paths for joining the LPWAN (see Figure 3).
- *Security Parameters section* includes a more detailed description of LPWAN security mechanisms (see Figure 4). During this phase the user has to complete specific tasks in order to visualize how the network server generates and verifies the message integrity code and the corresponding keys.
- *Threat section*, visualizes how LPWAN tries to prevent replay attack

3.1 VR Scheme's Learning Achievements

The presented VR environment improves learning and training processes because it allows capturing attention to IoT users for increasing their awareness of the transmitted data. Our VR training scheme uses a VR character for informing the user about the set of actions that he can make for increase data's confidentiality. Moreover, VR application has included in several points of navigation a VR presenter for familiarizing the user with the available set of actions for protecting his transmitted data. (see Figure 4). The proposed scheme presents the security features and cryptographic information in a logic and direct way. The utilised VR scenario uses several VR spaces that simulate conventional actions. User's avatar could make specific actions like navigation, interaction with objects, communication and objects creation for gaining a dipper understanding of available security tools of LPWAN.

The provided VR environment helps users to think without being influenced by others and it provides a VR experience for a set of connection activities. LPWAN's security tools need specific actions from the IoT user for connecting his device in LPWAN. It is very difficult and unrealistic for users to execute such privacy policies and complex security mechanism. Our VR scenario trains the user how to connect his device in order to follow the right connecting procedures. We have implemented two different VR scenarios where the user's avatar follows specific steps and takes specific actions for connecting two different types of IoT devices, a refrigerator and a mobile phone (see Figure 3). The security factors that must be taken into account by an IoT user for connecting a static or mobile IoT device are different. Our VR scheme help users to understand what factors have to consider for joining in LPWAN network. The main goal of the presented VR platform is that gives the opportunity to the users use some security tools and to visualize a set of vulnerabilities. Most of the security and privacy concerns are invoke by misconfiguration of users. Our VR scenario visualizes in various steps of its navigation the potential risks and vulnerabilities that users should

consider and address when they use LPWAN protocol. The presented training environment assess users' knowledge about the provided security level for every action their avatar makes and evaluates if they understand the potential security flaws for its actions (see Figure 4).
Finally the user through his VR navigation can control connection procedures of IoT network. The interconnection and communication among the IoT devices and LPWAN server vary according to the user actions or protocols phase. Our VR model visualize transmitted data packages information and servers' interactions in order the user to understand how security policy of LPWAN works and what are the bounds of the provided security level. The user will be able to develop analytic and problem solving abilities. Our proposed VR scheme simulates experiential real life use case scenarios for solving problems in order users to gain a better comprehension of security risks in LPWAN and to help the to understand the functionalities of security mechanisms. User's avatar can throw a dice for generating a random number or it may pic specific boxes for constructing a network package.

4 VR Exploitation's Security Requirements

In this work, we investigate how VR technology is able to create and evaluate experiential learning simulations that address IoT users' needs for privacy and security awareness. It has presented a 3D role playing game, which was tested by a group of students who evaluated handling the security features of a LPWAN. The majority of IoT Industrial use cases must take a very careful consideration of security requirements and the implemented VR training platform investigate users' awareness to the following privacy and security concerns in IoT networks:

4.1 Confidentiality/Non Leakage of Sensitive Information

Leakage of critical information to unauthorized users or competitors is unacceptable for any industry. Usually, an industrial plan deploys a lot of smart devices that are used for collecting manufacturing processes data. If these devices are hacked by an attacker, then he can monitor all industrial activities and access critical information. To avoid this attack, LPWAN uses symmetric data encryption between gateway and devices. VR users through their navigation to the learning world are able to understand how the encryption of the payload is by default enabled in every transmission in LPWAN. Moreover, VR user understands what information is transmitted by an IoT device thus the VR environment visualizes the contents of every transmitted package by including the information of identifiers and payload data. Complementary LPWAN do not use a specific gateway, thus our scheme visualizes how the data frames do not include any gateway identifier. In this way, user must be aware that it is possible for anyone to receive the encrypted data packets. LPWAN tries to authenticate the IoT device for detecting the unauthorized access.

