Realizing User Privacy and Security Issues in Edutainment e-Solutions

Osama A. Alsaadoun(✉) and Badar Al Lawati(✉)

DePaul University, Chicago, IL 60604, USA
oalsaado@depaul.edu, badar.allawati@gmail.com

Abstract. Edutainment set a unique approach for incorporating learning enriched with dynamic platforms of multimedia end enjoyment. Computerized systems built with edutainment philosophy represent an extended mechanism for wider user space and educational functionalities. Similar to other computer applications and systems, cybersecurity remains an obvious challenge for system users operators. In this paper, we review general categories of cybersecurity challenges that can affect edutainment systems. We also suggest practical recommendations that should be considered by designers and operators to improve cybersecurity resilience of edutainment systems.

Keywords: Edutainment · Cybersecurity · Identity and access management

1 Introduction

1.1 Edutainment

In the last 10 years, there has been an increase of Internet social network applications, an increase in the number of users of the internet, and an increased number of connected merchants, products, and services. More connectivity means changing environments that would lead to different user experience in different fields in the real world: education institutions, healthcare providers, financial companies, marketing agencies, etc. All of this had led to the convergence of different areas of technology that eventually created new hybrid technologies. Terms like gamification and edutainment are becoming commonly used by major software vendors and application providers with considerations in their next upgrade, or maybe already offering an add-on bundle on their existing platforms to add a "fun-flavor".

The term "Edutainment" was first introduced by [1] were defined it as: "is a hybrid genre that relies heavily on visual material, on narrative or game-like formats, and on more informal, less didactic styles of address". However [2] had a different definition: "Technology heavily laced with entertainment but essentially lacking in rigor or value".

1.2 Applied Edutainment

Edutainment is simply merging technology, entertainment, and education. Technology is more than just machines that stores data, execute commands, and display results. In their report [3] explained how they look at technology as: "The new technology is not

X. Fang (Ed.): HCII 2019, LNCS 11595, pp. 278–287, 2019.
https://doi.org/10.1007/978-3-030-22602-2_21

just an assemblage of machines and their accompanying software. It embodies a form of thinking that orients a person to approach the world in a particular way. Computers involve ways of thinking that under current educational conditions are primarily technical. The more the new technology transforms the classroom into its own image, the more a technical logic replaces critical, political and ethical understanding. The discourse of the classroom will center on technique, and less on substance. Once again 'how to' will replace 'why'."

So, implementing technology in the classroom is part of the journey into making learning more fun and interactive. However, there is always the fear of associating education with fun and entertainment. As [4] argue that if the technology is implemented in education without cautiously examining the environment then learning becomes an obstacle that needs to be overcome. "such an approach doesn't promote learning; it trivializes the learning process." [4].

1.3 Common Edutainment Models

There have been many attempts to evaluate technology's role in education, more specifically game-based learning. In his model Ehrmann [5] introduces the Flashlight framework, where he attempts to assess the relationship between 3 main constructs: The technology, the activity that uses the technology, and the education outcome. Another attempt was the CIAO! framework introduced by Jones et al. [6] where the researchers examined the context, the interaction between the learners and technology, and the attitudes and outcomes. However, what all of these attempts had in common is the intention to consider technology in general.

On the other hand, one of the major comprehensive models in edutainment is the game-based learning framework introduced by De Freitas, Oliver, and education: "The model requires the practitioner to consider four main dimensions in advance of using games and simulations in their practice" [7]. The 4 main dimensions of the framework should be considered when evaluating the environment that the tutor will undertake before implementing and game/technology into space.

- 1st dimension is: **Context,** where factors like historical, political and economic contextual factors as well as the availability of specific resources and tools are considered.
- 2nd dimension is: **Learner,** where attributes like age, how individuals learn in their learning backgrounds, styles, & preferences are considered.
- 3rd dimension is: **Internal Representational World,** which is simply the mode of presentation, the interactivity, the levels of immersion, and the fidelity used in the game or simulation [7]
- 4th dimension: **Process of Learning,** and this includes both during the course of formal circular-based learning and during the informal learning. This dimension focuses on the practitioners' reflection on methods, theories, models, and framework used to support learning practice.

