1 Authentic Execution of Distributed Event-Driven Applications with a Small TCB

1.1 Introduction

This paper studies the problem of securely executing distributed applications on a shared infrastructure with a small Trusted Computing Base (TCB). We focus on (1) authenticity and integrity properties of (2) event-driven distributed applications, because for this security property and class of applications, it is relatively easy to specify the exact security guarantees offered by our approach. Any physical output event can be explained by means of the untampered code of the application, and the actual physical input events that have happened.

The main contributions of this paper are: (1) The design of an approach for authentic execution of event-driven programs under the assumption that the execution infrastructure offers specific security primitives – standard Protected Modules (PMs) [16] plus support for secure I/O (Sect. 3). (2) A novel technique for implementing such support for secure I/O by means of protected driver modules on small microprocessors such as the MSP430 (Sect. 4). (3) A prototype implementation of the approach for an MSP430 microprocessor where all security primitives are implemented in hardware, which results in a very small TCB (Sect. 4). (4) An evaluation of the performance and security aspects of that implementation (Sect. 5).

1.2 Running Example, Infrastructure & Objectives

- The infrastructure is a collection of nodes (N i), where each node consists of a processor, memory, and a number of I/O devices (D i). Multiple mutually distrusting stakeholders share the infrastructure to execute distributed applications (A i).
- The event-driven application model and modules (M i) contain input- and output channels. Upon reception of an event on an input channel, the corresponding event handler is executed atomically and new events on the module's output channels may be produced.
- attackers that can manipulate all the software on the nodes. Attackers can deploy their own applications on the infrastructure, but they can also tamper with the OS. Attackers can also control the communication network that nodes use to communicate with each other. Attackers can sniff the network, can modify traffic, or can mount man-in-the-middle attacks. With respect to the cryptographic capabilities of the attacker, we follow the Dolev-Yao model [5].
- The deployer uses his own (trusted) computing infrastructure to compile the application A, to deploy the modules to the nodes in the shared

infrastructure, and to configure connections between modules, and between modules and physical I/O channels. At run-time, an actual trace of physical I/O events will happen, and the deployer can observe an actual sequence of physical output events.

1.3 Authentic Execution of Distributed Applications