istec

IoT Security Test and Evaluation Center

We are the Internet of Things Security and Evaluation Center (ISTEC) from Turkey, which was established in 2018 as a state university research center within Istanbul University-Cerrahpaşa.

ISTEC specializes in and focuses on IoT device cyber security, which includes hardware, software, communication, and regulatory compliance testing. Additionally, we are interested in the security of IoT environments (smart vehicles, smart homes, and smart cities), critical infrastructure security, machine learning and artificial intelligence (for cyber security via IDS, IPS, and SIEM), and GDPR compliance of services and products. ISTEC services top Turkish manufacturers of smart home appliances and electronics, including Arçelik, Beko, Grundig, Vestel and Turk Telekom.

We are pleased to inform you that ISTEC performs testing in accordance with ETSI TS 103 645, TRTEST IoT Device Criteria, and a variety of specific on-demand cyber security tests.

ISTEC is a solution partner of TRTEST Test and Evaluation INC, the Turkish Standards Institution, and TUBITAK BILGEM Scientific and Technological Research Council's Informatics and Information Security Research Center.

Here are our web pages and profiles with information about our activities and services.

iste.center

istec@istanbul.edu.tr

linkedin.com/company/istecenter/

twitter.com/istecenter

instagram.com/istecenter/

Our Successes

- We are supported by Istanbul Development Agency (ISTKA) of the Republic of Turkey Ministry of Industry and Technology in 2018
- We are currently a solution partner of TRTEST Test and Evaluation INC.
- Arçelik, Grundig, Beko, Vestel, and Turk Telekom, Turkey's leading manufacturers of smart home products and electronics, are included in our portfolio of clients for our services.
- We have discovered numerous vulnerabilities and notified manufacturers during our research.

Our Skills

- Software Security Tests
  - Web Security
  - Mobile Application Security
  - Cloud API Security
  - Reverse Engineering
- Hardware Security Tests
  - Physical Port Scan
  - Serial Bus Sniffing
  - Side Channel Attack
  - Reverse Engineering
  - Component Analyze
- Communication Tests
  - Wired Network Tests (All communication protocols and media)
  - Wireless Network Tests (Wi-Fi, BLE, ZigBee)
- Personal Data Analysis and GDPR Compatibility Tests
- Risk assessment and developing secure protocol for SCADA and Critical Infrastructures

Our Test Procedure

The IoT Testing Procedure of ISTEC is a procedure that is carried out in accordance with the terms of the agreement between the Manufacturer and ISTEC. As a result, it is vital to clarify the process in the methodology for IoT testing. To begin, the protocol and Confidentiality Agreement are created during the agreement procedure. For each product that the manufacturer wishes to have tested, a scope form is created. Following the completion of the Scope Form's Document Compliance Check and agreement, the Security Tests of the Methodology are performed. The manufacturer receives the Consequence Report as a result of the test studies, which comprises the attack scenario, findings, and solution suggestions. Verification Tests are conducted after the manufacturer has examined the Result Report and applied any necessary security upgrades, often giving the product an average of one month. The procedure is concluded with the Verification Report following the testing, particularly the vulnerabilities disclosed in the outcome report. If the device still contains vulnerabilities, the test procedure is repeated.