FORTRA

DATASHEET *(Beyond Security)*

beSTORM

beSTORM is an intelligent black box fuzzer that ensures the security of products before they are released or deployed. It is built to meet the priorities of efficiency, flexibility, and breadth common to testing teams across the corporate landscape. beSTORM uses a proprietary prioritization algorithm to automatically start attacking the highest probability vulnerabilities first, before methodically expanding into billions of attacks across the chosen protocols. These protocols can be known, augmented, proprietary, or unknown.

beSTORM achieves this testing through almost no user interaction. It can be set up outside of the system being tested and can be scaled to use multiple processors or multiple machines to substantially reduce testing duration. It will automatically log anomalies and vulnerabilities and continues testing, eventually producing actionable reports that can be disseminated across teams and acted upon.

A Dynamic Testing Solution

Language Agnostic - beSTORM runs billions of attacks by testing the binary application and as such is completely indifferent of the programming language or system libraries used.

Scalable - beSTORM tests the entire communication range. This allows it to scale effortlessly with products with large complicated code bases.

Flexible - The lack of source code interaction also allows for exportation and use of beSTORM tests to teams that do not have access to the source code.

Fighting tomorrow's war not yesterday's battle.
Static code tools run perhaps thousands or at best tens of thousands of tests based on a certain set of case studies or scenarios of known vulnerabilities. This is equivalent to bolstering the product against known past attacks. beSTORM however, performs millions and potentially billions of attack combinations across the entire communication range. This tests the product against not only known past attacks but unknown future ones that may be launched against it.

> ***"Beyond Security has built a lot of automation into its technology, but not at the expense of accuracy. At the end of the day, you're able to eradicate all vulnerabilities and stop things like backdoors and intruders from getting on the network."***
>
> **–Brandon Buhai,**
> COO at Beyond IP, a Chicago-based solution provider

Comprehensive and Flexible Testing

beSTORM is capable of testing both already known protocols and quickly learning and testing augmented, proprietary, or new protocols.

Comprehensive

beSTORM performs across all communication standards (even complex standards, such as SIP), and levels, including network, protocol, file, hardware, DLL and API. beSTORM delivers an exhaustive search of all possible input combinations to test input implementation for weaknesses. During these tests it operates with a powerful monitor that detects and informs future attacks when even the slightest buffer overflow, format string or memory exception occurs even if these anomalies do not crash the system.

Flexible

beSTORM supports the analysis of proprietary or augmented protocols. If beSTORM encounters a proprietary or augmented protocol, beSTORM's Auto-Learn will log this and begin building and expanding tests into this protocol. These input types may be network traffic that beSTORM captured, a file sample that contains the network traffic captured using other means or a syntax describing an API. beSTORM uses these data sets to determine how the protocol or file is built. If the complete specification is available, users can also create or extend beSTORM modules using an XML editor.

beSTORM is also able to convert protocol standard text into an automated set of tests by converting the BNF description used in technical RFC documents into attack language. This allows beSTORM to be immediately updated and run on any new communication standards that are released by simply uploading a RFC document or the equivalent.

"We are very impressed with the beSTORM product. One notable feature is its flexibility in adding new and proprietary protocols. We are actively expanding the usage of beSTORM in our overall product portfolio as part of the standard security testing procedure."

–Avishai Avivi,
Sr. Director DPI Technologies Group,
Juniper Networks

Actionable Reports

beSTORM is created with the end goal of remediation in mind. As such, beSTORM provides clean actionable reports which intricately detail encountered vulnerabilities that ended in a successful attack. Since beSTORM is behaviorally attacking the test product instead of testing against case studies, virtually all false positives are eliminated leaving the user with comprehensive and clean reports.

Found vulnerabilities can then be exported in a detailed vulnerability report that can be used to debug the application. Developers can load these vulnerability reports within their chosen development environment with zero knowledge of how to use beSTORM and immediately begin the debug process.

