cyberflood

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's CyberFlood provides a holistic approach to fuzzing with the ability to offer endpoint and true pass-through 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.

With the ability to find serious faults, CyberFlood 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. And with the industry's first server-response fuzzing capability you can now test one of the most common attack vectors utilized by hackers today.

Fuzzing Under Realistic Load

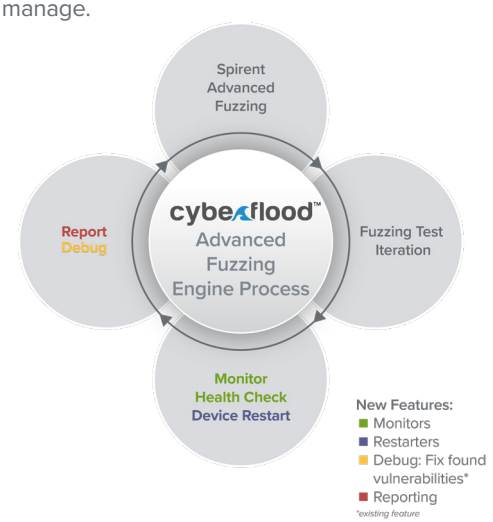
Spirent's CyberFlood fuzzing solution brings a level of flexible intelligence with a variety of new features to create custom test cases to find and fix threats. With SmartMutation™-based fuzzing you are assured of an almost unlimited number of test inputs to test the resiliency of the target with extreme 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, CyberFlood 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.

When testing through a device under test there is no need to setup real target service, CyberFlood provides true pass-through testing for any protocols making end-to-end fuzzing possible with little effort and equipment to setup and manage.

Advanced Fuzzing Engine

Spirent offers a scalable framework-based solution with SmartMutation providing virtually unlimited number of test cases to be executed, with the ability to scale from 1 to 30 concurrent fuzzing tests (depending on hardware configuration.) SmartMutation fuzzing seed values are used to easily alter the negative inputs used in the test, and to allow for the same test iteration to be used in ongoing or future tests providing complete repeatability.



cyberflood

Advanced Fuzzing

SPIRENT

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

CyberFlood 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 fuzzing test is active. Examples of monitors include: Syslog, SNMP, Remote Log, Remote Commander, HTTP and more.

True-Passthough Fuzz Testing

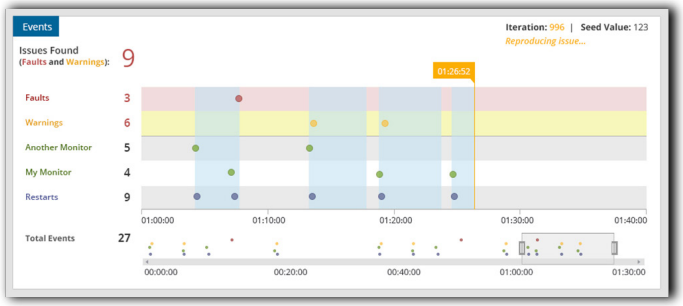
Setup compressive fuzzing test quickly and easily between physical or virtual CyberFlood test ports. There is no need to setup real target services to stress in-line devices saving time and cost.

Server Response Fuzzing

Not available in other solutions CyberFLood Fuzzing allows users to fuzz the server definition of the network protocol when testing a device confirming it can handle malformed responses across one of the most common attack vectors leveraged by hackers today. This provides a fast, easy way to test security devices with no false positives during testing.

Restarters

If a failure occurs you must be able to restart the target so testing can re-commence. CyberFlood Advanced Fuzzing provides a number of means to achieve this: virtually restarting via OpenStack and ESXi, 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, Remote API, SSH or Telnet can be used to also restart the DUT for maximum flexibility.



Real-time instantaneous fuzzing results.

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!

Spirent is a market leader in fuzzing TLS v1.3, QUIC and also competitively tests for HTTP/2 and MQTT.

As a subscription service, you are assured of the latest features within any protocol easily downloaded 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 Follow us @SpirentSecurity

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

US Government & Defense
info@spirentfederal.com | spirentfederal.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 D | 07/18