
WHITEPAPER

Device Security Assurance Center (DSAC)



—

If data is the new currency in today's interconnected world, then data communication is the transaction.

Introduction

Smooth data communication is central to running critical infrastructure, transportation and industrial networks of all kinds. It depends on the ability to migrate communication infrastructure, its management and associated connected applications from traditional technologies to externally accessible interfaces like ethernet-based networks or wireless based communication. But, these communication hubs along with modern-day software and hardware are increasingly susceptible to security breaches, hacking and cyber-attacks. In 2017, the NotPetya malware and the WannaCry ransomware attacks made international headlines⁽¹⁾. The latter ransomware attack impacted Windows servers and focused on a known vulnerability that could have been easily solved with patch management⁽²⁾.

Over the past several years, worrisome, major attacks have also resulted in serious breaches of personal data. A 2013 attack on Yahoo exposed information from billions of user accounts⁽³⁾. More recently, in 2018, Marriott reported its second major security breach in less than two years⁽³⁾⁽⁴⁾. The increasing frequency and sophistication of

attacks has drawn attention to the need for proper security controls and measures.

At ABB, we know that is essential to mitigate security threats and to implement layered security measures in our products and offerings. To accomplish these goals, we weave cyber security into our products life cycle, including testing. In 2009, we established the Device Security Assurance Center (DSAC) to improve product quality by testing with the aim of assuring our customers that we take cyber security seriously.

In this paper, we offer insights into our approach to cyber security testing and present information, which will help you understand just what we do at DSAC.

Device Security Assurance Center

DSAC's approach to testing

DSAC addresses possible cyber threats by identifying, device weaknesses and communicating this to the product development team for subsequent remediation. ABB's internal security assurance center is independent from the product development organization. As such, this center provides common testing for all ABB businesses as part of the secure development lifecycle process. DSAC leverages appropriate open source, commercial and proprietary robustness, vulnerability analysis and cyber security test tools in its product security testing procedures.

The center follows a consistent systematic approach to cyber security testing for ABB products. By closely collaborating with developers, DSAC not only provides an in-depth analysis of the test objects, but also recommends concrete improvement or mitigation actions.

Cyber security testing: an overview

Security assessment employs a multitude of testing techniques derived from ABB's testing policy to discover a variety of security weaknesses, eg, bugs and vulnerabilities. After all it is the smallest security flaws that often lead to the most disastrous security breaches. For robustness tests, test cases include reconnaissance, flooding/Storm-, and fuzzing test cases, as well as known vulnerability checks. Security testing is also performed on web and mobile applications. The center performs a security assessment of Android and iOS apps and audits mobile app files and data for security bugs. Every test is conducted in a coordinated manner by following a set of pre-defined test procedures that include analysis based on delineated pass criterion. Four basic categories of tests are conducted: basic hygiene testing, communication stack robustness assessment, web and API tests, and mobile application testing.

Basic hygiene testing

To check that basic requirements such as the Principle of Least Privilege are properly implemented, DSAC specialists conduct basic hygiene tests. These tests determine if open ports/services are required; they also analyze for known vulnerabilities within the product undergoing testing. For instance, an automated vulnerability scan can identify weaknesses and security holes (based on a published vulnerability knowledge base with a finite number of checks and tests). Vulnerability checks are made with tools like Nmap⁽⁶⁾ and Tenable Nessus⁽⁶⁾, among others, to identify vulnerable configurations etc. By attempting to crash targets, consume bandwidth and identify weaknesses, and so forth, test results enable vulnerabilities to be better understood; a DSAC specialist can then make recommendations concerning any discovered vulnerabilities. Importantly, such actions can also help in mitigation of such weaknesses in future product versions.

Communication stack robustness assessment

A robustness assessment measures the extent to which the network protocol stack implemented on an embedded device/software can survive unusual or intentional malicious traffic received from any network.

Two types of tests are conducted: resource exhaustion and fuzzing test.

- Resource exhaustion: This method simulates Denial of Service (DOS) attacks, eg, by flooding the device with a very high number of randomly generated packets.
- Fuzz testing: This test sends sets of random/invalid/malformed crafted protocol packets to the product being tested to discover security weaknesses (eg, coding errors such as buffer overflows and format string bugs) in the protocol implementation. Fuzzing can also be used to achieve DOS simulations because at times a device might reboot or service might cease without recovery.





