Zero Knowledge Proof over SGX

Guide: Mr. Assaf Barak

Ido Amitay
atrap11@gmail.com

Dan Blumenberg
Dan.blumen1@gmail.com

Daniella Fertouk
Daniella.fertouk@gmail.com

Project Goal

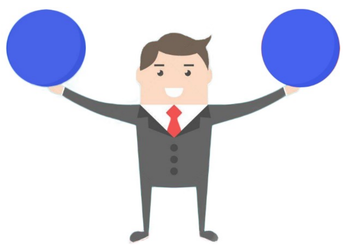
- Learning the Intel SGX Technology.
- In-depth study of the Attestation process – main feature of the SGX architecture.
- Studying the ZKP cryptographic protocol and commitment scheme.
- Writing a program that demonstrates the ZKP protocol over the SGX architecture. The verifier is running inside a secure enclave and the prover is an external application trying to gain the verifier's trust.

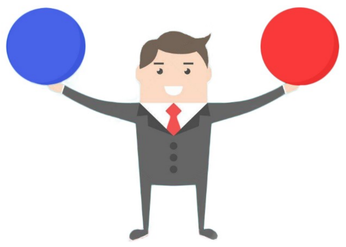
An Initial Goal

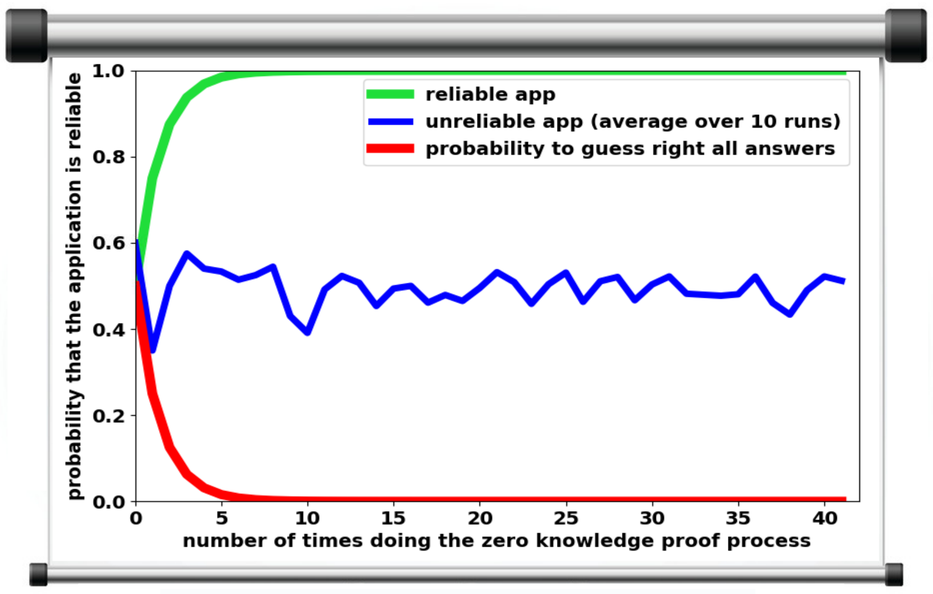
Our initial goal was to attack the SGX architecture by planting a rootkit inside the Linux kernel. Our rootkit was only capable of penetrating older kernel versions. After learning that only newer kernel versions support the SGX drivers we decided to change the aim of the project.

ZKP

- **zero-knowledge protocol** is a method by which one party (the *prover* Peggy) can prove to another party (the *verifier* Victor) that she knows a value *x*, without conveying any information apart from the fact that she knows the value *x*.
- In our project, we create a game that demonstrate the use of zero-knowledge proofs.
- The game:
  - Imagine that you hold two balls in front of a colorblind person, one blue and the other red.
    You want to prove the colorblind person that you can distinguish between those two balls.
    A colorblind person can't tell the difference between "red" and "blue".
  - Let's play a little game:
    let the colorblind person take the balls, put them behind his back and shuffle as much as he likes.
    He then show you the balls and you will determine if he had change their order or not.
  - We'll repeat this experiment 42 times to make it more accurate in terms of probability.
  - The colorblind person understands that it's almost **impossible** to guess the correct answer 42 times in a row (2^{-42}) so he should be convinced that you are indeed able to distinguish between the balls.





