Design And Implementation Of The Ascend Secure Processor

Abstract

- This paper presents hardware implementations of the Ascend secure processor, prototyped on an FPGA and taped out in a 32 nm SOI process.
- Ascend prevents information leakage over a processor's digital I/O pins — in particular, the processor's requests to external memory — and certifies the program's execution by integrity-verifying the external memory.
- In secure processor design, encrypting main memory is not sufficient for security because where and when memory is accessed reveals secret information.

CONT

- To this end, Ascend is equipped with a hardware Oblivious RAM (ORAM) controller, which obfuscates the address bus by reshuffling memory as it is accessed. To our knowledge, Ascend is the first prototyping of ORAM in custom silicon. Ascend has also been carefully engineered to ensure its timing behaviors are independent of user private data

EXISTING SYSTEM

- In this case, a mobile device is constantly monitoring its user's symptoms and wants to compute the like-lihood that the user has some condition given these symptoms.
- To outsource computation, the device sends a cloud server an encryption of fsymptoms, condition of interestg, which will be inputs to a program (call it MedComp()).
- After running MedComp() on the user's private data, the server sends an encryption of the result (e.g., "there is a 55% likelihood that you have the condition") back to the user..

- To maintain privacy, the server must never learn anything about the user's private inputs—the symptoms or diseases of interest—at any time before, during or after the computation completes

Disadvantages

- Users have become more computationally limited and computation outsourcing is becoming more common.
- Data privacy has therefore become a huge concern, as sensitive user data is being revealed to and can be attacked by malicious cloud applications, hypervisors/operating systems, or by insiders

Proposed System

- We give an overview of the Ascend execution model to securely run untrusted programs.
- 2) We provide a comprehensive overview of challenges in implementing a hardware Oblivious RAM (ORAM) controller, the core component in the Ascend design. We present new techniques to address these issues.
- 3) We implement and evaluate all our techniques on aFPGA prototype, and taped out the Ascend processor in 32 nm silicon

Advantages

- This work proves the viability ofa single-chip secure processor which can protect the privacy of software intellectual property or user data, as it interacts with an external memory device.

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

CONCLUSION

- This paper has described the Ascend execution model, for running untrusted programs operating safely on sensitive user data, as well as detailed implementation results for an Ascend prototype chip in silicon. This work proves the viability of a single-chip secure processor which can protect the privacy of software intellectual property or user data, as it interacts with an external memory device. The evaluation results are encouraging. The hardware mechanisms needed to support Ascend, when integrated into the 25 core test chip, are roughly the size of a single processor core.