SNS COLLEGE OF TECHNOLOGY
COIMBATORE - 641 035.
(An Autonomous Institution)

DEPARTMENT OF MECHANICAL ENGINEERING

19MEZ404-Connected and Automated Vehicles

UNIT II CONNECTED VEHICLE INFRASTRUCTURE

Introduction

There has been a steady increase in demand for improving the security of microcontrollers in the automotive market. When car electronics were first introduced back in the 1970s, the functions implemented were quite simple—they were discrete and unconnected to other components in the vehicle. The component that controlled the spark plugs in the engine did not communicate with the speedometer or tachometer in the dashboard. Long before the days of Bluetooth® cell phone controls or integrated audio systems, a trip computer might be the most cutting-edge feature found in a new vehicle. Over time, the combination of increased electronic complexity and integration with other fixed and portable components (e.g., keyless entry, audio systems, telematics, wireless communications, etc.) has provided portals into the control systems that are deeply embedded in the vehicle. User-accessible systems potentially contain personal and private information, while the embedded systems are inextricably tied into the fundamental physical behavior of the vehicle. These two aspects mean that if any of the vehicle control and information systems are compromised, the opportunity for theft or damage from external entities appears. Today's cars are also expected to hold even more private information as they become smart cards on wheels to simplify financial transactions at gas pumps, charging stations, parking lots, toll booths and drive-through establishments. The vehicle itself will be enabled to pay fees and fares, sometimes automatically. Security has come a long way since the initial introduction of simple features like car alarms and keyless entry. In today's vehicles, security features must include not just physical access and protection of confidential information, but also critical safety systems such as driveby-wire braking and steering. The increasingly interconnected nature of a vehicle's control modules means there is no safety without security. The nature of the automobile industry itself also introduces some additional interesting security considerations. In order to support a very long and reliable operating life (which may be an order of magnitude longer than most consumer products), the installation of counterfeit parts and control units must be prevented. The vehicle’s security systems can provide a means to do this using an authentication protocol. Another factor that can affect system reliability is the practice of “chipping” or modifying the operating parameters stored in memory. Security features can prevent “chipping” altogether or can detect the presence of any unauthorized modification and take action to mitigate or eliminate the effects of the modification so that the vehicle is still safe to drive, while indicating the need for corrective attention. Defining the architecture and implementation of secure microcontrollers requires a unique mindset. The designer must think like a hacker and come up with bulletproof ways to anticipate and prevent access to secure data. The great range of available attack mechanisms (often referred to as the attack surface) normally means that designers must make a trade-off between the developer’s cost of 3 Automotive Security: From Standards to Implementation White Paper freescale.com protecting against an attack (or a customer’s revenue lost as a result of an attack) versus the hacker’s cost of mounting the attack. For example, if it is necessary to reverse engineer the silicon to uncover security codes, it might not make commercial sense to attempt this on something like a TV remote control. There is also a great deal of activity in the industry at large to develop standards, specifications and guidelines for vehicle security. Standardization allows for greater interoperability between the various component suppliers to the auto industry. Having set specifications means that all manufacturers have an opportunity to develop security-aware products without compromise. Being able to follow published guidelines allows the manufacturer implementation freedom while adhering to the overall architectural requirements and specifications that enable interoperability. Standards, Specifications and Guidelines Antiquated methods of “security by obscurity” offer highly precarious and ineffective approaches for protecting most modern environments. Today’s most robust forms of security and encryption are those that survive scrutiny—in other words, security and cryptographic algorithm specifications that themselves do not have to be kept secret but are instead distributed in the public domain. Within the automotive engineering community, a number of specification activities are either ongoing or have reached sufficient maturity to be accepted as a standard. For example, the Secure Hardware Extension (SHE) specification developed by Escrypt for Audi and BMW via the HIS Working Group, with early cooperation from Freescale in 2008, has now been accepted as an open and free standard. The SHE specification defines a set of functions and a programmer’s model

(API) that allows a secure zone to coexist within any electronic control unit installed in the vehicle. The secure zone's most significant features are the storage and management of security keys, plus encapsulating authentication, encryption and decryption algorithms that application code can access through the API. These features help maximize flexibility and minimize costs. A later section of this white paper includes a description of the architecture of the SHE implementation on Freescale's MPC5646C single-chip microcontroller targeted at body control applications, where the security functions can be used for vehicle and ECU theft protection such as immobilizer activation. The EVITA project, funded by the EU, has developed a set of guidelines that details the design, verification and prototyping of a range of security architectures for automotive ECUs. A number of companies have been active in the EVITA project, including BMW, Continental, Fujitsu, Infineon and Bosch. EVITA defines the overall functionality of three different hardware security module approaches: –full, medium and light. Moreover, it specifies an elaborate set of functions and their parameters for managing security keys as well as encryption and decryption operations. A new European funded project called PRESERVE has emerged from the cooperating entities involved in EVITA. The aim of this new project is to develop, implement and test a scalable 4 Automotive Security: From Standards to Implementation White Paper freescale.com security subsystem for Vehicle-to-Vehicle and Vehicle-to-Infrastructure (conflated to the acronym V2X) applications. The ongoing work is expected to be completed by the end of 2014. The efforts of the PRESERVE project are targeted at demonstrating the secure transmission of data and control information for the future Intelligent Transportation System (ITS). The hardware security module implementation will include Elliptic Curve Cryptography (ECC), which is a form of public key cryptography. Another good example of a security standard comes from the National Institute of Standards and Technology (NIST), which has issued the FIPS (Federal Information Processing Standards) 140 standard for both software and hardware components. FIPS 140-2 defines four levels of security ranging from Level 1 with a simple single security function and no physical security requirements up to Level 4 that mandates physical tamper detection mechanisms and protection against environmental attacks, such as voltage and temperature. Freescale's P2041 devices support several encryption and authentication keys that are identified as being Critical Security Parameters (CSPs) in the FIPS 140-2 specification. An overview of P2041 security capabilities is described later in this white paper. Other somewhat proprietary specifications and guidelines exist to aid the development of secure embedded systems. ARM® developed its

TrustZone® security infrastructure, which has been integrated into microcontrollers and microprocessors from various manufacturers, including Freescale's i.MX series and Vybrid family of devices. Another standards organization is the Trusted Computing Group (TCG), which claims to provide open, interoperable and international standards for trusted computing. One specification released by this organization is their Trusted Platform Module (TPM)—published as ISO/IEC 11889 Parts 1-4. Like the SHE specification, TPM supports secure keys for authentication and encryption functions. Developers generally implement TPM as an external peripheral with a communication bus to another microcontroller in the system. TPM specifies non-volatile memory, secret key storage, a random number generator, RSA, SHA-1, HMAC and Vernam one-time pad algorithms. The Advanced Encryption Standard (AES) is optional for TPM devices. Security Mechanisms The mechanisms needed to manage the security of an application may be implemented in software, hardware or a combination of both. In general, some form of software execution is always needed. Hardware is usually provided to accelerate the execution of the cryptographic algorithms to meet the performance requirements of the application. For example, an SHA-256 algorithm used to checksum the contents of memory could easily be two orders of magnitude faster with hardware acceleration, in comparison to a purely software-based equivalent. The benefits of hardware acceleration become even more compelling for asymmetric cryptographic algorithms such as RSA and ECC, especially as the key size increases. Figure 1 shows the relative increase in computation time for software-based RSA authentication using a public key. With a hardware accelerator, the same public key authentication operation can be executed in under 100 microseconds.