VR training schemes includes two different VR scenarios in order to visualize how the LPWAN network authenticates an IoT device by two different joining methods.

The application data should remain confidential against theft and tampering since application data of IoT could be industrial or enterprise. The VR training scheme shows at different scenes of the navigation that a 128-bit Application Session Key is used to encrypt the data frame between the IoT device and the application server (see Figure 4).

4.2 Integrity

Preserving the data integrity is one critical requirement, so LPWAN have to include a method for preventing any unauthorized on stored and transferred data. Data integrity in LPWAN can be realized by the computation message authentication code (MAC) functions. The VR training scheme includes a 3D game for visualizing how the message authentication code is produced using the Network Key, which is confirmed by the Network server. It shows at different scenes of the navigation how an IoT device can be authenticated by using the network key. Finally LPWAN also encrypts the transmitted data file.

4.3 Robustness

An industrial IoT network should be shielded against various attacks and threats caused by human factors or natural disasters. LPWAN uses a frame counter for upstream and downstream messages which will block a transmission from being sent more than once. The VR scenario visualizes how this generated number prevents the replay attack.

5 Implementation Details

Here, we have designed, developed and presented a training scenario by using the Unity 3D environment. The Virtual reality application is built in WebGL Unity Project. The WebGL build option allows Unity to publish content as JavaScript programs that use HTML5 technologies and the WebGL rendering. Just a few web browsers support WebGL, and most of the mobile devices are not supported by Unity WebGL. Actually, Mozilla Firefox browser supports all the utilities of WebGL. We have created the 3D objects for the VR training environment via importing collada files, into the Project's asset. The VR training environment is accessed by iframe and when users navigate on a VR training game through the browser. The developed scripts in VR Training environment are created in Unity Project by writing scripts in C# Language.

