

MSF Introduces Robustness Testing at LTE IOT event

OULU, FINLAND and CUPERTINO, CA — MARCH 2, 2010 — At the upcoming LTE IOT interoperability event, MSF will introduce robustness testing. MSF is the first industry forum to include security testing in its program. The MSF LTE IOT event will take place March 15-26.

Robustness is introduced at the interoperability event to raise awareness of the need to test products proactively before the release and during development. MSF has a long tradition of organizing successful interoperability events. The goal of security testing is to increase awareness on security issues and to provide participating companies with information on potential security vulnerabilities.

The main strength of Robustness testing is its ability to find unknown vulnerabilities, in addition to known bugs. Most security solutions today only look for known vulnerabilities. While it is important to remove known bugs, unknown bugs pose a greater security threat, because there are no available patches for them. Once an attack is discovered, it takes time to locate the bug and to prepare a fix for it; meanwhile, the malicious users are free to continue their attacks.

Robustness testing, or Fuzzing, is an effective method for testing software robustness, because it targets the same security problems that attackers would look for. Fuzzing is basically doing what the attackers would do, but before the product is released and in a secure environment. In robustness testing, large numbers of protocol messages, (tens or hundreds of thousands) containing exceptional elements, are used to simulate malicious attacks. Fuzzing is a quick, proactive and easy way of assessing software security.

Codonomicon Defensics is the market's leading proactive fuzzing tool. The state-of-the-art protocol modeling and test generation technique ensures market leading test coverage and test efficiency. Defensics provides better test results by uncovering more security issues in less time. Protocol sequence and test case editing permits you to customize test cases and scenarios. General purpose tools such as Traffic Capture Fuzzer and Defensics for XML enable users to test any type of proprietary protocol as well as SOAP/XML applications. Defensics products are easy to integrate into existing tool libraries provided by third parties. Moreover, the comprehensive reporting capabilities and flexible licensing models enable reporting and reproduction capabilities across the entire software development organization.

To read more about robustness testing and fuzzing LTE networks, see Codonomicon whitepaper at: <http://www.codonomicon.com/products/lte/>

About Codonomicon Ltd:

Codonomicon develops security and quality testing software, which allows users to quickly find and identify both known and previously unknown flaws before business-critical products or services are deployed. Their unique, targeted approach to the fuzz testing of networked and mobile applications exposes more flaws and weaknesses than any other testing platform or methodology. Companies rely on Codonomicon's solutions to mitigate threats, like Denial of Service (DoS) situations and Zero Day Attacks, which could increase liability, damage business reputation and cripple sales. Codonomicon is a member of the SDL Pro Network. For more information, visit www.codonomicon.com.

About the MSF:

The [MultiService](#) Forum (MSF) is a global association of service providers, system suppliers and test equipment vendors committed to developing and promoting open-architecture, multiservice Next Generation Networks. Founded in 1998, the MSF is an open-membership organization comprised of the world's leading telecommunications companies. The MSF's activities include developing Implementation Agreements, promoting worldwide compatibility and interoperability of network elements, and encouraging input to appropriate national and international standards bodies. For more information, visit <http://www.msforum.org/>.