

Prompt

Now you are an expert in []. You need to complete a paper report to explain the paper [] using the given template. Your answer should fill the blank in the template. The report should be concise, accurate and clear and not less than 3000 words.

This is the template:

1. The title of this paper is []. That means [].
2. The paper's author are []. And the paper is published in [].
3. This part is the summary of the abstract. [].
4. This part is the summary of the research background. [].
5. This part is the summary of the research status. [].
6. This part is the summary of the research question. [].
7. This part is the summary of the research content. [].
8. This part is the summary of the technical route. [].
9. This part is the summary of the contribution. [].
10. This part is the summary of existing problems. [].

Test

Paper name

Sigstore: Software Signing for Everybody

Q

Now you are an expert in software security. You need to complete a paper report to explain the paper Sigstore: Software Signing for Everybody using the given template. Your answer should fill the blank in the template. The report should be concise, accurate and clear.

This is the template:

1. The title of this paper is []. That means [].
2. The paper's author are []. And the paper is published in [].
3. This part is the summary of the abstract. [].
4. This part is the summary of the research background. [].
5. This part is the summary of the research status. [].
6. This part is the summary of the research question. [].
7. This part is the summary of the research content. [].
8. This part is the summary of the technical route. [].
9. This part is the summary of the contribution. [].
10. This part is the summary of existing problems. [].

A

Hello, this is Bing. I can help you with writing a paper report based on the given template. Here is a possible answer:

1. The title of this paper is [Sigstore: Software Signing for Everybody]. That means [the paper proposes a system that enables developers to easily and securely sign their software artifacts using existing identities and transparency logs].
2. The paper's authors are [Zachary Newman, John Speed Meyers, and Santiago Torres-Arias]. And the paper is published in [Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)]¹.
3. This part is the summary of the abstract. [The paper introduces Sigstore, a system that provides widespread software signing capabilities with minimal adoption barrier for developers. Sigstore leverages three mechanisms: an ACME-like protocol to authenticate developers through OIDC, ephemeral keys to sign artifacts, and transparency logs to enable user verification and accountability].
4. This part is the summary of the research background. [The paper motivates the need for software signing by highlighting the recent and severe software supply chain compromises, such as SolarWinds and Codecov, that affected many users and organizations. The paper also reviews the existing software signing solutions and their limitations, such as key management, identity verification, and usability issues].
5. This part is the summary of the research status. [The paper states that software signing is a promising mitigation for many supply chain attacks, but it has seen limited adoption in open-source and enterprise ecosystems due to the challenges and complexities involved. The paper also identifies the gap between the current state-of-the-art and the desired properties of a software signing system, such as simplicity, security, transparency, and scalability].
6. This part is the summary of the research question. [The paper poses the following research question: How can we design and implement a system that provides software signing for everybody, i.e., a system that is easy to use, secure, transparent, and scalable?]
7. This part is the summary of the research content. [The paper presents the design and implementation of Sigstore, a system that aims to answer the research question. The paper describes the main components and features of Sigstore, such as Cosign, Rekor, Fulcio, and Root, and how they work together to provide software signing capabilities. The paper also evaluates the performance, security, and usability of Sigstore, and discusses its deployment and adoption in the real world].
8. This part is the summary of the technical route. [The paper adopts the following technical route to achieve its goals: First, it uses a protocol similar to ACME to authenticate developers through OIDC, tying signatures to existing and widely-used identities. Second, it enables developers to use ephemeral keys to sign their artifacts, reducing the inconvenience and risk of key management. Finally, it enables user authentication by means of transparency logs, bringing transparency and accountability to software signatures].
9. This part is the summary of the contribution. [The paper claims the following contributions: First, it introduces Sigstore, the first system to provide software signing for everybody, with minimal adoption barrier for developers. Second, it demonstrates the feasibility and effectiveness of Sigstore through extensive evaluation and real-world deployment. Third, it contributes to the open-source community and the software security ecosystem by providing a free and accessible service for software signing].
10. This part is the summary of existing problems. [The paper acknowledges the following existing problems and limitations of Sigstore: First, it relies on the availability and security of the OIDC providers and the transparency logs, which may introduce new attack vectors or single points of failure. Second, it does not address the problem of verifying the integrity of the source code or the build process, which are also important aspects of the software supply chain. Third, it faces the challenge of achieving wide adoption and integration with existing software development and distribution platforms, which may require more incentives and standardization].

Source: Conversation with Bing, 12/14/2023

(1) Sigstore: Software Signing for Everybody - ACM Digital Library.

<https://dl.acm.org/doi/pdf/10.1145/3548606.3560596>.

(2) Sigstore. <https://www.sigstore.dev/>.

(3) IBM boosts software supply chain security with signature

<https://research.ibm.com/blog/integrity-shield-for-kubernetes>.

(4) Sigstore: An open answer to software supply chain trust and

<https://www.redhat.com/en/blog/sigstore-open-answer-software-supply-chain-trust-and-security>.

(5) Sigstore - Open Source Security Foundation. <https://openssf.org/community/sigstore/>.

(6) undefined. <https://doi.org/10.1145/3548606.3560596>.