

Security for Collaborative Training

Security: Enabler for Information Sharing in Collaborative Synthetic Training Environments

Collaborative Synthetic Training Environments

Many industries today make use of realistic simulation environments for training purposes. Synthetic training is typically cheaper and safer than real-world training. In addition, a synthetic environment can simulate many training situations more easily than real-world exercises. Examples of users of collaborative synthetic simulation and training environments include defense, crisis management & emergency response, and air traffic management. These collaborative training scenarios involves many stakeholders, sharing of many information sources, and complex interactions and information flows.

No Security Means No Information Sharing

Information security plays a big role in information sharing for collaborative synthetic training environments because of the sensitivity and / or value of the information itself, and because of the increased dependence on the correct and timely information. Because responsibilities for certain business functions are normally clearly assigned, there is often an initial resistance to basing decisions on information provided by other sources that are perceived to be obtained in a less trustworthy manner. Good security helps mitigate this problem.

Information Flow Control in Online Games

For political and legal reasons, secure information sharing will only happen if all stakeholders trust the collaboration system to ensure that their information is only transmitted to authorized other stakeholders, that this information is only made available on a need-to-know basis, and that received information they are basing their decision-making upon comes from the intended source. This applies both to information intended for humans (e.g. communications) and machines (e.g. from simulated radar systems).

Need for 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 to other stakeholders needs to be minimized to prevent misuse. Depending on the trust boundaries, policy management can be under a centralized authority, or each trust boundary controls access to its own information autonomously. Defining and enforcing security policies for the large amount and complex nature of the content

exchanged between many nodes is a challenge. 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 detect and mitigate problems quickly.

ObjectSecurity's OpenPMF security policy management product is an important part of an online game security architecture. It uniquely enables 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