"The four dimensions together provide a framework for a consideration of both existing and future educational games & simulations, and may also be applied to other

forms of e-content where immersive spaces are used" [7]. What makes this model unique compared to other models is:

- Its' flexibility and ease of use
- Ability to help practitioners to reflect upon their own learning process
- Support for tutors aiming to develop practices and tools into the classroom
- Identify how software tools can support curriculum content most effectively

Learner Specifics Challenge Conflict Progress	**Pedagogy** Adaptation Assessment/Feedback Debriefing/Evaluation Instructions/Help/Hints Safety
Representation Action-Domain Link Control Interaction (Equipment) Interaction (Interpersonal) Interaction (Social) Location Problem-Learner Link Representation Sensory Stimuli	**Context** Fantasy Goals/Objectives Language/Communication Mystery Pieces or Players Player Composition Rules Theme

Fig. 1. Game-based learning framework [7]

2 Cybersecurity Prospective

In this paper, we limit our research to studying cybersecurity challenges and mitigations to computerized forms of edutainment systems, including web apps and handheld or wearable consumer devices. In a simplistic form, cybersecurity is defined as processes, practices, and technologies designed to safeguard computing systems and infrastructure from malicious and destructive activities from – typically unauthorized – users [8]. Cybersecurity generally extends to cover all modern computing domains, such as communication networks, backend database and storage systems, and frontend application interfaces [8, 9].

We believe studying cybersecurity factors in the context of edutainment systems not only helps elimination of possible disruptive impacts to educational experiences, but also provisions prospects for founding effective and scalable educational solutions with farther outreach and deeper user penetration. Such a study becomes further critical when realizing - through prior research – that significant number of online social networks and e-learning platforms' users are categorized as youth and adolescence

[10], a fact that practicality may subject edutainment systems to adhere legal, industrial, or environmental compliance mandates [10–12].

In subsequent sections, we continue this study by examining common categories of cybersecurity risks that can have a direct impact on edutainment systems. We then survey research work in human-computer interface (HCI) domain aimed to identifying cybersecurity elements that can help improving user experience without jeopardizing system usability aspects. Afterward, we propose an architectural framework that aligns typical edutainment systems' functional requirements as well as corresponding cybersecurity controls (Fig. 1).

2.1 Common Forms Cybersecurity Challenges

This section summarizes common forms of cybersecurity challenges that potentially can have a direct impact on edutainment systems. The analysis considers the forms of challenges mainly based on the source of threat, nature of the potential impact.

In general, prior research works [13, 14] classify cybersecurity into four categories:

- Disclosure: unauthorized access and release of proprietary and private information
- Deception: contaminating information to have incorrect representation or meaning
- Disruption: affecting the availability or quality of information and services
- Usurpation: malicious control of system components.

However, we restrict analysis in the following sections to potential cybersecurity challenges having direct and relevant impacts on edutainment system including cyberbullying, privacy invasion, network intrusion, and malware.

Cyberbullying
Prior research shows that very common forms of cybersecurity risks directly related to edutainment systems while used by relatively young users occur in the form of bullying. Similar to the physical form of bullying, cyberbullies basically aim at disrupting youth while interacting with e-learning applications, through means of peer-to-peer or group chat tools, eventually deterring the users away from their rightful learning platforms [10, 15].

Invasion of Privacy
In the context of information security, invasion of privacy is typically characterized as malicious and unauthorized practices leading to access or disclosure of personal or proprietary information. [12, 16–19]. In the context of edutainment, privacy issues can directly relate to a wide variety of user experience issues, such as disclosure of system users private information, performance records, or financial data. [12, 20]. It's also common that sectors of enterprises seek to access other forms of private user information – like user geolocation, types of software and hardware systems they own, and other contextual data – in targeted marketing campaigns, practices often deemed privacy-invasive. [12, 17, 21, 22].

Network Intrusion
A common risk to all computer systems – including edutainment ones – is malicious network activities conducted by unauthorized attackers [13]. Cybercrimes conducted

through network intrusion generally aim at unauthorized access and disclosure of private or confidential data, or to sabotage and affect the availability of offered services, a category of attacks normally referred to as denial of service (DoS) attacks [13, 23]. Providers of edutainment systems clearly need to factor in suitable network security controls [24, 25] to overcome such types of cybersecurity challenges when implementing networked systems.

Malware

Computer viruses and trojan horses have traditionally been regarded as a major method of committing cybercrimes for malicious purposes of destruction of computing resources, identity theft, or disclosure of private or proprietary information [13]. Clearly, risks of malware can have a direct impact on edutainment systems and its users by affecting their availability or quality of service.

