Security Issues in Serious Games Web Environments

Nuno Pontes

Lusofona University of Porto Porto, Portugal
nunopontes04@gmail.com

Abstract. The purpose of this paper is to have an overview about the concept of Serious Games, to try and understand the various types of games that exist in that realm, as the contextualization on where they sit through where "Serious" is concerned. Adding to that an array of examples as well as the contribute to real professional jobs, the importance these games bring to the professional world, the message that Serious Games transmit. The possible solutions to solving security problems, the importance that serious games can bring to cyber security issues and demonstration case study.

Keywords: Security, Educational Games, Digital games, Security Issues, Serious Games, Games, Game Web Environments

1 Introduction

When we reference games, we often associate the term with leisure and entertaining, however, serious games have another objective other than pure entertainment. The games which it refers to are more focused on to educational areas, publicity, military training, and medicine. Their objective is mostly to train professionals, workers, students and in some cases, via simulation when it comes to practical fields corresponding to the military. Similarly, to simulating military games, there's also Advert games, which pertains to publicity games, where the focus promotes a brand, a product or a service. Ultimately, whenever serious games are brought up, their objective will pertain to educational and learning purposes, either to help new businesses arise assist diversified professionals getting prepared to start their new work. Additionally, backtracking into the origin of the term, Serious Games, the idea of using games aimed at dealing with serious matters is an old concept. According to [1] "Americas Army game was the first successful and well-executed serious game that gained total public awareness." Even though a flush of Serious Games appears to begin in 2002, quite a few were simply designed for serious purposes before this date. By current day definitions, any digital game that was designed for a purpose going beyond entertainment can be considered a Serious Game. The very first game to ever be created, regarding popular culture, was Pong, for Atari console in 1972. Was effectively the first video game to embrace commercial success. Among the video games created before Pong, some titles were not designed for pure entertainment, but rather for serious purposes, to illustrate a scientific research study, to train professionals and to broadcast a message according to [1]. According to [1] "We are concerned with Serious Games in the sense that these games have an explicit and carefully thought out process and are not intended to be played primarily for amusement." The definition stated on [1] in the 1970s paper entitled "Serious Games", conveys to us, that it is a rule nowadays whenever the word game in brought up in a sentence it is strictly regarding the entertainment and leisure, which is far from the truth.

2 Serious Games about Web Environments

During the cold war, the army invested a sum of money into the research field, as well as some investments to fuel a few projects from this particular time-frame, which led to technology that is now prevalent in our daily lives, such as computers and the internet. Despite that fact, many of the first computers were initially conceived to operate under military purposes, ranging from ballistics, computations, resource management, to simulations. Officers around the globe used war games in place of training in addition to educational assistance, and such thing had been the spark to fuel the idea to create computer-influenced war games in research departments [2]. According to [2] "Hutspiel" was a strategy game created in 1955 and worked on this fashion by allowing two human players to experiment with the impact of nuclear weapons on a global battlefield. The game was highly detailed, as it simulated ammunition and fuel supply for each unit controlled by two players.

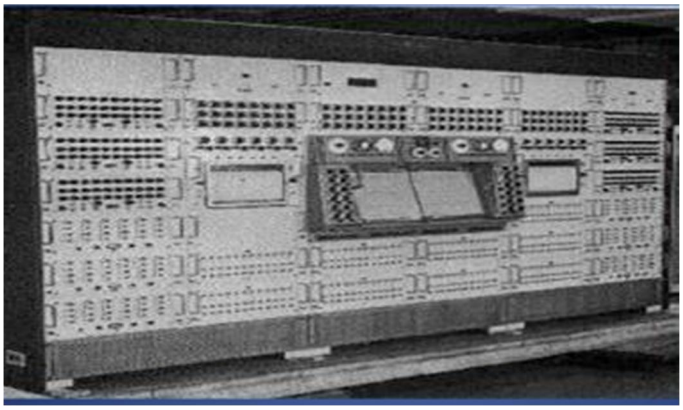

Fig.1. Hutspiel

Several other games were given the birth "post-Hutspiel" project, namely “T.E.M.P.E.R”, a cold war simulation game created in 1961, and “ARPA-AGILE COIN GAME”, another game which simulates an internal revolutionary conflict in a country. These strategical military games represent a step too much more complex simulation games [2]. Most of these games were not available for public use, and the little information found nowadays about them is mainly treated as unclassified military documents. None of these games were available for general public, the little information we could find about them comes from unclassified military documents. Which makes the tracking down for reference images rather complicated, most of them do not exist online for the public to see. However, we can classify the games mentioned previously on this paper as being the ancestors, so to speak, pf the simulation video games that appeared on personal computers in the 80s, when it comes to military topics games such as “Dunningan, 1992. The old projects were created to help to boost this field and served as good source for the current serious games available nowadays. Additionally, next will be approached their importance and impact to professional and educational fields.

