On-chip microprocessor security for defense against malicious hardware attacks

Computing devices have become increasingly susceptible to computer security breaches and cyber attacks. While many security mechanisms focus on combatting software vulnerabilities, there are also significant potential vulnerabilities from the microprocessor hardware that should not be overlooked. Microprocessor hardware attacks are difficult to isolate due to the complexities in component sourcing and design flow. As such, backdoor access to the microprocessor can be gained through malicious hardware design modifications. These modifications are often difficult to detect by standard software. This technology proposes an on-chip solution that is able to sensitively detect insider attacks on microprocessor components. The technology monitors communication between components to discern operations that have been tampered with.

Sensitive detection method leverages component communication to uncover widely undetectable attacks

Computational infrastructure is largely not suited to detect attacks embedded in hardware. This technology is a lightweight on-chip system that sensitively detects embedded backdoors that have been built into the microprocessor design. This technology exploits the division of work within components to ascertain attacks using two programs: TrustNet and DataWatch. TrustNet reports when a microprocessor component processes more or less data than expected, while DataWatch monitors data signatures to protect against manipulations of data that do not affect its length.

A prototype of the technology has been tested with the OpenSPARC T2 microprocessor.

Lead Inventor:
Simha Sethumadhavan, Ph.D.

Applications:
- Detection of design level insider hardware attacks
Detection of non-linear logic paths

**Advantages:**

- Superior detection of hardware attacks
- Robust on-chip performance regardless of data throughput
- The detection methods are themselves resistant to corruption

**Patent Information:**

Patent Pending (US 20130061322)

Patent Pending (WO/2014/137416)

Tech Ventures Reference: IR M10-061

**Related Publications:**


**Inventors**

Lakshminarasimhan Sethumadhavan