Ransomware is a modern variance of malware, where attackers victimize users by obtaining unauthorized access to their computer systems and then rendering critical data files inaccessible, normally by transforming them into formats that the users can no longer read. In order to have the files restored to their original formats, attackers extort the victims to pay monetary ransoms, under the promise attackers will restore the data to its original quality [26–28]. Like other forms of malware, ransomware's possible impact on edutainment systems is likely to be destructive and impairing.

2.2 Cybersecurity Requirements for Edutainment e-Solutions

In this paper, we limit the scope of research interest in Edutainment domain to the specific frameworks that can be modeled into computer-based applications, including online web, mobile, or similar forms of apps. This specification allows adapting existing research work to facilitate analysis and further enhancement of Edutainment applicability and solution offering.

To establish relevance to the Edutainment prospective, we first explain computer security basic requirements expected to improve security for e-solutions. Prior research [13, 14, 23, 29–32] recommends the following parameters:

- Confidentiality: secrecy of information as intended to the authorized user
- Integrity: information remains intact of unauthorized alteration while in transit or storage
- Availability: the state at which systems are expected to be available for user consumption
- Non-repudiation: parties in an information exchange cannot deny actions they commit
- Privacy: personal information is not revealed to others without their permission
- Authentication: parties in an information exchange are uniquely identifiable
- Authorization: access to system interfaces or system data is exclusively granted to the intended user(s)
- Auditing: the capability to determine system transactions, users or processes committed the actions, date, and other confirmation data
- Intrusion detection: the capability to detect attempts to obtain unauthorized access by rogue users or processes.

In addition to the outlined security requirements, researchers [30] highlight that "trust" is a critical cybersecurity quality that users expect to experience in computer applications. When this is mapped to the case of system, users develop the sense of security and confidence that such applications are designed to meet the following criteria:

- Convey features: systems should be designed to inform the users on their security features and capabilities.
- Visibility of system status: systems should make their security status observable to their users.
- Learnability: system interfaces should be intuitively designed to enable users to learn how to use them.
- Aesthetic design: that displays relevant security information to users
- Errors: error message should be relevant and provide support to the users to resolve system issues.
- Satisfaction: enable the users to have a satisfactory experience

3 Addressing Cybersecurity Challenges

This section discusses recommendations on approaching the analyzed cybersecurity challenges to facilitate provisioning edutainment services inline with the defined cybersecurity technical and functional requirements.

4 Enforcement of Identity and Access Management

Identity and access management (IAM) is a suite of processes and all underlying technologies for the creation, management, and usage of digital identities in a computing landscape. In practice, it covers the process of establishing the identity of users and govern the activities or services that users can perform or consume. [17, 33, 34]. IAM supports a range of security services including authentication, authorization, and activity auditing.

Incorporating IAM controls into edutainment systems is expected to considerably address its cybersecurity challenges. For instance, implementing strong authentication modules into application interfaces will enable users to be granted secure access preserving experience and confidence in the system. Enforcing granular authorization rules for different categories of system users is critical to reduce or eliminate unauthorized access and disclosure of confidential information. Moreover, IAM can provide the processes and tools to achieve advantages to edutainment systems including:

- System assurance and user trust, as the IAM inherently ensures such qualities are maintained through the authenticity of users and systems.
- Preservation of confidentiality and privacy to system data and user information.
- Ensure data integrity by restricting access to users only if their identities are verified and according to authorization their functional roles.

- Misusers of system resources cannot repudiate their actions as IAM ensures accountability.

In the context of edutainment systems, we suggest a simplified IAM framework typically capable of accommodating relevant cybersecurity requirements:

4.1 Adopting a Secure Computing Model

A major milestone for edutainment system owners to consider is the development and maintenance of a rigid, resilient, and effective security computing model. Centered around a thorough IAM program, such a model should be adopted to address additional security requirements, especially the high availability of system resources to combat the effects of network threats including DoS and malware attacks (Fig. 2).