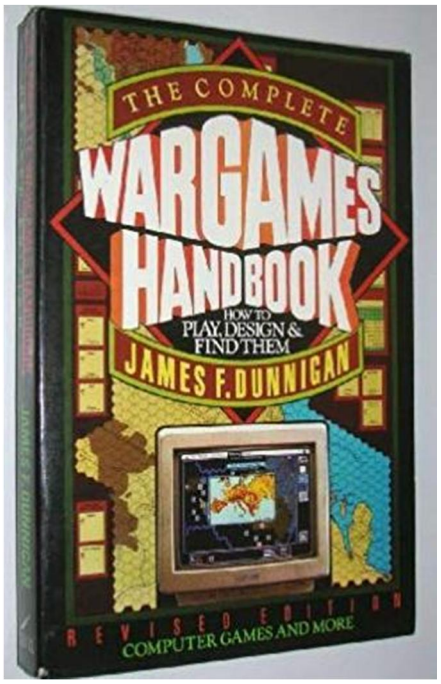

Fig.2. Dunningan

3 Importance of Serious Games

Serious Games carry the weight and responsibility to transmit messages in a more meaningful, interactive and interesting way. It is certainly a viable addition to aid professional work, in order to educate interns/workers on their fields of work, by making the learning process into an appealing experience.

There have been given a few different purposes for Serious Games over the course of years, such as personal development, medical health, publicity, product promoting, military, social science and corporate purposes. A clear sign of the importance over the last decade, the UK and the US carried out a cyber war game to test the resilience of the financial sector in the City of London and on Wall Street. The attack orchestrated in London banks was designed to test out the City's defenses against online saboteurs. The exercise was useful but the real challenge lays in co-coordinating across the industry to make sure a crisis scenario is never reached [3].

Serious Games work because they appeal to nearly all ages, certainly to adults, making teaching bearable and transferring knowledge, a much more enjoyable and intuitive experience. The feeling of being connected to Serious Games is often due the social aspect of our human nature, allowing ourselves to be connected to others like us, like a ranking system commonly seen in many kinds of games, rather scoring high on the ranking charts allowing individual games to reference other players and create a feeling of kinship.

According to a study [4] carried out by the Pew Research Center, proving that 97% of teenagers play some sort of digitalized game, which comes to enable Serious Games to be highly relatable to a huge portion of the population, as players tend to feel in control, or rather autonomy. Having met that feeling of autonomy, they learn and manipulate outcomes within the game

itself, while learning and educating themselves as they play. Efficiency talks volumes, because if we make a mistake in a game we do not die, for example when it concerns piloting training. Much the same is relatable with other professional roles in society, we will not lose a real case if we are lawyer roleplaying. And that is the beauty of games, they are in a different reality as the one we live in. They guide us, providing enough ammo and fuel, to transfer enough confidence to make mistakes, while actively learning, and not being afraid of the consequences. The more a game is played the less frequently the mistakes are made, growing out our efficiency [4].

Serious Games are useful in that regard because they have this gist in turning what could be taxing and boring, into potentially transfiguring a subject into a more entertaining, powerful way of introducing new concepts. However, even if things seem quite promising and revolutionary when it comes to new learning processes, the threats to that web environment are not free of problems, which is something that will be addressed next, the issues concerning web environment.

