Application-Aware Reliability and Security: The Trusted ILLIAC Approach

Ravishankar K. Iyer
Coordinated Science Laboratory and the Information Trust Institute
University of Illinois at Urbana-Champaign
1308 W. Main Street
Urbana, IL 61801
rkiyer@uiuc.edu

Abstract

Security and reliability are the key attributes in building highly trusted systems. System security violations (e.g., unauthorized privileged access or the compromising of data integrity) and reliability failures can be caused by hardware problems (transient or intermittent), software bugs, resource exhaustion, environmental conditions, or any complex interaction among these factors. To build a truly trustworthy system, the designer must find ways to mitigate (avoid and tolerate) against accidental errors and malicious attacks.

Trusted ILLIAC is a reliable and secure cluster-computing platform being built at the University of Illinois Coordinated Science Laboratory (CSL) and Information Trust Institute (ITI), involving faculty from Electrical and Computer Engineering and Computer Science Departments. Trusted ILLIAC is intended to be a large, demonstrably trustworthy cluster-computing system to support what is variously referred to as on-demand/utility computing or adaptive enterprise computing. Such systems require that a significant number of applications co-exist and share hardware/software resources using a variety of containment boundaries. Current solutions aim at providing hardware and software solutions that can only be described as a one-size-fits-all approaches. Today’s environments are complex, expensive to implement, and nearly impossible to validate.

The challenge is to provide an application-specific level of reliability and security in a totally transparent manner, while delivering optimal performance. A promising approach lies in developing a new set of application-aware methods that provide customized levels of trust (specified by the application) enforced using an integrated approach involving reprogrammable hardware, enhanced compiler methods to extract security and reliability properties, and the support of configurable operating system and middleware. Our approach is to demonstrate such a set of integrated techniques that span entire system hierarchy: processor hardware, operating system, middleware, and application.

At the processor level, a Reliability and Security Engine (RSE) provides a hardware framework that enables embedding low-cost, reprogrammable hardware modules to provide application-aware error detection and security services (e.g., process hang detection, selective duplication of the instruction stream, and detection of memory-corruption attacks).

At the operating system level, we propose a trusted microkernel that is a software framework deployed as a loadable kernel driver in Linux. This framework provides support for rapid detection of failures and attacks, including transparent application checkpointing and recovery.

At the middleware level, we employ a self-checking, run-time framework to provide detection and recovery to applications using flexible and configurable software solutions. A set of well-defined communication gateways facilitates the robust, low-overhead flow of information between the system and applications, while providing trust guarantees.

At the application level, we plan to enhance the Illinois COMPACT compiler to support the automated generation of assertions for runtime detection of accidental failures and malicious attacks, while accelerating application performance. The idea is to use information generated during the compilation process and at run-time to identify patterns in data variables and compose compact signatures of correct application behavior. Assertions for runtime signature checking can be integrated within the application or implemented directly into the RSE hardware. A distinctive, integral concept of the Trusted ILLIAC is that of a validation framework, which constitutes a cornerstone for quantita-
tive assessment of alternative designs and solutions. Such evaluation is crucial in making design decisions that require the management of tradeoffs, e.g., between cost (in terms of complexity and overhead) and efficiency of proposed mechanisms. The framework leverages years of experience in analytical and experimental evaluation of highly reliable and secure systems, on comprehensive fault and attack injection technology, and on modeling and simulation tools developed in Illinois.