A Secure Processor Architecture for Encrypted Computation on Untrusted Programs
Technology #18209

Applications

Ascend is a secure processor architecture that guarantees privacy of data in a cloud or cloud-like environment. This technology is highly relevant to cloud computing applications that involve maintaining sensitive information including financial information and medical records.

Problem Addressed

Data privacy is a huge problem in cloud computing applications that require sensitive data to be stored and computed upon in the cloud. Computation requires the data to be exposed to the cloud servers, which may be attacked by malicious applications, hypervisors, operating systems or insiders. Encrypted computation has the potential to solve the data privacy problem. In encrypted computation, the user specifies encrypted inputs to a program, and the server computes on encrypted inputs to produce an encrypted result. This encrypted result is sent back to the user who decrypts it to get the actual result. The Inventors have developed Ascend, a secure processor architecture that supports private computation of arbitrary programs.

Technology

Ascend considers cases where the program is supplied by the server, the user or a third party and can be either public or private (encrypted). The program is not trusted by the user in all cases. In this context to be “trusted,” a program must not be intentionally malicious and must be provably free of any bugs that have the potential to leak information about the program data. Data from the user is always considered private.

Ascend guarantees privacy by employing obfuscated instruction execution; the processor does not disclose what instruction is being run at any given time, be it an arithmetic instruction or a memory instruction. Ascend obfuscates the instructions that it executes to make forward progress in the program, which in turn obfuscates all external input-output (I/O) and power pins. Each pin carries a digital or analog signal at a given time and these signals change over time in program dependent ways. To obfuscate when the value on each pin changes, Ascend performs a program data-independent amount of work to evaluate each instruction. All processor circuits must fire on each instruction fetch to give off the impression that any instruction could have been executed and on/off-chip memories must be accessed only at public time intervals. To obfuscate the bits and memory access
pattern on the I/O pins, external memory requests must be made using oblivious RAM (ORAM) techniques. The adversary learns an estimate of the number of cycles required to complete the computation, which can be shown to be the least amount of leakage possible.

Advantages

- Ascend is only marginally more complex than a conventional processor to implement
- Periodic accesses to external instruction and data memory are performed through an Oblivious RAM (ORAM) interface to prevent leakage through memory access patterns

Categories For This Invention:

Computer Sciences & Information Technology
Cyber Security

Intellectual Property:

Technique for secure computation
Issued US Patent
8,909,967

Inventors:

Srinivas Devadas
Christopher Fletcher
Marten van Dijk

Publications:

A Secure Processor Architecture for Encrypted Computation on Untrusted Programs
Proceedings of the seventh ACM workshop on Scalable trusted computing
October 2012, pp. 3-8