4 Cyber Security Problems

In the midst of education process from online services, which provide coverage for professional games, there might be certain complications, adapting the form of viruses, trojan, hacking, amidst others. Most of us enjoy playing, either casually, socially or professionally, however, online threats exist and more often than not they are issues to pay attention to. For instance, there are few specific and well-known threats usually can cause complications. Teslacrypt was designed to encrypt game-play data for dozens of video games, prompting the user to pay a ramson to decrypt those files. Targeting some well-known games including Call of Duty and Minecraft, it basically blocks the access to saved game files, configuration files or game files [5]. There are other problems which are alarming when it comes to security issues. Password stealing is known practice among cyber-gaming, either professionally or casual play. In this case, there are various types of spyware called keyloggers, which capture keyboard events and try to steal access credentials, there are also pieces of malicious code that attempt to steal access credentials for online games or platforms [5]. One of the most popular scam plots is when a player receives a chat message from another player offering to join his team, then the unknow player is usually super friendly and praises the victim for his skills, telling him that he should join this team of great players. The deceit resides when the victim is encouraged to download and install an application, it can adopt the form of a voice communication program. The attacker will be insisting on the fact that the victim cannot be part of the group, if the software is not installed on his system. Least as we expect the executable is definitely not something to help the victim joining the group, but rather a malicious software that is capable of stealing account credentials [5]. One of the most problematic cases are those of an android trojan which hides himself among the games in google play, which allows the attacker to control devices remotely, thanks to its backdoor capabilities. By imitating games and e-learning apps [5]. Another case remotes to a fake Minecraft app that installs scareware, which was downloaded by more than 600,000 android users. Which consists on the following, after showing the victims sign of fake viruses or threats on their device, it then tried to convince the users to subscribe to a premium SMS service in order to remove the fake threats [5].

Usually the TeslaCrypt attacks as follow: infects a machine, scans all drivers for files, encrypts the files with an algorithm, and replaces the desktop with some sort of ransom message [6]. There might be much more ways to disrupt the peaceful web gaming or just web browsing, but there are very common and effective in way, because they can be easily used all that's needed is for the victim to be unaware of what their circumstances currently are and they will fall for the deceit. One particularly dangerous threat to computer users is phishing. This is a type of attack, in which victims get invited by scam emails to visit fraudulent websites. The attacker creates a fraudulent website which has the look and feel of the legitimate website. The users are invited by sending scam emails to access the fraudulent website and steal their money. [7]

Another thing to note are fake apps. Nowadays apps are our day-to-day download or rather we use them quite often if we compare it to a few years ago, such is the evolution of technology [8] Apps tend to be very efficient in many of our daily tasks, school, cooking, car service, grocery shopping and of course gaming. And the apps can also be used in many electronic devices, such as laptops, tablets, and smartphones. Therefore, being careful is an overstatement, because the bottom line is that there are fake apps masquerading as official games, and even updates. In the theme which I am writing this article for it is important to note that there are many apps for professional learning, being games or simply any kind of apps to serve as support to digital learning.

Showcasing solutions to the main issue on the next chapter, when it comes to fight off all the threats referred. Usually when we mention Cyber Security it is often concerned to applying measures to ensure confidentiality, integrity and availability of digital data that is either stored, sent or received. The security defenses can range from protection software to risk, to training about awareness, all of them do prevent security breaches, such as loss of data, theft or damage to our computing system.

According to a recent report released by [9] on the threat overview during the period from October'1st to December 31st, 2017 "fourth quarter," most of the threats are targeting government entities (48%), energy and telecommunication sectors (15% and 11%), which reflects the threat actors' intent in impacting the national economy, while the number of the Threat Alerts was slightly higher (7%) as compared to the third quarter of 2017. As explained on the graphic bellow:

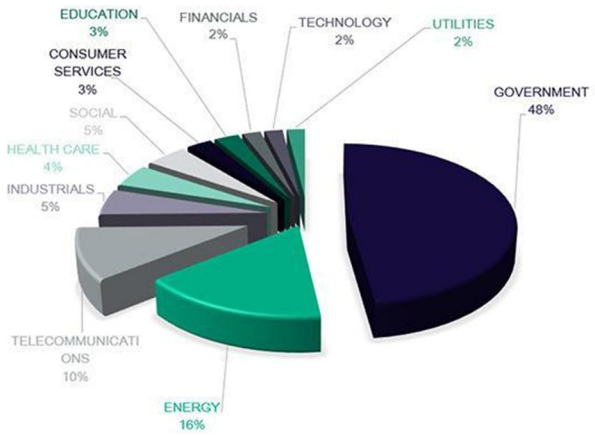

Fig.3. Graphic for the amount of security violations

There are currently some practical curses that help enhancing cybersecurity skills two practical, project-oriented, courses on cyber-attacks and defense. They focus specially on adversary thinking, a crucial skill for cybersecurity experts who must be able to think like an attacker in order to set up effective countermeasures. While this skill can be exercised in Capture the Flag games, challenges, and competitions, their courses introduce an innovative approach. The learners are guided to create a serious security game deployed at the KYPO cyber range, which allows emulating real threats and attacks in a controlled environment [10].

In order to boost the cybersecurity knowledge amongst ourselves the Dutch government issued a serious game, naming it ThreatBattle. A game that basically helps boosting the cybersecurity awareness to avoid eventual collateral damage done by security threats.

