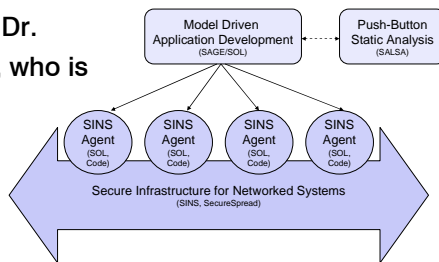


Press Release – ObjectSecurity partners with U.S. Naval Research Laboratory to productize SINS middleware

(Washington D.C., USA and Cambridge, UK – 01 May 2007) – ObjectSecurity, a leading expert for middleware security, trusted SOA, and model driven security policy, announced today that it has partnered with the U.S. Naval Research Laboratory (NRL) to productize NRL's SINS software technology. Both ObjectSecurity and NRL intend to work together to complete the SINS prototype and bring it to a certified, ready-to-market product state. SINS is currently at a full prototype technology readiness level (TRL) and all concepts have been successfully validated.

According to NRL's Dr. Ramesh Bharadwaj, who is responsible for the SINS project, and his colleague Jim Kirby, NRL intends to pursue several funding opportunities for their planned SINS commercialization strategy with ObjectSecurity.



SINS: Middleware for Mission-Critical Deployments

SINS middleware supports the implementation of secure, distributed applications. It has some unique features that differentiate it from other middleware:

- ▶ **Guaranteed Delivery vs. Best Effort:** For high system reliability, SINS guarantees that all messages get delivered to all relevant applications in the same order (called total ordering), and that messages only get delivered to all relevant applications or none at all.
- ▶ **Guaranteed Preservation of Global Properties:** For high system reliability, SINS also guarantees that certain system properties, such as ranges of system variables, meet specified constraints (global shared state). Static analysis is done using NRL's SALSA tool. Dynamic analysis, reporting, and response at run-time are done using monitoring agents (e.g. security agents).

- ▶ **Application Survivability:** To make sure SINS applications still function in hostile environments, SINS supports a replication and state propagation mechanism which tolerates the loss of individual nodes without losing information or functionality.
- ▶ **Strong Information Security:** To ensure good information security, SINS includes a number of features, such as group confidentiality by encrypting all data using the Blowfish algorithm with a contributory key agreement protocol, security monitoring/reporting agents.
- ▶ **Model Based Application Development:** To simplify application development, NRL's SAGE and SOLJ technologies allow SINS applications to be easily developed using graphical UML tools. SAGE also enables the easy reconfiguration of application functionality and deployment.
- ▶ **Support for Central Administration:** To monitor and manage system activity and incidents effectively, SINS supports the use of a central console application. In addition, monitoring consoles can also be deployed on several (or all) nodes.
- ▶ **Certifiable Code Base:** Thanks to its very small code base, SINS is ideally suited for accreditation under Common Criteria, even to higher EALs.
- ▶ **Scalability:** SINS can scale to tens of thousand of hosts and hundreds of thousands of agents.

Commercial Technical Support and Services

SINS is vendor-supported by ObjectSecurity on behalf of NRL. Support contracts, consulting, and development services help you evaluate, deploy, and maintain SINS applications.

To learn more, we invite you to talk with us about the solution that works for your needs and environment.

Please contact us at: info@objectsecurity.com.

www.objectsecurity.com