PRESS RELEASE

TrustInSoft Mathematically Guarantees Zero-Bug Mobile Applications with New Application Security Test

Bye, bye Pegasus: the new offer allows mobile app developers to prove the absence of vulnerabilities in C and C++ code, libraries, and APIs

San Francisco and Paris, September 15th, 2021 – Cybersecurity software company TrustInSoft today announced a new offer for mobile app developers to prove the immunity of their code to cyber threats, in the wake of recent events involving Pegasus software. This latest application security test (AST) leverages TrustInSoft Analyzer, an exhaustive code analyzer powered by the latest advancements in formal methods, to prove the absence of bugs in APIs and libraries often used in complex mobile application backends.

TrustInSoft's AST comes at a time when mobile application security is being called into question, with the resurgence of spyware software Pegasus and its alleged hacks. Such attacks typically exploit a vulnerability in a program's source code, which often serves as the entry point for remote code execution, permitting the attacker to gain full control of a program. This was the case in 2018 when WhatsApp was hacked using a source code vulnerability called buffer overflow, which could have been prevented with thorough source code analysis. TrustInSoft's latest AST provides assurance to developers that the APIs and libraries used in their application are vulnerability-free and immune from similar zero-day exploits.

The new AST relies on formal methods: mathematical approaches that allow developers to prove the immunity of their source code to cyberattacks that exploit code vulnerabilities. TrustInSoft's solution offers an accessible, easy-to-use technology whose exhaustive approach detects 100% of undefined behaviors and reduces code verification time by 4x.

Fabrice Derepas, TrustInSoft's CEO, stated, "The mobile applications we use every day are as vulnerable to subtle and dangerous cyberattacks as any software. Formal methods can help harden the source code of APIs and libraries used in these applications to avoid vulnerabilities like those found in WhatsApp, before they can become exploitable."

For more information: https://trust-in-soft.com/blog/2021/08/05/how-to-protect-your-code-from-pegasus-spyware/

About TrustInSoft

TrustInSoft participates in the Application Security Testing market alongside vendors such as Mathworks, Parasoft, Synopsys and Veracode. TrustInSoft Analyzer is a hybrid static and dynamic code analyzer that automates Formal Methods to mathematically guarantee C/C++

code quality, security and safety. TrustInSoft has customers worldwide in the automotive, IoT, telecom, semiconductor, aeronautics and defense industries. The company received awards and recognition from NIST, RSA and Linux Foundation. For more information, visit: https://trust-in-soft.com/

Press Contact

Ashley Zupkus

press@trust-in-soft.com