In this game a concept called "transreality" is used, on which its meant that the game takes security elements from the players real-life situations and incorporates them into the game [11]. Another serious game exists named Qbit in which the participants are challenged to show their true colors in a game situation on the prison island of Alcatraz. Basically, the game helps identifying the success factors and points to the attention regarding security awareness, management or project group, providing an insight into behavioral and practical working methods [12]. Although the game doesn't focus mainly on computing aspect, in other words, the technological part of it, it does, however still boost up and improves the sense of responsibility and risk awareness, and a better understanding and commitment regarding cyber security.

According to [13] which launched its first training product in December after over 20 years in the online gaming industry, named Ares. The benefit of cyber ranges [13] says, is that "in a virtual environment, if we break the network, we just respawn it." They approximate a real-life scenario without the real-life risk. The project was useful on the way that it does not rely on instructors and is intuitive enough. Their new product Ares introduced game theory and artificial intelligence to cyber security training [13].

It is important to note that serious games nowadays play such an important role when it comes to give pointers to educational fields, professional fields as well, serious Games, can be a great asset to society, research, and business, because lately society focuses much more in digital world, and with the upcoming of internet, the smartphone, and bitcoin [14]. In general, adults and even children, live inside a system that already required them to adapt with modern technology and be ready to move rapidly to more advanced technologies. It is quite logical that people grown to adapt to this situation and learn how to make use of it. In other words, modern media will become their learning objective [14].

The positive aspect of this is that the cybersecurity professionals behind the project itself are also gamers, and thus it makes this simulation-based gaming platform the potential solution for cybersecurity training.

Another study that was issued in 2016 namely '2016 Data Security Incident Response Report' by [15], the top reason that caused 37% of all data security incidents last year was Phishing/hacking/malware. The second largest number of incidents, 24%, can be tracked back to employee actions or mistakes. External theft of devices (17%), vendors (14%), internal theft (8%), and lost or improper disposal (6%) complete the figure bellow.

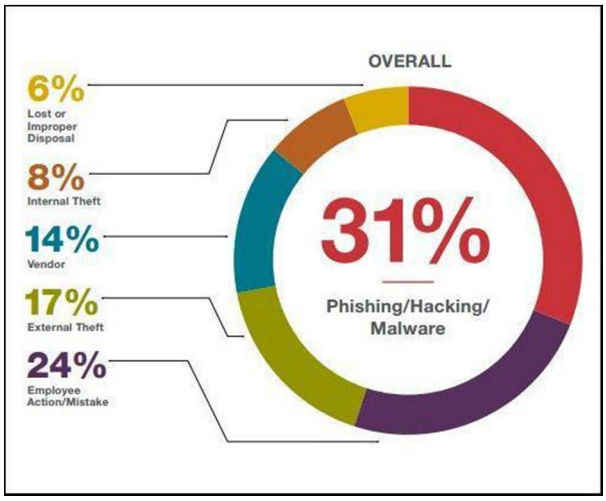

Fig.4. Study about the data security incident

Furthermore, on the table below there was a study done by [15] where it displays a few games that concern to cyber security, while also having details that describe the type of game, topics and target audience. Most are free to play, and their main focus is online security. The study is as follows according to [15] where they say that the number of studies into cyber security is rising exponentially, and nearly all studies focus on efforts to train and raise awareness within the general public.

Game Name	***Game Type***	***Methodology***	***Results***
TiER	Interactive role-play	EEG and Eye tracking	Unclear
Anti-Phishing Phil	Mobile application training safety of link URLs	Think aloud, pre-test & post-test experimental vs. control, SUS usability questionnaire	Positive impact on learning, awareness and phishing susceptibility
Security games by Next Generation Security (NGSEC)	Web-based	Comparing on-task performance	Significant improvement in game
CyberCIEGE	3D virtual world (sims style)	Unclear Experiment & self-assessment Theoretical review of cognitive principles	Sufficiently flexible to illustrate a wide range of topics and positive early indication Positive Unlcear, but there is a need to create a science of games
PicoCTF	Web-based	Survey	Positive educational experience according to students & instructors

Table 1. CyberSecurity Games

5 Solution for Security Problems

All these security exploits can be daunting to deal with if all we want is merely to make use of technology to learn our job craft, or simply to indulge ourselves in casual web browsing or playing games. There are, however, various ways to also defend ourselves against these security breaches to our web environment.

The principles for our daily technologic devices, such as computers, smartphones and tablets, is much the same. We have to be cautious about opening unknow files attached to email messages or instant messages, as well as checking the authenticity and security of downloaded files and new software.

