Category:Principle

From OWASP

This category is for tagging articles related to application security principles.

Contents

What is an application security principle?

Application security principles are collections of desirable application properties, behaviors, designs and implementation practices that attempt to reduce the likelihood of threat realization and impact should that threat be realized. Security principles are language-independent, architecturally-neutral primitives that can be leveraged within most software development methodologies to design and construct applications.

Principles are important because they help us make security decisions in new situations with the same basic ideas. By considering each of these principles, we can derive security requirements, make architecture and implementation decisions, and identify possible weaknesses in systems.

The important thing to remember is that in order to be useful, principles must be evaluated, interpreted and applied to address a specific problem. Although principles can serve as general guidelines, simply telling a software developer that their software must "fail securely" or that they should do "defense in depth" won't mean that much.

Some proven application security principles

- Apply defense in depth (complete mediation)
- Use a positive security model (fail-safe defaults, minimize attack surface)
- Fail securely
- Run with least privilege
- Avoid security by obscurity (open design)
- Keep security simple (verifiable, economy of mechanism)
- Detect intrusions (compromise recording)
- Don’t trust infrastructure

- Don’t trust services
- Establish secure defaults (psychological acceptability)

Applying security principles

Consider the exercise of designing a simple web application that allows one to send email to a friend. By evaluating and interpreting each principle, we can arrive at many of the threats to this application and ultimately derive a set of protection requirements. We want to end up with a complete list of what is required to offer this service securely.

References

- Saltzer and Schroeder (http://web.mit.edu/Saltzer/www/publications/protection/Basic.html) (see section 3)
- The Six Dumbest Ideas in Computer Security (http://www.ranum.com/security/computer_security/editorials/dumb/index.html)
- Gary McGraw's 10 steps to secure software (http://news.com.com/2008-1082-276319.html)
- OWASP Development Guide Project
- Engineering Principles for Information Technology Security (EP-ITS), by Gary Stoneburner, Clark Hayden, and Alexis, NIST Special Publication (SP) 800-27 (PDF) (http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf)
- Secure Design Principles (http://www.developer.com/java/data/article.php/10932_3667601_1) from "Foundations of Security: What Every Programmer Needs To Know" by Neil Daswani, Christoph Kern, and Anita Kesavan (ISBN 1590597842 (http://www.biblio.com/isbn/1590597842.html))
- High-Assurance Design (http://assuredbydesign.com/haa/) by Cliff Berg, 2005, Addison-Wesley. Foreword by Peter G. Neumann. Design principles and patterns for secure and reliable design.

How to add a new Principle article

You can follow the instructions to make a new Principle article. Please use the appropriate structure and follow the Tutorial. Be sure to paste the following at the end of your article to make it show up in the Principle category:

```
[[Category:Principle]]
```

Pages in category "Principle"

The following 18 pages are in this category, out of 18 total.

A **D cont.** **M**

- Assume attackers have source code
- Avoid security by obscurity

D

- Defense in depth
- Detect intrusions
- Don't trust user input
- Don’t trust infrastructure
- Don’t trust services

E

- Establish secure defaults

F

- Fail securely
- Fix security issues correctly

K

- Keep security simple

L

- Least privilege
- Minimize attack surface area

P

- Positive security model

S

- Secure Coding Principles
- Separation of duties

T

- The Insecure-Bootstrapping Principle

U

- Use encapsulation

Retrieved from "https://www.owasp.org/index.php?title=Category:Principle&oldid=121314"
Category: OWASP ASDR Project