System Requirements

Recommended

- Quad-core processor (i5+ or equivalent)
- 8GB of RAM (Windows 10)
- 1GB available HDD space

beSTORM was designed to run on low power systems as well with the following

Bare minimum requirements

- x86-64 CPU
- 1GB of RAM (Linux, Docker, Embedded application)
- 250MB of HDD space

Protocols

New Modules: IoT WebAP • IoT AutoLearn • IoT Mesh Networks • OpenAPI AutoLearn

Basic IPv4:
ARPv4 • ICMPv4 • IPv4 • TCPv4 • UDPv4

Basic IPv6:
ICMPv6 • IPv6 • TCPv6 • UDPv6

Basic Network Clients: DHCP • DNS • FTP • HTTP • HTTPS • HTTPS v1 1 (SSL/TLS Web Client) • NTP-PMP • NTP • SMTP • SSH

Basic Network Servers: DHCP Server (Simple) • DNS Server (Simple) • FTP Server • HTTP Server (Simple Web Server) • HTTPS Server (Simple Web Server) • SMTP Server (Simple) • SSLServer (Simple)

Bluetooth: A2DP • AMP (Alternative MAC/PHY) • ATT • FTP • GAP • GATT • HFP • HOBT • HOGP • iBeacon Profile • L2CAP • MCAP • OBEX • RFCOMM • RSC • SDP

CANbus/Automotive: SAE J1939 • OBDII- • CAN-bus

EDSA: EDSA 401 Ethernet • EDSA 402 ARPv4 • EDSA 403 IPv4 • EDSA 404 ICMPv4 • EDSA 405 UDPv4 • EDSA 406 TCPv4 • EDSA v2-401 Ethernet • EDSA v2-402 ARPv4 • EDSA v2-403 IPv4 • EDSA v2-404 ICMPv4 • EDSA v2-405 UDPv4 • EDSA v2-406 TCPv4

Files: ANI • AVI H264 AC3 • AVI Xv d Codec • BMP • DOC • GIF • HTML • ICO • JASC PAL • JPEG • MKV • MP3 • MP4 • PAL • PDF • PNG • PPT • TGA • TIFF • UPX • WAV(PCM) • XLS

Hardware: Fastboot • HDCP v1.1 • HDCP v2.0 • HDM v1.3 • URB • USB Mass Storage • USB Request Block • ZigBee

Metro Ethernet: BFD • Ethernet Protocol • LLDP • LLDP (Simple)

Network: AMQP • BGP • BVLC • CDP • CGMP • DHCP • Diameter • DNS • Ethernet Protocol • FTP • HSRP • HSRP v2 • HTTP v1.0/1.1 • HTTPS v1.0/1.1 (SSL/TLS Web Client) • CAP • CMPv6 ND • MAP • K ES • LDAP • LDP • L SP • LLMNR • NAT-PMP • NFS Client • NNTP • NTP • NTP-PMP • POP3 • Radius • RANAP • RMI Client • RSH • SDP • SMB Client • SOAP over HTTP • SSH • Syslog • TAPA • Telnet • TFTP • UDPLite • Web Application Protocol

Mobile: GTP v1 (GTP-U) • M3UA

SCADA: CIP Ethernet/IP • DNP3 Master • DNP3 Master Serial • DNP3 Master Serial (Simple) • DNP3 Slave • DNP3 Slave Serial • DNP3 Slave Serial (Simple) • EtherCAT • EtherCAT over UDP • Ethernet/ P • IEC 61850 GOOSE • IEC 60870-5-101 Master • IEC 60870-5-101 Slave • IEC 60870-5-104 Master • IEC 60870-5-104 Slave • IEC 61850 MMS Master • IEC 61850 MMS Slave • Modbus Master Simple Protocol • Modbus Master Serial (Simple) Protocol • Modbus Master Serial Protocol • Modbus Master Protocol • Modbus Slave Ser al Protocol • Modbus Slave Protocol • Modbus ASCII Master Serial • Modbus RTU Serial • PROFINET PTCP • PROFINET RT

Simple Network Clients: HTTP (Simple Web Cl ent) • SNMP v1 Simple • SNMP v2 Simple • SNMP v3 Simple • SNMP v3 Simple with MD5 • SNMP v3 Simple w th MD5 and DES • SNMP v3 Simple with SHA • IPP (Simple)

Routing: DVMRP • IGMP v1/v0 • IGMP v2 • IGMP v3 • OpenFlow • OpenFlow • OSPF v1 • PIM v2 •RIPng • VRRP

TLS: TLS v1 2 Client

Tunneling: LLC • PPPoE • RGMP • SCTP • Teredo Protocol • TPKT (RFC 1006)

VOIP: ISUP (SIP- , SIP-T) • MGCP (Megaco, H 248) • MEGACO (over M3UA) • RTP • SLP svrloc • SIP • SIP Register • STUN

VPN: IPsec AH • ISAKMP • L2TP

WIFI: IEEE 802 11 AP Simple • IEEE 802 11 AP • IEEE 802 11 Subscriber • IEEE 802 11u • IEEE 802 1Q

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.