

Codonomicon DEFENSICS Robustness Tester for Bluetooth 2.x

Bluetooth is often thought to be separate from the security critical systems, but that is a dangerous assumption. Consider, for example, a Smartphone or PDA, Bluetooth enabled cars or medical devices. A practical testing of 31 Bluetooth enabled devices in mid-2006 revealed less than 10% survival rate when subjected to Defensics Bluetooth robustness testing solution. Defensics Bluetooth is a testing solution of choice for the quality and security minded vendors.

Codonomicon Robustness Tester for Bluetooth technology is a black-box testing product with ready-made Bluetooth test cases. The tests verify how well an implementation can withstand invalid and malformed traffic. By using the test tool, you can easily hunt down defects that are otherwise hard to find. The tests result in improved product stability and security, which protects your end-users and corporate brand. Codonomicon Robustness Tester for Bluetooth technology consists of a set of separate test suites, each which tests a particular Bluetooth protocol layer or profile. All relevant protocols and profiles are covered. The tests have been designed in accordance with Bluetooth Core specification 2.0 where applicable, but implementations based on any earlier versions of the specification may still be tested as well. In addition all relevant Bluetooth profile specifications are covered.

Test tool general features

- **Fully automated black-box negative testing**
- **Ready-made test cases**
- **Written in Java(tm)**
- **GUI, command line, remote interface modes**
- **Instrumentation (health-check) capability**
- **Support and maintenance**
- **Comprehensive user documentation**
- **Results reporting and analysis**

Supported Protocols: L2CAP, SDP, RFCOMM, OBEX,

Supported Profiles: OPP, FTP, IrMC Synch, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP

DEFENSICS robustness testing has found a number of critical flaws in Bluetooth implementations. Examples include cases where mobile phones have been rendered completely useless as a result of negative tests, with the only remediation being reflashing the device. Anyone could conduct attacks similar to these tests and, in the case of modern smartphones, they could result in a loss of important data.

As Bluetooth finds its way to new application areas like medical devices (with Bluetooth Medical Device Profile, MDP), it is important to harden the implementations against malicious attacks and unintentional bad input. In the following sections, we will give results of real-world testing and insights into the Bluetooth threat evolution. The DEFENSICS Bluetooth robustness tester currently covers all of the major profiles and stack layers, starting from L2CAP to individual profiles, such as HFP and HSP.

Tested Messages/Elements (not complete!)

L2CAP Test Suite (3705 Tests):

Echo Request, Information Request, Connection Request, Disconnect Request, Configure Request, Command Reject

SDP Test Suite (5956 Tests):

Service Search Request, Service Attribute Request, Service Search Attribute Request

RFCOMM Test Suite (6553 Tests):

DLC Connection Request, Parameter Negotiation Request, Connection Request, MSC Response, MSC Command, Data Command

OPP Test Suite (23615 Tests):

Connect, Disconnect, Get Business Card Pull, Put, Put (Multipart), Abort, SetPath,

BNEP Test Suite (12804 Tests):

Ctrl Setup Connection Request, Ctrl Filter Net Type Set, Ctrl Filter Multi Addr Set, Msg General Ethernet, Msg Compressed Ethernet

AVRCP Test Suite (1228 Tests):

Unit Info Command, Subunit Info Command, Passthrough Command (Play and Stop)

A2DP Test Suite (3966 Tests):

Discover, Get Capabilities, Set Configuration, Get Configuration, Reconfigure, Open, Start, Close, Suspend, Abort, Security Control, A2DP Media Packets

HFP AG Test Suite (3528 Tests):

Indicator Control Read and Test (AT+CIND), Mobile Termination Event Reporting (AT+CMER), Call Related Supplementary Services (AT+CHLD), Bluetooth Retrieve Supported Features (AT+BRSF), Bluetooth Voice Recognition (AT+BVRA), Bluetooth Noise Reduction + Echo Cancelling (AT+NREC), Volume Gain of Speaker (AT+VGS), Volume Gain of Microphone (AT+VGM)

