Code review

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-115, OWASP

1. Planning

2. Overview

3. Preparation

4. Inspection

5. Rework

6. Follow-up

Static testing

* automated tools designed to detect common software flaws, such as buffer overflows

Dynamic testing

* web application scanning tools to detect the pres- ence of cross-site scripting, SQL injection, or other flaws in web application.
* synthetic transactions to verify system perfor- mance. These are scripted transactions with known expected results. The testers run the synthetic transactions against the tested code and then compare the output of the transac- tions to the expected state. Any deviations between the actual and expected results repre- sent possible flaws in the code and must be further investigated

Fuzz Testing

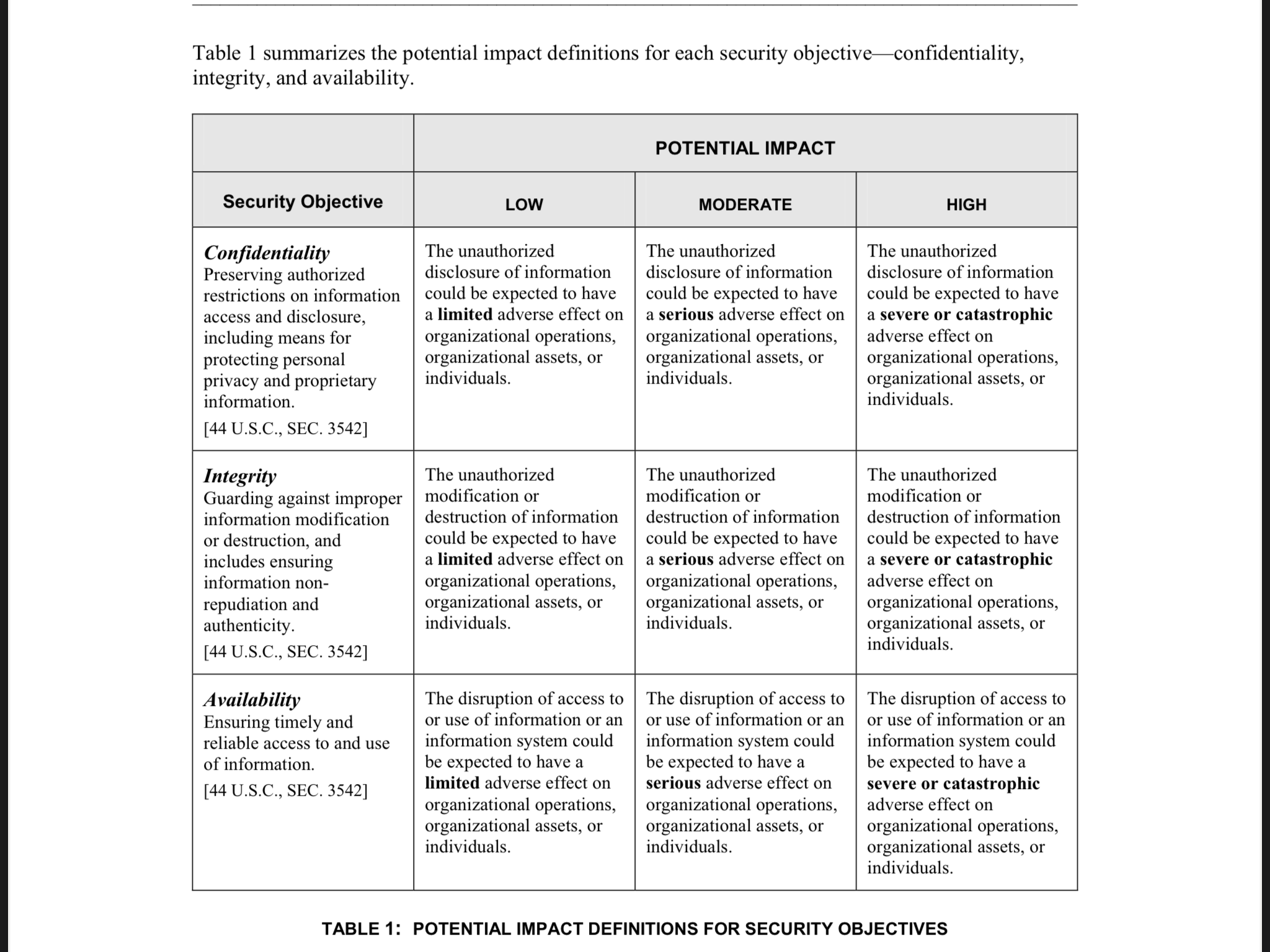
The fuzz tester then monitors the perfor- mance of the application, watching for software crashes, buffer overflows, or other undesir- able and/or unpredictable outcome

* Generational (Intelligent) Fuzzing Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program

**Reference**

1. <https://owasp.org/www-project-web-security-testing-guide/>
2. <https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html>
3. <https://dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html>

**Appendix**

**FIPS-199**