Tailored Vulnerability Assessment

OVERVIEW

Assured Information Security (AIS) has a proven track record well versed in the vulnerability assessment and analysis of complex systems. Our approach has been used to identify security vulnerabilities in software systems, computer networks, infrastructure devices, wireless networking equipment and embedded systems for over 10 years.

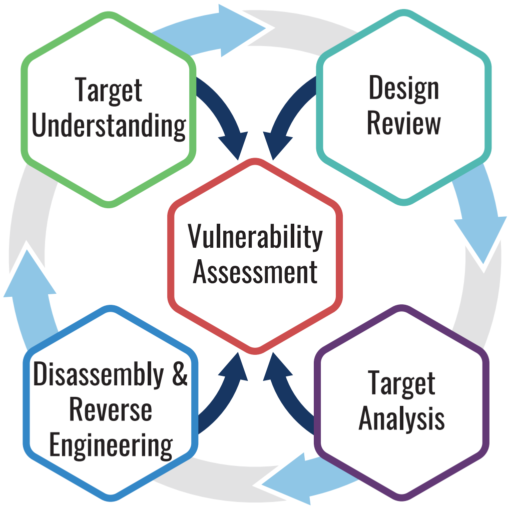
eeo/aa: 2/5/2019/1

Tailored Vulnerability Assessment

Process

The AIS vulnerability assessment methodology is a cyclic assessment process where the team's knowledge of a target evolves, and new test cases and attack vectors are identified and incorporated into the assessment.

The basic process taken by AIS to perform a security analysis of any software system or hardware device is guaranteed to follow the same basic steps every time. The roots of this process lie in the fundamental engineering need to fully understand and evaluate any piece of technology we test. This process is normally separated into five major phases as detailed in the diagram to the right. The target understanding and design review process provide the background and details required to understand the system and its potential flaws. The disassembly and reverse engineering process and the target analysis phase allows for the advanced interaction and monitoring of the system to identify the potential vulnerabilities. The vulnerability assessment process provides a means to generate the attacks against the system and observe functionality, including failure, where applicable.



Applicability

The AIS vulnerability assessment process is designed to evaluate overall system functionality, verify security soundness, identify observables and limitations, and characterize behavior that may lead to system compromise or failure. Software packages and systems are tested to ensure overall functionality is achieved at the level the customer desires. Once functionality is proven, the AIS security assessment process applies state of the art vulnerability detection methodologies against the target system in an effort to identify any possible weaknesses in the system.

This process identifies limitations of the target system and provides the customer with insight as to where their software or system may fall short when targeted by an attacker. Analysis focuses primarily on identification of vulnerabilities caused by:

- Insecure design and implementation
- Software input validation
- Authentication and encryption weakness
- Exposed network communications
- Component and environment dependencies

BENEFITS

Tailored vulnerability assessment of a target system can provide the client with several benefits including:

- Identify vulnerabilities in systems before they are exploited
- Establish a baseline understanding of the security of a target system
- Evaluate adherence to design policies or regulatory compliance
- Protect the system from attacks by hackers, competitors, and general outsiders
- Reduce costs and downtime associated with attacks and vulnerabilities within their system
- Protect and strengthen their public and customer reputation

ABOUT AIS

AIS is a cyber and information technology company that plays a leading role in supporting critical cyber operations for the United States Department of Defense and Intelligence Community. AIS employs cyber engineers and scientists throughout the United States.

FOR MORE INFORMATION

bd@ainfosec.com

New York • Colorado • Georgia • Oregon • Massachusetts • Maryland • Virginia

Assured Information Security • 315.336.3306 • WWW.AINFOSEC.COM

ais