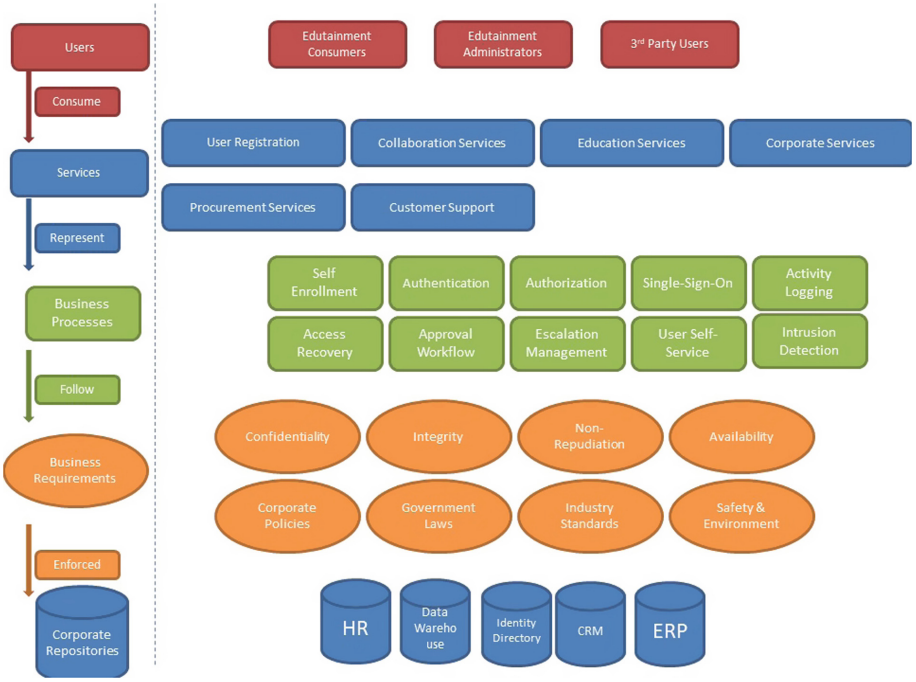

Fig. 2. IAM framework for edutainment systems

An interesting applicable model is the one by Romansky and Noninska [12] who suggest a secure computing model for e-learning applications that follow the National Institute of Standards and Technology's (NIST) visual model for cloud computing. This model features a layered architecture of system backends and application interfaces and draws functional boundaries that address the cybersecurity requirements suggested for edutainment systems. Clearly, this model, shown in flowing figures can be adapted to meet similar functional designs for edutainment systems:

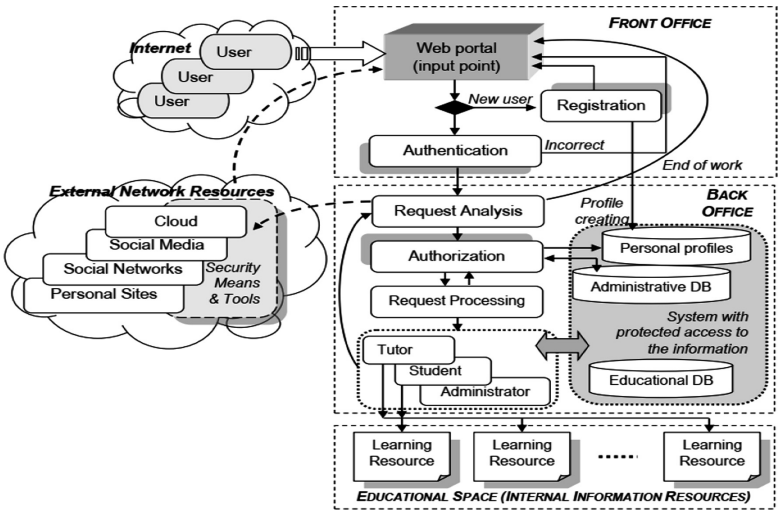

Fig. 3. Architecture of Combined e-learning environment [12]

5 Conclusion

In this paper, we briefly identified edutainment systems and conducted a brief analysis of potential categories of cybersecurity challenges that can impair its values to users. While Edutainment systems can take a variety of forms to deliver its services, online-based solutions follow other computing service models when considering cyber risks (Fig. 3).

Edutainment systems need to incorporate cybersecurity measures in its core designs. Our research presented absolute cybersecurity requirements that developers should embed in edutainment systems to ensure users' sense of trust.

References

1. Buckingham, D., Scanlon, M.: That is edutainment: media, pedagogy and the market place. In: International Forum of Researchers on Young People and the Media, Sydney 2000
2. Mckenzie, J.: Beyond Edutainment and Technotainment, Fron Now On, 10 (1)[Online] 11 de septiembre de 2003 (2000)
3. Apple, M.W.: The new technology. Comput. Sch. **8**(1–3), 59–82 (1991)
4. Bloom, M.V., Hanych, D.A.: Skeptics and true believers hash it out. Community College Week **14**(15), 17 (2002)
5. Ehrmann, S.C.: Studying teaching, learning and technology: a tool kit from the flashlight program. Active Learn. 36–39 (1998)
6. Jones, A., et al.: Evaluating CAL at the open university: 15 years on. Comput. Educ. **26**(1), 5–15 (1996)
7. De Freitas, S., Oliver, M.: How can exploratory learning with games and simulations within the curriculum be most effectively evaluated? Comput. Educ. **46**(3), 249–264 (2006)

