Secure Embedded Platform for Networked Automotive Systems

M. Gomathisankaran
Dept. of Computer Science and Engineering
University of North Texas

K. R. Namuduri
Dept. of Electrical Engineering
University of North Texas

1 Introduction

Modern automotive systems contain numerous electronic sensors and embedded processors. The embedded processors are used for tasks ranging from control and maneuvering, to navigation, and to communication among the vehicles. A vehicle-to-vehicle network or vehicular network, with its added functionality and communications requirements, further increases the complexity of the embedded system. The design of a safe, reliable, and secure embedded platform, suitable for networked automotive systems, is a challenge for our generation. Our focus in this position paper is on the security of the embedded system suitable for the networked automotive systems.

The embedded platform in an automotive system is severely resource constrained in terms of energy, memory, and operating system support. The safety and security of an automotive system is jeopardized if an adversary can access and manipulate either its physical environment or its resident program variables.

Henzinger and Sifakis characterize an embedded system through two sets of constraints on its design space, namely: *reaction constraints*, which specify deadline, throughput, and jitter; and, *execution constraints*, which specify performance, energy, power, area, and failure rates. Reaction constraints are a result of the interaction with the environment, whereas the execution constraints are a result of the resource constrained design. These constraints force us to develop a comprehensive embedded system design approach that integrates the design paradigms from hardware, software, and control theory, in a consistent manner.

2 Automotive Embedded Systems Security

The safety an reliability of the automotive system depends on the underlying security mechanisms that the embedded system can provide. Below, we discuss the desirable characteristics of a secure embedded platform for networked automotive systems.

Protection from cyber-attacks: Since the automatize embedded system is networked and it interacts with the physical world, it is vulnerable to classical cyber attacks such as intrusions, eavesdropping, buffer-overflow attacks, port scanning, side-channel attacks, man-in-the-middle attacks, and denial of service attacks from hackers. It is imperative that the embedded system design must consider all possible cyber attacks.

Run-time integrity: A distinguishing characteristic of an embedded system is that it constantly interacts with its operating environment. This requires the embedded system, consisting of devices, software and configuration, adapt itself with the evolving and dynamic physical environment. The design of an embedded system should include reliable mechanisms to verify its integrity and to prove its integrity to other nodes in the network. Furthermore, the embedded system must support modes that allow for remote updates in a trusted manner.

Application confidentiality: Significant intellectual property may be embedded in the applications hosted by an embedded system. This intellectual property, typically consisting of personal information and copyrighted algorithms, need to be protected both from the host operating system of the embedded system and from an external adversary such as a physical side-channel attacker.

Authentication: Each embedded system (node) in the networked system should be able to authenticate any other node that wishes to join the network in real-time before passing on accepting information from it. The authentication process must be designed in such a way that it can handle intermittent disconnections caused by intermittent connection failures.

3 Research Challenges

Specific research challenges that need to be addressed in the design of a secure platform for automotive systems include the following:

- P1 a secure execution mechanism that provides confidentiality and integrity guarantees for embedded software,
- P2 a run-time integrity verification mechanism which allows remote verification, and
- P3 an authentication mechanism that allows for trusted communications and remote updates over the network.

A hardware enabled root-of-trust is the key to address the three research challenges. The complexity of this root-of-trust needs to be tailored to match the capability of the adversary. Embedded systems, broadly speaking, come in three flavors (1) without any operating system (OS) support, (2) light-weight OS support - only with scheduling and without virtual memory, and (3) full-fledged real-time OS. Since OS is an adversary in an embedded system context, the complexity of the root-of-trust needs to match that of the OS. For example, light-weight cryptography techniques may suffice for the first the first two cases, but not for the third situation.

The problems P2 and P3 steer the embedded system to reveal information about its state, whereas the confidentiality aspect of P1 favors information-hiding. The challenge is to identify a unified solution to all these problems, even in the light of their apparent conflicting nature. Instead of designing independent mechanisms, we can think of fundamental building blocks that can be incorporated in the solution of all the three problems. The design of the security solution must take into account that an embedded system operates in potentially malicious environment, and its adversary is capable of physical access to the embedded system. This additional capability of the adversary mandates that the security solution be rooted in hardware, as software only solutions cannot prevent physical attacks.

4 Research Community

Global Engineering Network Initiative (GENI) is one avenue that we can pursue to sustain community interest in this area of research. GENI community consists of academic researchers as well as industry professionals. The authors actively participate in GENI conferences, which are held four times each year.

5 Biography

Dr. Gomathisankaran is an Assistant Professor in the department of Computer Science and Engineering at the University of North Texas. He received his Ph.D. in Computer Engineering from Iowa State University and was a post-doctoral research associate at Princeton University working in the Princeton Architecture Laboratory for Multimedia and Security. His research interests include secure systems architecture and cryptography.

Dr. Namuduri is an Associate Professor in the department of Electrical Engineering at the University of North Texas. He received his PhD degree in Computer Science and Engineering from the University of South Florida, in 1992. His current areas of interest include Information Security, Video Communications, and Consensus Building in Decentralized Systems.