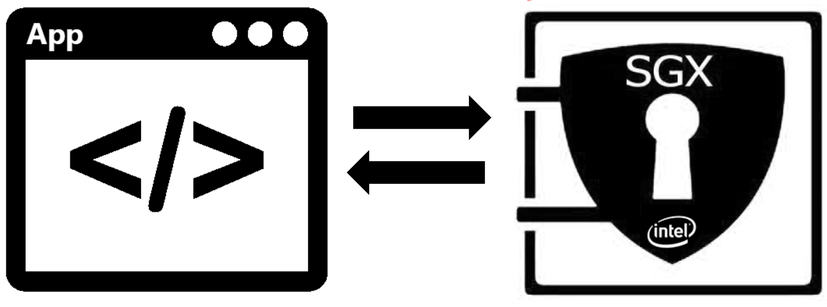


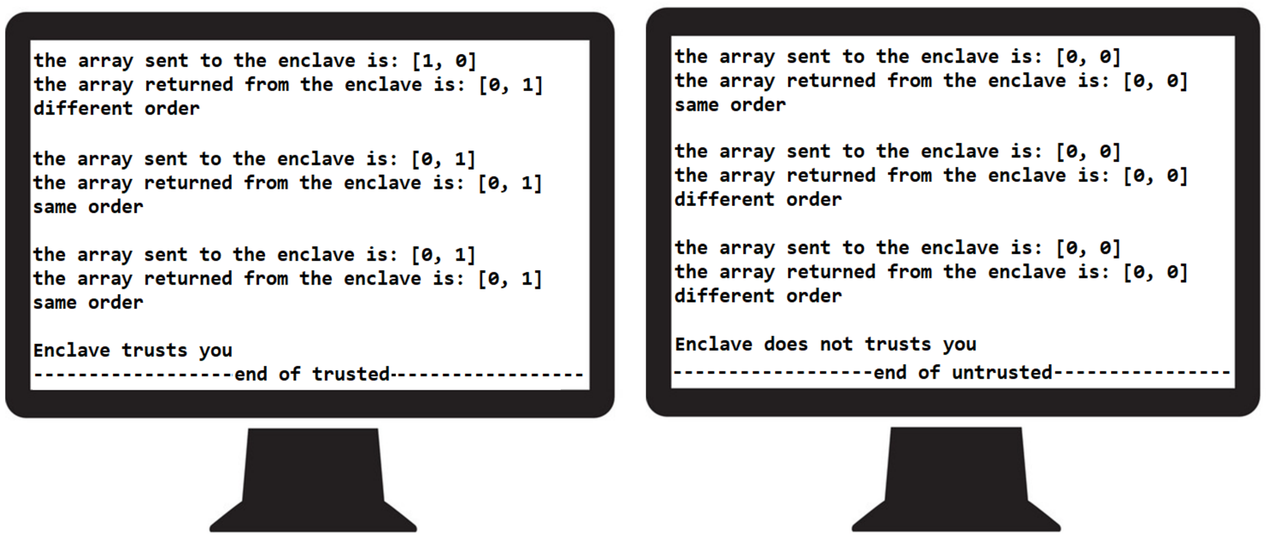
Probability analysis of the reliability of external application depending on the number of experiments and the probability of guessing the right answer

Intel SGX

- Intel SGX protects an application's secrets from malicious software by creating isolated memory regions of code and data called enclaves. These non-addressable memory pages are reserved from the system's physical RAM and then encrypted, allowing the application to access its secrets without fear of exposure.
- In our project, we decided to deeply explore the attestation process of intel SGX technology. The process of local attestation allows a source-enclave to prove to a target enclave running locally on the same platform, that the source-enclave is indeed running on a genuine Intel SGX platform.

System operation





An example of 2 running apps, where one satisfy the ZKP and gain the enclave's trust while the other one does not.