

# Security for Online Game Development

## Preventing Cheating for Massive Multi-Player Online Games

### Preventing Cheating Through Security

Cheating reportedly exists in all multiplayer online games, with potentially serious impact for many online players around the globe. The impact is particularly serious in large, long-lasting online games. The internet provides both the anonymity and the resources to cheat in online games. Numerous cheating techniques are known, including device modifications (e.g. tapping / lagging, disconnecting), bug exploits, game code modification, system software modification, and network packet interception, tampering, manipulation, denial-of-service, collusion (just to name a few). Good online game security requires a multi-faceted approach. Protection of payment details and virtual assets is an obvious critical requirement, which first of all means making modifications to the client game or system software / hardware as difficult as possible.

### Information Flow Control in Online Games

In addition, the information transmitted between the participants and the server – which ultimately determines much of the outcome of games – also needs to be protected. In particular, information should only be available to clients on a need-to-know basis. This means that a hacked client will not be able to gain access to any unauthorized game information. Information can be intercepted and/or manipulated in real-time while in transit. This can be done passively (e.g. attacks such as ghosting and extrasensory perception) or actively (e.g. wall-hacks). Such information attacks can be performed on the client machine itself or by a proxy. Encryption helps, but is only a part-solution.

### Game-Wide Security Policy Management

A critical piece of the security architecture is fine-grained security policy management to regulate the flow of the right information to the right clients. Broadcasting unnecessary information needs to be minimized to minimize the attack surface. Defining and enforcing security policies for the large amount and complex nature of the content exchanged between nodes in online games is a challenge. Moreover, this challenge gets amplified by the number of nodes involved in multi-player online games. Incident monitoring is an added challenge because of the amount

and complexity of alert information that needs to be mined as near to real-time as possible to allow game administrators to deal with cheating before damage materializes.

ObjectSecurity's OpenPMF security policy management product is an important part of an online game security architecture. It uniquely enables game administrators to define security requirements closer to the thinking of the actual game logic and content, which is more manageable for humans than defining detailed technical policy rules the used software platform supports (e.g. application server policies). Using "model-driven security", the OpenPMF solution automatically turns these games-centric policies traceably into technical security policy rules that are enforced across the IT landscape at run-time. It also monitors for incidents. OpenPMF can protect many standard technology platforms based on service-centric, data-centric, publish-subscribe-centric, invocation-centric architectures. Proprietary technologies can also easily be supported.



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a "model-driven security" approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

### Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

[www.objectsecurity.com](http://www.objectsecurity.com)