

Secure Application Development Resources

DAS EISPD Enterprise Security Office

May 1, 2008

Secure application development is more than just application coding techniques. In order to develop secure applications an organization must have a stable development environment with solid development practices; it must support application security as a business goal, integrate security processes and standards across business and technical units, periodically review application and business processes, and support ongoing security education for developers, analysts and managers.

A decent overview of application development security concerns, suitable as an introduction for anyone who wants to better understand the problem, is Microsoft's "Writing Secure Code – Best Practices" Powerpoint presentation (<http://msdn.microsoft.com/en-gb/security/aa473879.aspx>) . Although this goes into more coding detail than non-developers will normally need, it quickly covers many of the important areas at an overview level. For a more in-depth analysis of general issues surrounding developing application security, the Burton Group has several papers available to subscribers. A good place to start is their "Application Security:Everybody's Problem" paper (<http://www.burtongroup.com/Client/Research/Document.aspx?cid=709> – Note that access to this document requires registration from a "state.or.us" email address and is limited by license to State of Oregon employees).

In addition to the business infrastructure support of secure applications, integration of security into all aspects of the software development life cycle (SDLC) is necessary. One common example is the failure to identify and integrate security requirements early in the application development process, resulting in costly fixes at a later time. A good description of the role security should play in all phases of the SDLC is the National Institute of Standards and Technology's "NIST-SP800-64 – Security Considerations in the Information System Development Life Cycle" (<http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>).

For intensive technical training on secure programming and testing techniques, the System, Audit and Network Security (SANS) organization is a valuable resource for developers. The Enterprise Security Office has had positive experience with their information security courses. SANS developer courses can be found at: <http://www.sans.org/training/courses.php#developer> . SANS also offers developer security certification.

Detailed secure coding guidelines can be found at the Open Web Application Security Project (OWASP). They have a variety of resources to educate developers on Web application security pitfalls. The "Top Ten Application Security Vulnerabilities for 2007" (http://www.owasp.org/index.php/Top_10_2007) is a compilation of the most prevalent and dangerous Web application vulnerabilities with descriptions of how they work, how to guard against them, and code examples for avoiding them. Comprehension of this document and adoption of its guidelines should be required for all developers and application testers who contribute to Web application development.

Developing secure applications is a topic that requires not only extensive education but also dedicated and ongoing organizational support. The resources and recommended reading presented here provide guidance for agencies undertaking this effort.