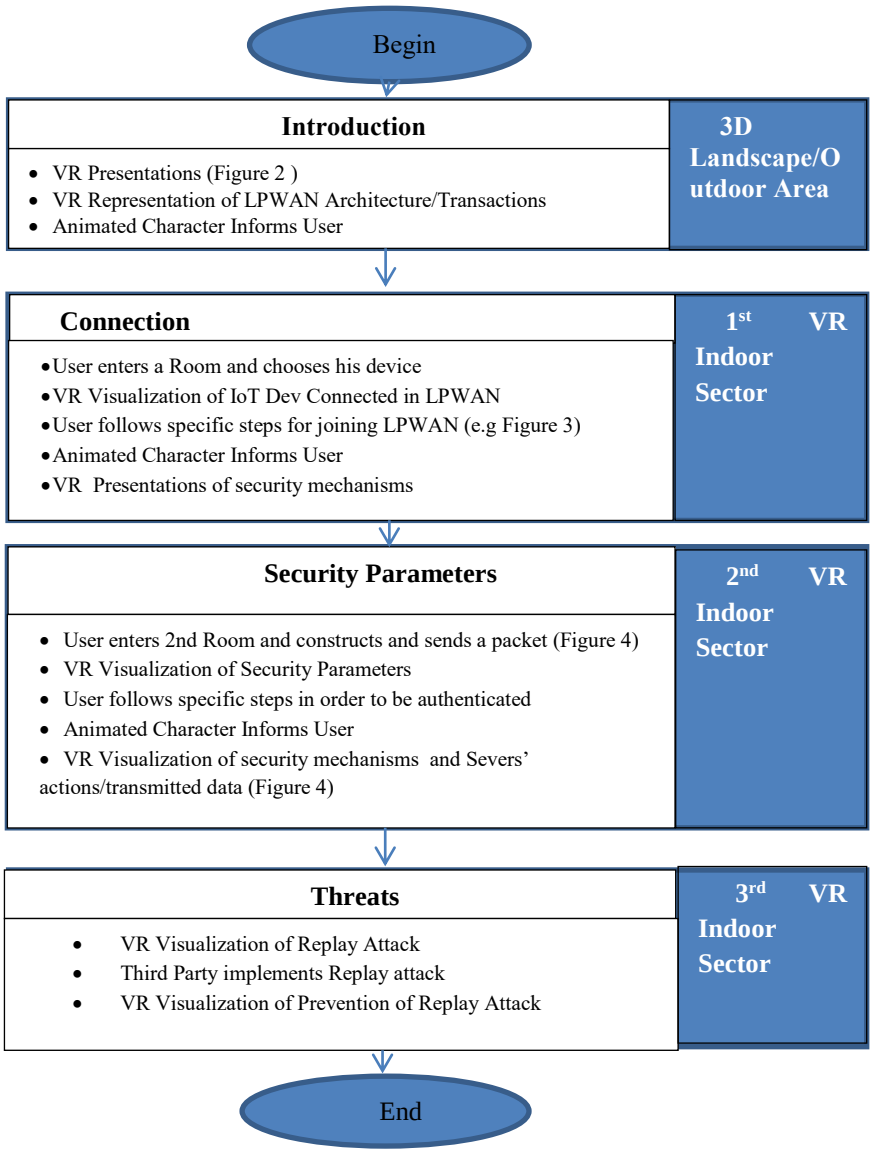

Fig. 1. VR Training Phases.

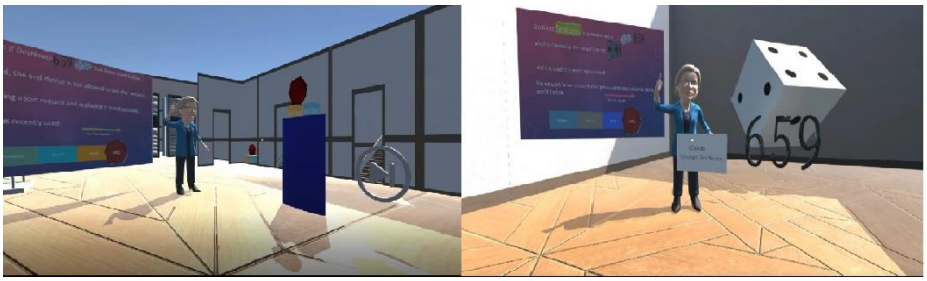

Fig. 2. VR Presenter for informing User.

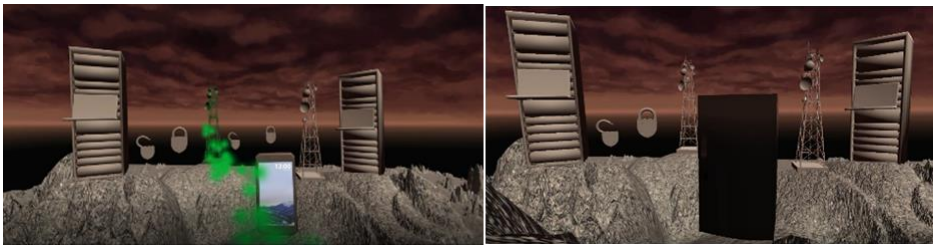

Fig. 3. VR for connecting two different IoT devices.

Fig. 4. Transmitted package from Network server and Packet Construction

6 Conclusion and Discussion

This work presents developing and usage a Virtual Reality (VR) training environment that can help potential users of LPWAN to familiarize with the provided security mechanisms by LPWAN and to increase their security awareness. We used a small group of master students in Computer Security theme for training purposes. Most students found the proposed VR scheme useful for exploiting new technologies. In addition, we explored how useful students found the VR technology as a training tool. Whereas 95% of them believe that VR is the easiest and most convenient way to explore IoT system's functionalities. All students strongly agreed that protecting their data in an IoT environment is important to them. Overall, 85% of the students

declared that they would prefer the utilized VR scheme to include more entertaining and game role characteristics. We are planning to further update VR model and to redesign the VR use case scenarios in order to provide a more entertaining game-role based experience.