HFP Unit Test Suite (1031 Tests):

Bluetooth Supported Features Response (+BRSF), Indicator Control Read Messages (+CIND), Volume Gain of Speaker (AT+VGS), Volume Gain of Microphone (AT+VGM)

HSP AG Test Suite (1334 Tests):

Keypad Control (AT+CKPD), Volume Gain of Speaker (AT+VGS), Volume Gain of Speaker (AT+VGS), Modem Reset (ATZ)

HSP Unit Test Suite (617 Tests):

Ring, Volume Gain of Speaker (AT+VGS), Volume Gain of Microphone (AT+VGM)

FTP Unit Test Suite (31528 Tests):

Connect, Disconnect, Put File, Put File (Multipart), Abort, Get File, Delete File, Create Folder, Set Folder, Delete Folder

IrMC-Sync Unit Test Suite (15702 Tests):

Connect, Disconnect, Put VCard (level 1), Get Phonebook (level 2), Get VCard (level 3)

PBAP Test Suite (15701 Tests):

Connect, Disconnect, Pull Phonebook (SIM0), Pull Phonebook (SIM1), Pull VCard, Set Path

SAP Test Suite (1816 Tests):

Connect Request, Disconnect Request, Transfer ATR Request, Transfer APDU Request (Select),

DUN Test Suite (9674 Tests):

Select Bearer Service Type (AT+CBST), Define PDP Context (AT+CGDCONT), Dial Command (ATD), Hang-Up Command (ATH/+CHUP), Echo Command (ATE), Request Manufacturer Identification (AT+CGMI), Request Model Identification (AT+CGMM), Request Revision Identification (AT+CGMR), Request Product Serial Number ID (AT+CGSN), Call Mode (AT+CMOD), Cellular Result Codes (AT+CRC), DTMF And Tone Generation (AT+VTS), HSCSD Device Parameters (AT+CHSD), HSCSD Current Call Parameters (AT+CHSC), Network Registration (AT+CREG), Operator Selection (AT+COPS), Calling Line ID (AT+CLIP), Calling Line ID Restriction (AT+CLIR), Call Waiting (AT+CCWA), Supplementary Service Notification (AT+CCSN), Advice Of Charge (AT+CAOC), Phone Activity Status (AT+CPAS), Read Message (AT+CMGR), Select Service for MO SMS Messages (AT+CGSMS), Phonebook Read (AT+CPBR), Phonebook Write (AT+CPBW)

Tested Messages/Elements, Main Tests Groups, Tests Cases, Tests

Each Protocol/Profile has several **Main Test Groups**. Each main Test Group includes several **Test Cases**. Each Tests Case includes several **Tests**.

The example below is from **PBAP**.

7 Main Test Groups

Example: PBAP Pull Phonebook SIM1

PBAP Pull Phonebook SIM1 has over 125 Test Cases.**Examples are (with number of supported Tests):**

PBAP-Pull-Phonebook-SIM1-Payload-underflow	69 Tests
PBAP-Pull-Phonebook-SIM1-Payload-overflow	10 Tests
PBAP-Pull-Phonebook-SIM1-Payload-repeat	10 Tests
PBAP-Pull-Phonebook-SIM1-Hi-Generic-OneByte-multiple	20 Tests
PBAP-Pull-Phonebook-SIM1-Hi-Generic-FourByte-multiple	20 Tests
PBAP-Pull-Phonebook-SIM1-Hi-Generic-ByteSequence-multiple	20 Tests
PBAP-Pull-Phonebook-SIM1-Hi-Generic-UTF16-multiple	20 Tests

Results of all tests are shown in a summary screen in which the numbers of errors during a given Test Case are shown.

© Codenomicon, 2009

ARS Software GmbH
Starnberger Str. 22
D-82131 GAUTING/Munich
Tel. +49-89-8934130
info@ars2000.com
www.ars2000.com