Resource exhaustion tests are performed with regular and malicious packets that aim to exhaust resources such as network bandwidth, CPU time or memory. Product reliability and availability of the target can be assessed using tools such as IP Stack Integrity Checker (ISIC), or Achilles Test Platform tool⁽⁷⁾.

Fuzz testing, on the other hand, aims to identify (zero-day) vulnerabilities in software implementation, etc. A variety of tools are employed to identify programming implementation flaws in protocol implementation, eg, Achilles Test Platform⁽⁷⁾ and Synopsys Defensics⁽⁸⁾.

Inappropriate responses, no message responses; and failure of the product to continue to adequately maintain essential service, or even to maintain the device's normal state when it reboots, are important testing results that demonstrate potential security vulnerabilities within the product. Developers use these result to initiate mitigation/improvement actions.

Web and API testing

These tests are used to find vulnerabilities in web and API applications in ABB products. Tests identify issues in the backend database, web server and communication protocol used; as well as logical flaws and security flaws in recently updated language, access management and session management. In general, these tests function to:

- Identify security vulnerabilities or flaws on external facing APIs and whether internal APIs are bound to web applications
- Verify security configuration of the application/interfaces of the product undergoing testing

Specifically, web vulnerability scanning, eg, with Burp Suite Professional, relies on automatic and manual analytical techniques to identify weaknesses in both the application and architecture, eg, cross site scripting, injection flaws, sensitive data exposure and security misconfiguration among others. Significantly, these tests are run on a web application against OWASP Top 10⁽⁹⁾.

Automated API security assessments discover possible OWASP API Security Top 10⁽¹⁰⁾ vulnerabilities in the API implementation with toollike Netsparker API⁽¹¹⁾.

Mobile application testing

Testing of mobile applications relies on security assessments of Android and iOS apps to rapidly detect publicly disclosed vulnerabilities on identified exported activities using appropriate tools, eg, QARK⁽¹²⁾ and MobSF⁽¹³⁾. The simplicity and efficiency of these tests enable isolation of security weaknesses with respect to authentication mechanisms, files, backend databases, web API and any logical issues found.

Detecting and reporting for a better product

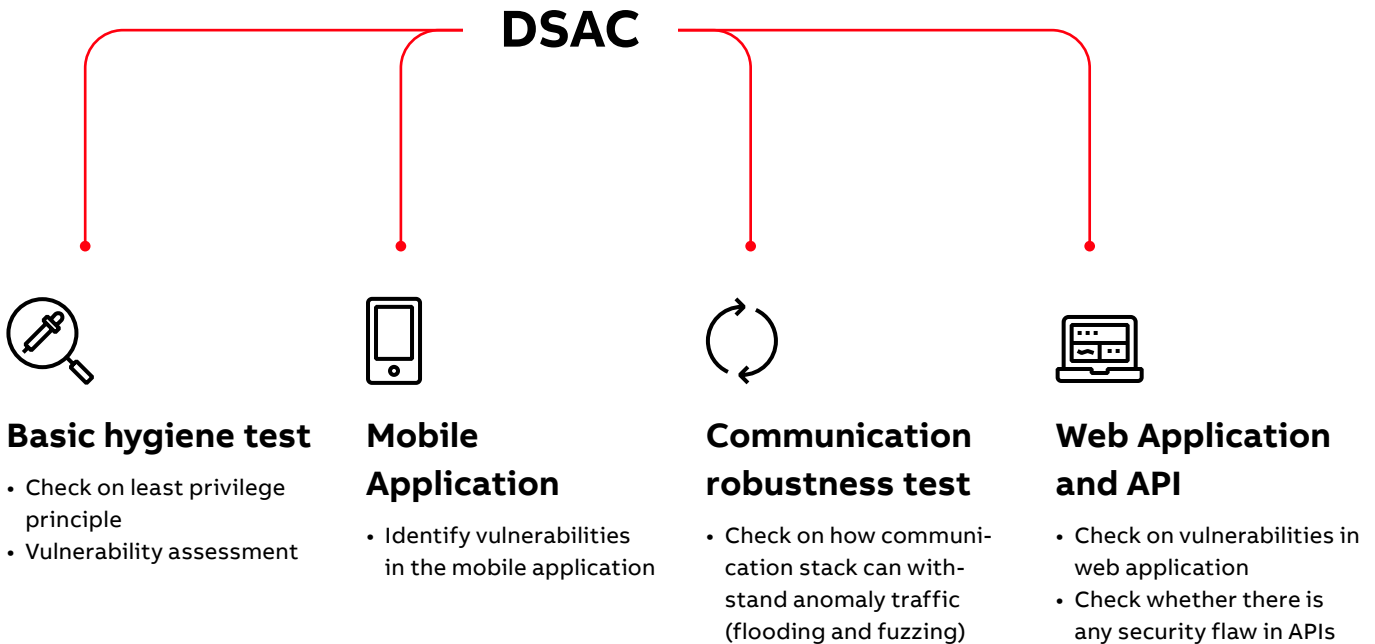
As a trusted technical partner, ABB's DSAC facility was the first vendor lab accredited by Wurldtech to perform Achilles (ISA Secure partner) CRT test Level 1 and Level 2 certification on ABB products. This achievement is a manifestation of the expertise and experience that DSAC specialists exhibit whenever they examine products.

