



CASE STUDY

SECURITY IN ONLINE GAMES

Rudra Kamal Sinha Roy

Product Manager

iViZ Techno Solutions Pvt Ltd

An IDG Ventures Company





Introduction

With the emergence of technology in recent years, the gaming industry has changed significantly enabling new ways of playing games. PC or console games are not any more the only mode in the gaming world, since we are seeing a new era of online games. However along with all the fun, security landscapes for computer games have also changed. From PC games where the main concern is copy protection, online games, however has a different requirement for security. Firstly, online games are meant to be a distributed E-commerce application which leads to complicated security issues. On the other hand, online games have their own unique security challenges. Usage of cutting edge technology (e.g computer graphics, artificial intelligence, human computer interaction and programming) along with ignorance of game security issues has made the online gaming providers and players land into trouble.

The client

The client is one of the most popular global flash games in the world and hosts its own proprietary games. The client has its own studios and creative art, production and programming teams to make sure that each game they create and host is of the best quality. They are probably the world's largest flash game producer producing almost one new flash game a day. They are also the leading MMOG (Massive Multiplayer Online Games) game operator in India. They are the exclusive licensee of SEGA's Car Racing MMOG Game and have distributed the game across the breadth and width of India.

Security Issues for the client

The main security issues with the client were "cheating" in their gaming application and maintaining secure internal network and infrastructure. While cheating is a security issue across all gaming segment, complex bugs like those involving "time and state" were threatening the client's multiplayer online role-playing game (MMORPGs). A year back the client had moved to Web services and service-oriented architecture (SOA)



built with technologies like Ajax and Ruby. This has invested heavily to the security concerns of their gaming application. The primary security challenges for the client's online games came from variety of sources: players to sophisticated attackers. The attacker used to break the games' security and accumulate virtual items or gained experience points for their characters. Many of these items, and even the characters themselves, were then sold off to the highest bidder.

Their effort so far

Hired a consultant: They hired a consultant who uses publicly available software. The results, however, had not been consistent across all environments and, therefore, not repeatable and scalable. Also, effectiveness depended on the skill of the tester, not the quality of the methodology. Thus they hadn't been quite successful with this approach because it merely helped towards betterment of the security posture in the gaming application and their internal network.

Develop internal security capabilities: As the earlier approach failed, they tried to internally develop security testing and maintenance capabilities. But they quickly found out that it's difficult to find security professionals with sufficient knowledge, and publicly available tools are not quality assured, which can sometimes backfire. The fact that this option required a lot of time from a highly specialized team invariably made it expensive.

iViZ approach

Because of the technology uniqueness, iViZ was engaged to carry out in depth penetration testing and help secure the client's application and network. iViZ allocated a team of 2 penetration testing engineers to work on the project. iViZ utilized its On Demand Penetration testing technology to find out vulnerabilities from a black-box perspective. The testing team additionally carried out specific manual tests to find out critical vulnerabilities for the gaming application. The approach that iViZ adopted for this exercise is:



- Understand the gaming functionality and technology used
- Identify all the critical assets involved in the architecture
- Study and identify architectural vulnerabilities
- Automated Vulnerability assessment
- Exploitation and verification of cheating techniques
- Manual testing for broken trust models
- Accurate Attack vector identification
- Developing proof-of-concepts for presentation
- Training to the development team about the findings and issues
- Re-test for critical vulnerabilities to verify appropriate remediation

How the client benefitted?

- Found out all existing infrastructural and application vulnerabilities
- Verified the possible ways of online cheating and remediated the same
- Carried out testing at regular intervals at a much lesser cost which increased ROI
- The client's team developed significant knowledge in software security
- Introduced secure coding practices for secure game development
- Black-box test gave complete perspective of the attacks from outside world
- Gaming experience became better with improvement in system performance
- "Lag" caused by botnets are completely removed
- ROI increased with effective utilization of bandwidth and network resources
- Safeguarded brand integrity and enhanced gamers' loyalty.