DOI: https://doi.org/10.3217/978-3-85125-530-0-28

Proposed Model security best practices using Immersive Virtual Reality in Social Engineering.

Sergio Ordoñez [1], Adolfo Melendez, Leticia Neira

[1]FIME-UANL, San Nicolas de los Garza Nuevo León, México
sergio.ordonezg@uanl.mx
adolfo.melendez@uanl.mx
leticia.neira@gmail.com

Abstract. In this study is presented a virtual environment similar to the Smart cities, with the purpose of allow the user to interact with the different threats that would be exposed by the use of IT in the daily life, looking with this grant to the user a learning method in a real environment of the activities that are confronted with the practices within a smartcity, in order to raise awareness in the user variants of attacks that are submitted, using inmmersive learning as a training method. Cases of threats and vulnerabilities will be recreated with social engineering practices such as phishing, spoofing, wireless attacks and sniffers mainly. This look for to get awareness of best security practices, likewise, raise awareness that we are exposed alarming when it comes to use of technological resources as a means of support for our daily activities.

Keywords: Virtual Reality, Immersive Learning, Social Engineering, Smart Cities, Cybersecurity

1 Introduction

The use of Immersive learning as a learning method [6] will be use in this study to act as a way of training in good safety practices, regarding the use of tools presented by Smart Cities to facilitate the lives of citizens of these. With the improvements brought by these cities and the benefits also presented the risks exposed, since they represent the opportunity for hackers to obtain information due to the bad security practices that users of these services do. The present study presents several scenes that using Immersive Learning and Virtual reality will be present for try to teach users a model of good security practices, to minimize the amount of risks to which they are exposed.

These scenes are performed simulating some situations involving good security practices, such scene were done with 3dmax for the 3d models, Unity3d as game engine, and oculus is used for exposure in virtual reality.

DOI: https://doi.org/10.3217/978-3-85125-530-0-28

2 Background

The term Smart Cities is not new, it is a term that could be related to the intelligent growth used by Bollier in 1998 [1], movement of the end of the 90 that used some terms for the planning of the cities. The term evolved and was adopted by many companies in the technology area from 2005 and today becomes a daily term, using the Internet of things as a means for the development of these cities. This has brought impressive benefits to cities ranging from reduced resource use, reduced CO2 emissions to the environment, such as New York in 2007, to the exploitation of multiple transportation systems and the implementation of these practices in the Healthcare sector.

2.1 Social Engineering

Social engineering causes millions of dollars every year to be lost through this method that cannot be detected or stopped and is based on the ability to exploit a basic human characteristic: the tendency to trust. [2] Using high-quality social engineering, combined with old exploit codes and some malicious PowerShell-based programs, the Dropping Elephant group managed to steal critical data from high-profile diplomatic and economic organizations related to China's foreign relations.

3 Proposed model

The proposed method to train people in the use of the most common stage where they may have a security problem, were made in Unity3d and will be exposed in oculus. The scenes created for these tests will be the following: Preventing Impersonating Attacks, Use of automatic cash dispensers, Unsecured Wireless connections, Forms to provide information on websites, Cellular network in secure networks.

4 Results

The result of this study will be evaluated through a security system using neural networks and evolutionary algorithms, which will allow to verify the number of incidents to which the users were vulnerable in this simulation, and with this will allow us to strengthen said security system. In order to provide users with a framework to obtain useful information on the cases to which more users were vulnerable.

DOI: https://doi.org/10.3217/978-3-85125-530-0-28

References

1. C. Harrison and I.A. Donnelly. A THEORY OF SMART CITIES. 2011.
2. C. Hadnagy. Social engineering the art of human hacking, page 40, 2010.
3. B.D. Medlin, J.A. Cazier and D.P. Foulk. Analyzing the vulnetability of U.S Hospitals to Social Engineering Attacks: How many of your employees would share their password?. 2008.
4. R.S. Patel. Kali Linux Social Engineering, pages 20–24. 2013.
5. L. Torres-T EvoNorm, a new evolutionary algorithm to continuous optimization, 2014.
6. S.W. Greenwald, D. Citron, H. Bedri and P. Maes. Note-Taking in Virtual Reality Using Visual Hyperlinks and Annotations, 2016.
7. G. G-Clavell. (Not so) smart cities?: The drivers, impact and risks of surveillanceenabled smart environments, 2013.