With reliance on ABB's holistic approach to all areas of cyber security, it comes as no surprise that DSAC has the key function of detecting and classifying security vulnerabilities accordingly based on a pre-defined classification scheme that also takes into account the product team's input. Apart from this, the center prepares comprehensive test reports that include analyses and results of all issues discovered; details of all actionable insights and a clear description of all vulnerabilities discovered. Furthermore, reports include information about the complexity of these vulnerabilities. In addition, the report delineates the steps that are necessary to address and mitigate each weakness that is discovered.

Hence, DSAC not only simplifies the work of the development team by reproducing the reported security issues in a controlled laboratory environment, but they also provide indispensable recommendations about how to fix any identified flaws.

Through comprehensive security testing, ABB's approach to product security underpins our offerings and demonstrates continued care with regard to our customers' operational integrity and data security. After all, cyber security and data protection start with people, process and technology and are fundamental to our business and our customers' successful digital transformation.

01 ABB's DSAC center carries out a multitude of tests to discover possible weaknesses in products.



- (1) The 15 biggest data breaches of the 21st century, [Online]. Available: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>. [Accessed: June 25, 2020].
- (2) A. Greenberg, "The Wannacry Ransomware Hackers Made some Real Amateur Mistakes", in Wired, May 15, 2017, [Online]. Available: <https://www.wired.com/2017/05/>. [Accessed May 12, 2020]
- (3) B. Barrett, "Hack Brief: Marriot Got Hacked. Yes, Again", in Wired, March 31, 2020, [Online]. Available: [https://www.wired.com/story/marriott-hacked-yes-again-2020/#:~:text=That%20hack%20compromised%20the%20information,5.2%20million%20guests%20at%20risk](https://www.wired.com/story/marriott-hacked-yes-again-2020/#:~:text=That%20hack%20compromised%20the%20information,5.2%20million%20guests%20at%20risk.). [Accessed June 25, 2020]
- (4) T. Brewster, "Revealed: Marriot's 500 Million Hack Came After a String of Security Breaches", in Forbes, Dec. 3, 2018, [Online]. Available: <https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#9380850546f4>. [Accessed June 25, 2020]
- (5) Nmap.org, "NMap Port Scanner", Nmap.org. [Online]. Available: <http://nmap.org>. [Accessed May 12, 2020].
- (6) Tenable, "Nessus Vulnerability Scanner", Nessus.org. [Online]. Available: <https://www.tenable.com/products/nessus>. [Accessed May 12, 2020].

- (7) Achilles Test Platform from GE Digital, https://www.ge.com/digital/sites/default/files/download_assets/achilles-test-platform-from-ge-digital-datasheet.pdf. [Accessed June 25, 2020].
- (8) Synopsys.com, "Synopsis Defensics", Synopsys.com. [Online]. Available: <https://www.synopsys.com/software-integrity/security-testing/fuzz-testing.html>. [Accessed May 12, 2020].
- (9) OWASP, "Top 10 Web Application Security Risks", OWASP.org. [Online]. Available: <https://owasp.org/www-project-top-ten/>. [Accessed June 7, 2020]
- (10) OWASP, "API Security Top 10", OWASP.org. [Online]. Available: <https://owasp.org/www-project-api-security/>. [Accessed June 7, 2020].
- (11) Netsparker, "Web Application Security Solution", [Online]. Available: <https://www.netsparker.com/>. [Accessed June 25, 2020].
- (12) QARK, "Android mobile app security assessment tool". [Online]. Available: <https://github.com/linkedin/qark/>. [Accessed May 12, 2020].
- (13) MobSF, "MobSF mobile app security scanning framework". [Online]. Available: <https://github.com/MobSF/>. [Accessed: May 12, 2020].



—

**ABB Device Security
Assurance Center**