8. Systems, C.: What Is Cybersecurity? (2019)
9. Labs, K.: What is Cyber-Security? 2019 03/17/ 2019]; Available from. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
10. Mishna, F., et al.: Risk factors for involvement in cyber bullying: victims, bullies and bully–victims. Child Youth Serv. Rev. **34**(1), 63–70 (2012)
11. Regulation, P.: General data protection regulation. INTOUCH 2018
12. Romansky, R., Noninska, I.: Implementation of security and privacy principles in e-learning architecture. In: Proceedings of the 29th International Conference on Information Technologies (InfoTech-2015), St. Constantine and Elena, Bulgaria (2015)
13. Bishop, M.: Introduction to Computer Security (2004)
14. Badr, S.: Security Architecture for Internet Protocols, Ph.D. Thesis, Military Technical College, Cairo (2001)
15. Berson, I.R., Berson, M.J., Ferron, J.M.: Emerging risks of violence in the digital age: lessons for educators from an online study of adolescent girls in the United States. J. Sch. Violence **1**(2), 51–71 (2002)
16. Maher, A., Najwa, H., Roesnita, I.: Towards an efficient privacy in cloud based e-learning. In: Proceedings of the International Conference on Intelligent Systems, Data Mining and Information Technology (ICIDIT 2014), Bangkok (2014)
17. Alpár, G., Hoepman, J.-H., Siljee, J.: The identity crisis. security, privacy and usability issues in identity management. arXiv preprint arXiv:1101.0427 (2011)
18. Grant, J.A.: The national strategy for trusted identities in cyberspace: enhancing online choice, efficiency, security, and privacy through standards. IEEE Internet Comput. **15**(6), 80–84 (2011)
19. Choudhary, A.R.: Compound identity measure: a new concept for information assurance. In: IEEE Information Assurance Workshop (2006)
20. Bandara, I., Ioras, F., Maher, K.: Cyber security concerns in e-learning education. In: Proceedings of ICERI2014 Conference, 17th–19th November 2014
21. Bohli, J.-M., Langendörfer, P., Skarmeta, A.F.: Security and privacy challenge in data aggregation for the iot in smart cities. In: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, pp. 225–244 (2013)
22. Andrejevic, M.: Privacy, exploitation, and the digital enclosure. Amsterdam LF **1**, 47 (2008)
23. Kizza, J.M.: Guide to Computer Network Security. Springer, London (2009). https://doi.org/10.1007/978-1-4471-4543-1
24. Hussain, H., Embi, Z.C., Hashim, S.: A conceptualized framework for edutainment. Informing Science, InSite-Where Parallels Intersect, 1077–1083 (2003)
25. Santonen, T., Faber, E.: Towards a comprehensive framework to analyse edutainment applications (2015)
26. Ganorkar, S.S., Kandasamy, K.: Understanding and defending crypto-ransomware. ARPN J. Eng. Appl. Sci. **12**(12), 3920–3925 (2017)
27. Shinde, R., et al.: Ransomware: studying transfer and mitigation. In: 2016 International Conference on Computing, Analytics and Security Trends (CAST). IEEE (2016)
28. Luo, X., Liao, Q.: Awareness education as the key to ransomware prevention. Inf. Sys. Secur. **16**(4), 195–202 (2007)
29. Stojanović, Z., Dahanayake, A.: Service-oriented Software System Engineering: Challenges and Practices. IGI Global, Hershey (2005)
30. Johnston, J., Eloff, J.H., Labuschagne, L.: Security and human computer interfaces. Comput. Secur. **22**(8), 675–684 (2003)
31. Regulwar, G.B., Gulhane, V.S., Jawandhiya, P.: A security engineering capability maturity model. In: 2010 International Conference on Educational and Information Technology (ICEIT). IEEE (2010)

32. Chehab, M.I., Abdallah, A.E.: Assurance in identity management systems. In: 2010 Sixth International Conference on Information Assurance and Security (IAS). IEEE (2010)
33. Clauß, S., Köhntopp, M.: Identity management and its support of multilateral security. Comput. Netw. **37**(2), 205–219 (2001)
34. Lee, S.C.: An introduction to identity management. SANS Institute (2003)