Open Web Application Security Project (OWASP)

AppSensor Project Team

Response to NIST SP 800-137 (Initial Public Draft)

Introduction

The following four comments are submitted on behalf of the OWASP AppSensor project team, following our own consultation process.

Our feedback to NIST on continuous monitoring relates to our experiences of building security controls directly into software code so that applications are are attack aware, and able to undertake context-specific pro-active defensive measures.

Response

a) Actual real-time

Page 10 refers to "real-time or near realtime security-related information", but elsewhere (e.g. pages 1, 2, 6, 7, 13, 14, 29, etc) the phrase "near real-time" is used instead. The guidance should explicity include actual realtime monitoring at each reference to "near real-time", so that it is not excluded from the guidance.

b) Automation

In "3.2 Role of Automation in Continuous Monitoring", human analysis will not necessarily be required for the interpretation of findings in application-specific attack detection and response, because the actions are undertaken in real-time within the timeframe of the user request and software response. Instead, human analysis will be required to assess, define and implement the policies in advance. Thus in some situations the number of steps shown in Figure 3-1 on page 20 (Continuous Monitoring Process) may be one less, when "Analyse/Report" and "Respond" are collapsed into a single item. This concept also relies on some overlap between the tiers indicated in Figure 2-1 on page 8 (Organization-wide Continuous Monitoring) i.e. the software application combines information from Tier 3 (information systems) and Tier 2 (mission/business) giving a very low false positive attack detection rate.

c) Security automation domains

The list and descriptions of the eleven security automation domains in Appendix D (pages D-2 and D-3) does not seem to adequately cover, or allow for, application-specific attack detection and response. Neither "Event & Incident Management" (section D.1.2) nor "Network Management" (section D.1.6) describe what the much broader possibilities when building defensive measures into the software code itself. In this development defense in depth pattern, there is full knowledge of the business logic, user session, user role, user permissions, input data formats, allowable entry points, historical usage, etc, and proactive defensive measures can be undertaken in real-time. It is vastly different to the IDPS described (in D.1.2) due to the contextual awareness and the ability to detect and respond to attacks that are otherwise unanticipated. We therefore propose a twelfth domain of "Application Management".

OWASP would be pleased to provide some draft text for this proposed domain if required, linking the reduction in operational risk to the security controls in NIST SP 800-53.

d) Security automation examples

In D.3 Automation and Data Sources", the bulleted list of "examples of security automation activities" (page D-11), we would suggest adding a fifth item "Building in application-specific attack detection and response" since this is a relatively new concept which may not be considered due to lack of awareness and thus the potential benefits left unexploited.

About the OWASP AppSensor project

This response is submitted on behalf of the OWASP AppSensor project team. The AppSensor project defines a conceptual framework, methodology and example code that offers prescriptive guidance to implement attack detection and automated response into software applications. The concept has been piloted and is in use defending real-world applications.

Further information:

- AppSensor project
  http://www.owasp.org/index.php/OWASP_AppSensor_Project
- Detection points
  http://www.owasp.org/index.php/AppSensor_DetectionPoints
- Response actions
  http://www.owasp.org/index.php/AppSensor_ResponseActions

About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a U.S. recognized 501(c)(3) not-for-profit charitable organization, that ensures the ongoing availability and support for our work at OWASP.

Further information:

- OWASP Foundation
  http://www.owasp.org/index.php/OWASP_Foundation
- About The Open Web Application Security Project
  http://www.owasp.org/index.php/About_OWASP