Acknowledgements

This work has been partially supported by the "TIPHYS 4.0- Social Network based doctoral Education on Industry 4.0" project No 2017-1-SE01-KA203-03452 funded by ERASMUS+ of the European Commission.

References

[1] S. Büttner et al., "The Design Space of Augmented and Virtual Reality Applications for Assistive Environments in Manufacturing: A Visual Approach.," in *International Conference on PErvasive Technologies Related to Assistive Environments.*, 2017, pp. 433–440.

[2] L Stuchlíková, A Kósa, P. Benko, and P. Juhász, "Virtual reality vs. reality in engineering education.," in *15th International Conference on Emerging eLearning Technologies and Applications*, 2017, pp. 1-6.

[3] DW. Carruth, "Virtual reality for education and workforce training," in *15th International Conference on Emerging eLearning Technologies and Applications.*, 2017, pp. 1-6.

[4] J. Ryoo, A. Techatassanasoontorn, and D. Lee, "Security Education using Second Life," in *IEEE Security and Privacy*, 2009.

[5] j. Ryoo, A. Techatassanasoontorn, D. Lee, and J. Lothian, "Game based InfoSec education using OpenSim," in *15th Colloquium for Information Systems Security Education*, 2011.

[6] L Camarinha-Matos, R Fornasiero, and H. Afsarmanesh, "Collaborative Networks as a Core Enabler of Industry 4.0," in *IFIP Advances in Information and* , vol. 506, 2017, pp. 3-17.

[7] B Ervural and B. Ervural, "Overview of Cyber Security in the Industry 4.0 Era," in *Industry 4.0: Managing The Digital Transformation*.: DOI:0.1007/978-3-319-57870-5_16, 2018, pp. 267-284.

[8] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Communications*, vol. 23, Oct. 2016.

[9] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys Tutorials*, pp. 1-1, 2017.

[10] Alexandros-Apostolos A. Boulogeorgos, Panagiotis D. Diamantoulakis, and George K. Karagiannidis, "Low Power Wide Area Networks (LPWANs) for Internet of Things (IoT) Applications: Research Challenges and Future Trends," *CoRR*, vol. abs/1611.07449, 2016. [Online]. HYPERLINK "http://arxiv.org/abs/1611.07449" http://arxiv.org/abs/1611.07449

[11] M Luvisotto, F Tramarin, L Vangelista, and S Vitturi2, "On the Use of LoRaWAN for Indoor Industrial IoT Applications," *Wireless Communications and Mobile Computing*, p. 11, 2018.

[12] P. Pavlou, "State of the information privacy literature: where are we now and where should we go?," *MIS quarterly* , vol. 35, no. 4, pp. 977–988., 2011.

[13] B.A. Price, K Adam, and B. Nuseibeh, "Keeping ubiquitous computing to yourself:a practical model for user control of privacy.," *International Journal of Human-Computer Studies* , vol. 63, no. 1, pp. 228–253., 2005.

[14] D.E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: a top-down survey," *Computer Networks 2018.*, 2018.

[15] E. Aras, G. S Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of lora," *3rd IEEE International Conference on Cybernetics (CYBCONF 2017)*, pp. 1--6, 2017.

[16] Y. Chatzigiannakis, V. Liagkou, and P Spirakis, "Providing End-to-End Secure Communication in Low-Power Wide Area Networks (LPWANs)," in *2nd International Symposium on Cyber Security Cryptography and Machine Learning (CSCML 2018).*, 2018.

[17] A. Emekcan, R. Gowri, L. Piers, and H Danny, "Exploring the security vulnerabilities of lora," in *3rd IEEE International Conference on Cybernetics (CYBCONF)*, vol. 06, 2017, pp. 1-6.

[18] J. Michorius, "Whats mine is not yours: Lora network and privacy of data on publishing devices.," in *25th Twente Student Conference on IT*, 2016.

[19] S. Naoui, M.E. Elhdhili, and L.A. Saidane, "Enhancing the security of the iot lorawan architecture," in *International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN 2016)*, 2016, pp. 1–7.