The use of an antivirus, malware software and antispyware software is a must, as well as using a firewall if the case is to use a computer device. Identity and also a backup to our personal data and creating and using testing passwords do play an important role when it comes to security. The protective software cannot do all the work, this must come from each of us, the sensitivity to avoid certain things that might slip through our protective systems. [16]

There are also when it comes to professional gaming environments, security practices, that can help boost our experience risk-free of rather problematic events. The Administrator Mode risk, which consists in some games requiring the use of administrator mode. It's important to make sure the game vendor is reputable and download the game from a site we believe we can trust. Usually free download of games sometimes conceals malicious software. Including "plug-ins" sometimes required to run games. Bottom line is by operating on administrator mode, we open ourselves to the risk that an attacker could gain complete access to our personal computer. [16]

Playing the game at the game site can often make the experience risk-free. Because when we play an online game usually on a web browsing, we can use the administrator mode, and when we are done playing the game, we can just switch back to a user account and simple browse the web. This will reduce the risk of ending up on a malicious web site as well [16].

6 Conclusion

In this paper about security on web game environments, the theme was approached with special emphasis to security, in order to have it safe it's important to know the risks. First of all, as I talked about in this paper, a Serious Games, is a game which is more than just entertainment, it is often aimed to education, or helping people, supporting them to change their behavior or simply a cause in the world. In media we have educational films, documentaries, and the rise of serious games comes from the acknowledgement, the interactivity. The interactive games are known a powerful media, in order to make a message stick deeper and also being more convincing.

From a learning point of view this method of teaching is more effective, its more about active learning because there is no choice in order than participate to progress on a video game, thinking about what we are doing as opposed to be sitting on a living room watching the documentaries or simply watching videos to learn, this would be under a very passive experience. The great benefit from using serious games is to change specific patterns in our

behavior, changing them for the best, to stray away from regular mistakes and being aware of certain details we would do normally. For instance, on the medical field, serious games, can potentially save a few lives, in terms of the results, it is aiming to get the great thing about games, since they are digital we can measure everything as they are really analytical.

When it comes to cyber defense, cyber security, I've noticed the absence of these types of games in the casual entertainment of game market, and in my opinion, this is relevant because if we've got serious games in the casual game market we can reach a larger audience and that is relevant special in education if we want to reach a larger audience and fight more efficiently against cybercrime. The ideal scenario is to reach a broader number of people not just a specific group of people of X company or school, the idea should be to reach everyone or as much as possible.

This paper served to educate me in this field further, as well as helping me understand how important the serious games are in this current century, even more so since we live in a digital era. This way of learning is perfect to boost our confidence, to help us know what is dangerous, and to cyber security specially, it's a way for experts and non-experts raise awareness for what can be dangerous when dealing with digital threats, whether they reside on a serious game web environment or simply when browsing the web.

References

1. Samari N.; "Brain Feasts, Longer Reads", (2015).
2. Minhua M.; Andreas O.; Lakhmi C. J.; "Serious Games and Edutainment Applications", (2011).
3. Scuffham M., Franklin J.: "Cyber-attack 'War Game Tests", (2013).
4. Lenhart A.; Kahne J.; Middaugh E.; Rankin M. A.; Evans C.; Vitak J.; "Teens, Video Games, and Civics", (2008).
5. Porolli M.; "Online Threats and How to Avoid Them", (2016).
6. Wang S.; "Analysis of the TeslaCrypt Family", (2017).
7. Vayansky I.; Kumar S. A.; "Phishing - Challenges and Solutions", (2018).
8. Yan L. and P.; "Fake Apps: Feigning Legitimancy".
9. NCSC; "2017-Q4 Threats and Rist Report", (2017).
10. Svabensky V.; Vykopal J.; Lastovicka M.; "Enhancing Cybersecurity Skills by creating Serious Games", (2018).
11. Grevelink J.; "Serious Games for Cybersecurity", (2015).
12. QBIT; "A Serious Game", <https://www.qbit.nl/awareness-training/serious-games/>.
13. Oesch T; "Serious Games for Serious Topics: Training Cybersecurity Professionals Us-ing AI-Powered Games", (2017).
14. Mans B.; "Serious Games", (2017).
15. Bartl P.; "Enterprise Gamification & Serious Games for Cybersecurity – The Human Factor", (2016).
16. Hayes J. E.; "Playing it Safe: Avoiding Online Gaming Risks", (2008).