2023-04-14

Created: 2023-04-29 22:44:53

Questions

- Basic Concepts `(230328.TEE.txt)`
  - `[09:47]` How do I check the TEE OS is secure. Are there any secure certificates of TEE OS?`(TEE.0328.md)`
  - `[09:54]` Does OP-TEE mach the certificates? `(TEE.0328.md)`

Q & A

Basic Concepts `(230328.TEE.txt)`

Question: `[09:47]` How do I check the TEE OS is secure. Are there any secure certificates of TEE OS?`(TEE.0328.md)`

Answer:

To ensure that a TEE OS (Trusted Execution Environment Operating System) is secure, you can look for several indicators, including compliance with industry standards, certifications, and independent security evaluations. While there isn't a single "secure certificate" for TEE OSes, there are certifications and evaluation processes that can help you assess the security of a particular TEE OS.

1. Common Criteria (CC) Certification: Common Criteria is an international standard for evaluating the security of IT products, including TEE OSes. A TEE OS that has undergone a Common Criteria evaluation and achieved a certification provides a certain level of assurance regarding its security properties. The certification levels range from EAL1 (lowest) to EAL7 (highest), indicating the depth and rigor of the evaluation. Check for a TEE OS with a relevant Common Criteria certification (e.g., EAL4 or higher) for a higher level of confidence in its security.

2. FIPS 140-2/140-3 Certification: The Federal Information Processing Standards (FIPS) 140-2 and 140-3 are U.S. government standards for cryptographic modules used in IT products, including TEE OSes. A TEE OS with FIPS 140-2 or 140-3 certification has undergone testing and validation to ensure that its cryptographic implementations meet specific security requirements. Although this certification focuses on the cryptographic aspects, it can provide additional assurance regarding the security of a TEE OS.

3. GlobalPlatform Compliance: GlobalPlatform is an industry organization that defines standards and specifications for secure elements and TEEs. A TEE OS that is compliant with GlobalPlatform specifications demonstrates adherence to a set of industry-defined security requirements and best practices.

4. Independent Security Evaluations: In addition to certifications, a TEE OS that has undergone independent security evaluations, audits, or penetration testing by reputable security firms or researchers can provide further assurance regarding its security. Look for published reports or case studies detailing the results of such evaluations.

5. Vendor Reputation: Consider the reputation and track record of the TEE OS vendor when evaluating the security of a TEE OS. A vendor with a history of providing secure solutions and promptly addressing vulnerabilities can be a good indicator of the overall security of their products.

In summary, there isn't a single "secure certificate" for TEE OSes, but a combination of certifications, industry standard compliance, independent security evaluations, and the vendor's reputation can provide a good indication of the security of a particular TEE OS.

Question: `[09:54]` Does OP-TEE mach the certificates? `(TEE.0328.md)`

Answer:

OP-TEE (Open Portable Trusted Execution Environment) is an open-source TEE project that provides a TEE OS and related components, with a focus on portability and compliance with GlobalPlatform specifications. While OP-TEE aims to follow industry standards and best practices, it is essential to differentiate between the OP-TEE project and commercial products based on OP-TEE.

As an open-source project, OP-TEE itself does not directly hold certifications like Common Criteria or FIPS 140-2/140-3. However, OP-TEE-based solutions developed by vendors or integrated into commercial products may undergo such certifications or evaluations.

Commercial TEE products based on OP-TEE may pursue certifications, such as:

1. Common Criteria Certification: Vendors can choose to submit their OP-TEE-based products for Common Criteria evaluation, achieving certification at the appropriate EAL (Evaluation Assurance Level) to demonstrate the security of their solution.
2. FIPS 140-2/140-3 Certification: OP-TEE-based products can also be submitted for FIPS 140-2 or 140-3 certification to validate the security of the cryptographic modules used in the product.
3. GlobalPlatform Compliance: While OP-TEE is designed to be compliant with GlobalPlatform TEE specifications, individual implementations may still need to undergo testing and validation to ensure full compliance with the standards.

It is essential to recognize that the certifications belong to the specific commercial products based on OP-TEE and not to the OP-TEE project itself. When evaluating the security of an OP-TEE-based solution, consider the certifications and evaluations obtained by the specific product or vendor, as well as their overall reputation and track record in the industry.
