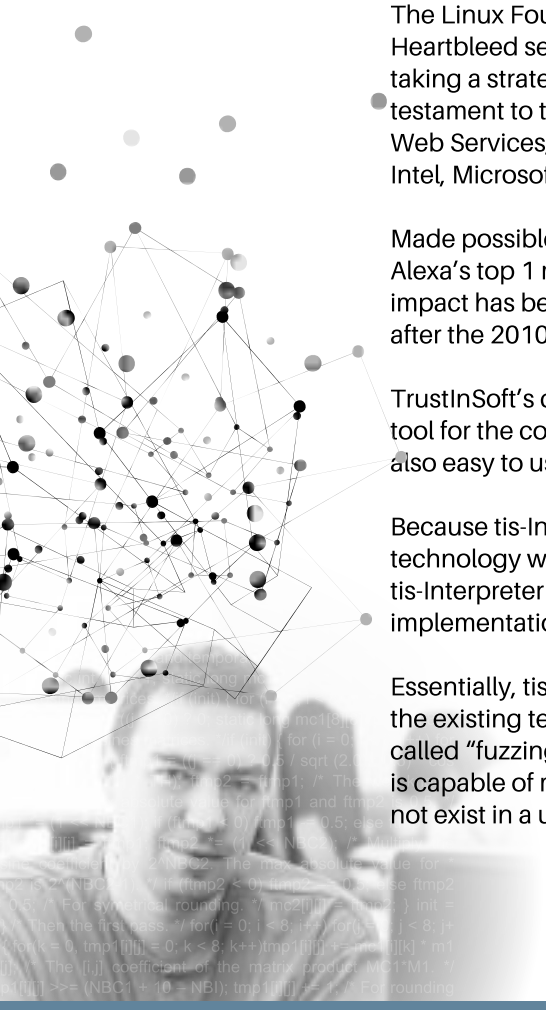
TRUST IN SOFT

TrustInSoft Selected by Linux Foundation's Core Infrastructure Initiative to Help Improve Cybersecurity

CALIFORNIA, San Francisco – August 17, 2015 –The stakes have never been higher for the open-source software community and the millions of people across the world who rely on a wide variety of software, such as OpenSSL, where security is critical. That's why the Linux Foundation's Core Infrastructure Initiative has selected TrustInSoft to leverage its groundbreaking technology to help provide the open source community with an easy-to-use tool that is also effective at finding bugs in open-source critical code that other technologies miss.

"We're excited to be a part of this revolutionary collaboration," shares Pascal Cuoq, Chief Scientist and Co-Founder of TrustInSoft. "Our inclusion in this initiative represents an important confirmation of the value that our unique technology brings to the open-source community as well as software designers and integrators across a wide range of business and government sectors. We've already begun to develop and test our tis-Interpreter tool, and we believe that the open-source community will be as excited as we are about the results."

The Linux Foundation formed the multi-million dollar Core Infrastructure Initiative in response to the Heartbleed security crisis. Collaborating with experts from multiple fields, the Linux Foundation is taking a strategic approach to strengthening the software critical to the security of the Internet. A testament to the significance of the project, the Core Infrastructure Initiative is supported by Amazon Web Services, Adobe, Bloomberg, Cisco, Dell, Facebook, Fujitsu, Google, Hitachi, HP, Huawei, IBM, Intel, Microsoft, NetApp, NEC, Qualcomm, RackSpace, salesforce.com, and VMware.



Made possible by a vulnerability in a single line of code, Heartbleed compromised as many as 55% of Alexa's top 1 million websites and one-sixth of all SSL-certified websites. The total cost of Heartbleed's impact has been estimated at half a billion dollars, the same amount spent by the Red Cross in Haiti after the 2010 earthquake.

TrustInSoft's contribution to the Core Infrastructure Initiative is to demonstrate that the tis-Interpreter tool for the company's TrusInSoft Analyzer will not only find flaws that other technologies miss, but is also easy to use by software developers.

Because tis-Interpreter will be capable of detecting vulnerabilities with no false positives, this new technology will help developers save time identifying potential bugs while also improving security. The tis-Interpreter tool has already been used with great success on s2n, Amazon's new open-source TLS implementation

Essentially, tis-Interpreter is a specialized version of TrustInSoft's TIS Analyzer that takes advantage of the existing tests that developers write by hand and that security auditors generate by a technique called "fuzzing." The commercially available TIS Analyzer remains the only technology in the world that is capable of mathematically demonstrating that the common vulnerability of a buffer overflow does not exist in a use of SSL/TLS implemented in HTTP.

TrustInSoft
http://trust-in-soft.com

Media Contact
Fabrice Derepas
CEO TrustInSoft
fabrice.derepas@trust-in-soft.com

TRUST IN SOFT

TrustInSoft Selected by Linux Foundation's Core Infrastructure Initiative to Help Improve Cybersecurity

"Since our company's founding in 2013, one of our goals has been to establish ourselves as a game changer in the cybersecurity world," explains Cuoq. "We're changing the way software security works in banking, telecom, transportation, energy, defense, aeronautics, and IT by providing tools and services that are able to mathematically guarantee that software is immune to entire families of known flaws."

TrustInSoft was recently named as one of 10 finalists for the RSA® Conference Innovation Sandbox Contest 2015 which recognizes and promotes new approaches to information security technology. TrustInSoft was also recognized by the National Institute of Standards and Technology (NIST) as the only company to use Frama-C to succeed in satisfying the Ockham criteria for all five of NIST's classes of weaknesses.

By design, TrustInSoft is just one part of a growing team of companies and experts working to solve the security problem. Other projects in the Linux Foundation's Core Infrastructure Initiative include:

• GnuPG – GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories.
• Network Time Protocol Daemon – The Network Time Protocol daemon (ntpd) is an operating system program that maintains the system time in synchronization with time servers using the Network Time Protocol (NTP).
• OpenSSH – OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Unfortunately, OpenSSH has been plagued by numerous vulnerabilities over the past years, and it's important to ensure that a flaw as critical as Heartbleed will not emerge.
• OpenSSL Audit – The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library. The Core Infrastructure Initiative is funding a complete audit of OpenSSL.
• Debian Reproducible Builds – Debian developers Holger Levsen and Jérémy Bobbio are steering a large-scale effort to eliminate unneeded variations from the build processes of thousands of free software projects, as well as provide tools to understand the source of these differences and update the infrastructure to allow developers to independently verify the authenticity of binary distributions such as Fedora, Ubuntu, and OpenWrt.
• The Fuzzing Project – Spearheaded by security researcher Hanno Böck, this project uses zzuf, Address Sanitizer, and American fuzzy lop to find bugs in open source projects. Many well-known vulnerabilities, including several GnuPG and OpenSSL bugs reported earlier this year, were found by Böck's efforts.

To learn more about TrustInSoft's technology, or to arrange a proof of concept demonstration for your organization, visit www.Trust-in-Soft.com.

About TrustInSoft

TrustInSoft develops solutions that validate mission-critical software and eliminate attack vectors reduce thereby reducing cyber risks, lowering the cost of designing safety-critical systems, and reducing liabilities. Founded in 2013, the Paris-based company produces TrustInSoft Analyzer, an advanced static source code analyzer, based on the open source Frama-C platform. TrustInSoft Analyzer enables software developers and integrators to exhaustively detect the most frequent and dangerous families of threats before deployment. TrustInSoft also offers professional services and expertise to formally audit safety and security-critical existing software components. For more information visit www.Trust-in-Soft.com.

Media Contact
Fabrice Derepas
CEO TrustInSoft
fabrice.derepas@trust-in-soft.com