PRESS RELEASE

TrustInSoft's Exhaustive Static Analysis Proves the Security of Trusted Execution Environments

TrustInSoft today released a new white paper that explains how organizations that rely on Trusted Execution Environments (TEEs) within their devices could benefit from exhaustive static analysis to prove them secure and reliable.

PARIS and SAN FRANCISCO, Nov. 9, 2021 -- TrustInSoft, a cybersecurity software company, today announced the release of a new white paper "How Exhaustive Static Analysis Can Prove the Security of Trusted Execution Environments (TEEs)." This free white paper explains how exhaustive static analysis can drastically improve the performance in ensuring the security and reliability of a TEE versus traditional software testing.

Anyone developing software code within Trusted Execution Environments can benefit from TrustInSoft's free white paper to learn:

- Why a TEE must be perfectly reliable and impervious to attack
- The challenges of properly validating a TEE
- Why traditional software testing will fail to validate your TEE
- Why formal methods are ideal for validating code that needs to be perfect
- How exhaustive static analysis guarantees trust in your TEE and will fit easily in your existing development process
- How exhaustive static analysis will fit easily into your existing development process
- The major benefits of exhaustive static analysis
- What to look for when choosing an exhaustive static analysis solution…

and much more.

All Software Bugs within Trusted Execution Environments Must Be Eliminated

The TEE is a key component in many consumer devices, including smartphones, tablets, set-top boxes, and game consoles. A fortified area within the main processor designed to protect sensitive data and applications, a TEE must be perfectly reliable in execution and totally impervious to unauthorized access.

Every TEE, however, is built from software code—code developed by humans. Unfortunately, when humans develop code, they tend to infest that code with coding errors, commonly referred to as "bugs"— some 70 bugs per 1000 lines of code on average, according to data pipeline management and analytics firm Coralogix.

Bugs cause code to perform in unpredictable ways. They present opportunities for hackers to penetrate. For a TEE to reliably fulfill its function, all bugs within its code must be eliminated.

"Until recently, finding and eliminating bugs from software code has been a cat-and-mouse game. As software size and complexity has increased and cybercrime has risen, this game has become increasingly serious, putting millions of Euros worth of business capital at risk," said Fabrice Derepas, Founder and CEO of TrustInSoft. "TrustInSoft has designed a new technology based on mathematical formal methods that can allow developers to guarantee their Trusted Execution Environment is 100% free of coding errors and functions exactly according to its specification."

How Exhaustive Static Analysis Can Prove the Security of TEEs can be downloaded for free from TrustInSoft's website at https://trust-in-soft.com/how-exhaustive-static-analysis-proves-tee-security/

Plus, don't miss TrustInSoft's webinar on Proving the Security of Low-level Software Components and TEEs, November 16th at 9 am PT. Register here: https://trustinsoft.ac-page.com/semiconductor-webinar

About TrustInSoft

TrustInSoft participates in the Application Security Testing market alongside vendors such as Mathworks, Parasoft, Synopsis and Veracode. The 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 global customers 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