Security Vulnerabilities in Game Software:

Ethical Values and User Privacy

Yunus Emre Ekinci

Department of Computer Engineering, Istanbul Arel University

Professional Responsibilities and Ethics

Tahsin Ayhan KEPEKLİ

April 6, 2024

Abstract

This article addresses ethical issues related to digital security and data privacy within the discipline of computer engineering. It includes a discussion of how ethical violations can occur through a hypothetical event, how this situation can be handled, and what consequences it will have.

Introduction

Nowadays, the development of technology and the resulting communication methods has led to an increase in the data in circulation, the storage of these data with or without consent, and their unethical use for personal purposes. In this article, a hypothetical ethical violation scenario that we may encounter as a computer engineering student will be examined.

Data security breach

Let's imagine that, as a computer engineer, we are on the development team at Awaken Games, a game studio. The studio is a successful company with good sales figures for today's market. The company often releases story-based and single-player games, but they are designing their latest game as a role-playing game with massive multiplayer, and the studio is releasing the game as early access to keep investors happy. The game has been receiving a lot of negative feedback since it was first released, and as the developer team, you have been working hard to respond to feedback and fix in-game errors. During the editing, you realize that there is a security vulnerability that allows unauthorized access to the information that the players enter to register, such as their name, surname, e-mail, and the credit cards they use for in-game micro-purchases. Thanks to the vulnerability, you detect that user data is at risk and has the potential to be stolen. Although you report the situation to the upper management, the management declares that in-game errors are a priority and does not allocate enough resources to security vulnerabilities.

In this case, you are left with an ethical dilemma. On the one hand, you want to protect players' personal information, but on the other hand, you also have to comply with the studio's policies and the process to be followed. What needs to be done in this situation? Should we take action to protect users' privacy and security or act in accordance with management's decision?

In conclusion

This scenario gives a different perspective to think about what kind of ethical decisions and dilemmas an employee may face and what attitude to follow in such situations. Such scenarios enable the sharing of ideas on ethical principles in difficult situations that may be encountered in business life and discussions on how to deal with these difficult situations.

References

[1] https://www.cybersecurity-help.cz/vdb/software/client/games/

[2] https://www.imperva.com/blog/cyber-attacks-gaming-industry/

[3] https://www.kaspersky.com/resource-center/threats/top-10-online-gaming-risks

[4] https://www.identity.com/cybersecurity-challenges-in-the-gaming-industry/