Spirent **Avalanche NEXT**™

Advanced Fuzzing

Applications and Security Test Solutions

Background

Accidentally discovered in the 1980's by Barton Miller, a Professor of Computer Sciences at the University of Wisconsin, Madison, fuzzing has grown in popularity for a variety of reasons. For starters, it's easier and often more effective in generating and running arbitrary inputs than it is to perform manual code audits, or using software for reverse engineering. With the ability to find most serious faults, fuzzing is most effective when used in conjunction with extensive black box testing, with no access to source code. It can be left up and running for days, to reveal bugs missed in manual audits, while providing an overview of the target software's robustness.

Spirent provides a holistic approach to fuzzing with the ability to offer endpoint and pass thru fuzzing capabilities with fuzzing only or for more robust testing fuzzing under high load of emulated l4-7 application and attack traffic.

Fuzz testing or fuzzing delivers invalid, unexpected, or random data to the inputs of a computer program, OS, or hardware system while monitoring for application or program crashes. It's a relatively easy and more effective tool in generating and running arbitrary inputs than it is to perform manual code audits, or using software for reverse engineering. Uncover previously undetected bugs and compromises in your system, while hardening your program against random data. Going deeper than scans or "dumb" protocol testing, use fuzzing to discover vulnerabilities the same way hackers do.

With the ability to find serious faults, fuzzing is most effective when used in conjunction with extensive black box testing, with no access to source code. It can be left up and running for days, to reveal bugs missed in manual audits, while providing an overview of the target software's robustness.

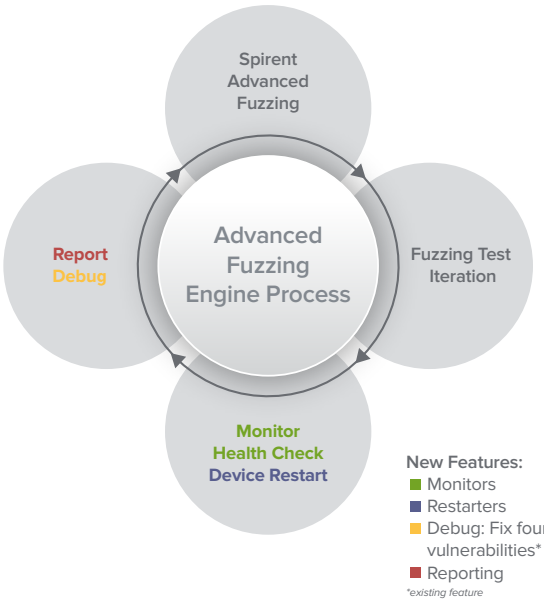
Pros and cons of fuzzing alone

Spirent's Fuzzing solution brings a level of flexible intelligence with a variety of new features to create custom test cases to find and fix threats. By using mutation-based fuzzing you are assured of almost an unlimited number of test inputs to test the resiliency of the target with extreme accuracy of results. Fuzzing by itself — with no other traffic targeting the device under test (DUT), is a valid means to find unknown vulnerabilities. However, when a DUT is under stress and managing other traffic, testing results can be very different.

As a hyper-realistic L4 - L7 traffic generator, Avalanche NEXT can do standalone fuzz testing of targets to pinpoint faults. For further stressing of devices Advanced Fuzzing offers testing while under extreme load of legitimate or malicious attack traffic, which can further expose vulnerabilities that might go undetected.

Advanced Fuzzing engine

Spirent offers a scalable framework-based solution with enhanced mutation-based test cases to provide maximum test coverage to support customer-imported protocols, with the ability to scale from 1 to 30 concurrent fuzzing tests (depending on hardware configuration.) Mutation-based fuzzing seed values are used to easily alter the negative inputs used in the test, and to allow for the same mutation to be used in ongoing or future tests.



Spirent **Avalanche NEXT**™

Advanced Fuzzing

Spirent services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements.

For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

Reporting

Avalanche NEXT Advanced Fuzzing quickly and easily shows you when a fault is found. Spirent reporting will showcase hard faults that are reproducible in additional to warning faults that happen once but are not reproduced so you can further debug a potential vulnerability or threat with the devices or system under test.

New features

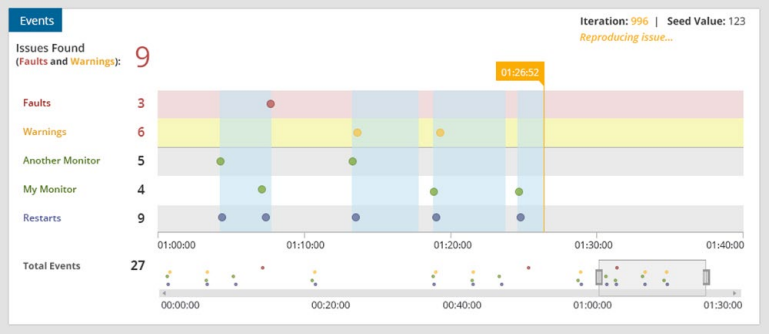
Monitors

Confirm the service being tested is still operational, so you can design and configure multiple ways to measure service activity while the fuzz testing is active. Examples of monitors include:

- Syslog
- SNMP
- Remote Log
- Remote Command
- HTTP
- Ping
- File Downloader

Restarters

If a failure occurs you must be able to restart the target so testing can re-commence. Avalanche NEXT Advanced Fuzzing provides a number of means to achieve this: connecting the target to a network-attached external power source, and a restart device-under-test (DUT) after a non-recoverable fault. Our Advanced Fuzzing solution will support third-party PDUs with open SNMP support. You can connect to the DUT and restart a service-via-management-interface, or via a REST API call using HTTP. Additionally, SSH or Telnet can be used to also restart the DUT for maximum flexibility.



Protocol library

Up-to-date protocol library, powered by Spirent TestCloud™ delivers a subscription-based solution for the latest protocols to the fuzzing library as they are made available. Protocols are available individually or in a growing and diverse set of protocol packs including:

IPv4 - IPv6 - Network Discovery - Web Services - SCADA - Authentication - Network Services - Network Configuration - Switching - Routing - Link Layer - Media - Storage - Encryption - Mail Services - Mobility - and more!

As a subscription service, you are assured of the latest features within any protocol. Subscribe to easily download from Spirent TestCloud Test Content Service.

For more information on supported protocols, protocols packs and other licensing options, please contact your Spirent sales representative.

spirent.com

AMERICAS 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539 | salesasia@spirent.com

Rev. A | 02/16