TrustZone: Integrated Hardware and Software Security

Enabling Trusted Computing in Embedded Systems

Author:
Tiago Alves and Don Felton, ARM

Synopsis:
The rising interest in solutions for trusted computing is largely driven by the potentially severe economic consequences of failing to ensure security in embedded applications.

Ensuring security in both wired and mobile applications has become imperative. Making an embedded product safe from malicious attacks has consequences for hardware and software design, as well as the physical attributes of the design. It is now accepted that the best protected embedded systems must have security measures designed-in from the outset, starting with the specification for the processor or CPU core.

ARM is enabling system security by integrating protective measures into the heart of its cores and providing secure software to complement the efforts of semiconductor manufacturers, product OEMs and operating system partners. For OEM partners, the issue of platform integrity has become paramount. For network operators and content providers, concerns over digital rights management (DRM) and m-commerce are growing.

Through a combination of integrated hardware and software components, ARM's TrustZone™ technology provides the basis for a highly-protected system architecture, with minimal impact to the core power consumption, performance or area. TrustZone is a safe execution environment that enables semiconductor and OEM developers to incorporate their own application-specific security measures in tandem with their own hardware and software IP. TrustZone software components are a result of a successful collaboration with software security experts, Trusted Logic, and provide a secure execution environment and basic security services such as cryptography, safe storage and integrity checking to help ensure device and platform security. By enabling security at the device level, TrustZone provides a platform for addressing security issues at the application and user levels.

Why is Security So Important?

There are many examples of the very significant costs associated with the failure of embedded systems to resist malicious attacks. These span multiple applications and industry segments, and include both direct costs and lost revenue opportunities. The need to improve security has been particularly driven by the ever-increasing spread of wireless systems that encompass data services and payment applications.

The technical issues associated with the realization of data services over mobile devices provide both a revenue opportunity, but also a threat to security. A smartphone optimized primarily for data services requires that the terminal becomes an open platform for software applications. Whilst this is essential to deliver the full range of user applications and services, it also means that the mobile device becomes more vulnerable to attack.

There are several security scenarios that are causes for concern. The first is the potential to rapidly propagate viruses over a mobile network through a user's phone book, with the worst-case outcome being denial of the operator's service – essentially bringing down the wireless network. The second threat model involves the vulnerability of end-users' private data – for example, private keys for enabling financial transactions or banking applications, email messages and remote access to corporate networks. The inability to safely hold this type of information on a mobile terminal may inhibit the growth of such services. Viruses also have the potential to disrupt operation of the phone itself – for example, blocking calls within the radio cell.

Within the mobile phone sector, security issues with handset identity codes cost the industry billions of dollars every year. The unique International Mobile Equipment Identity code (IMEI) is a 15-digit code used to identify an individual GSM mobile, while SIMLock should ensure that a handset can only be used with the subsidizing operator's SIM card. On many handsets, both of these codes can be broken with little effort. The result of this is an opportunity for fraud to be committed on such a scale that some statistics suggest it is driving 50% of street crime[1] through mobile phone thefts.

Protection of digital content through digital rights management is another important area where security is becoming a mandatory requirement for consumer protection, as well as the protection of commercially valuable content.

The significant growth in wireless connectivity is also elevating security to the top of the list of functional system requirements.

The growth of wireless LAN is one aspect of this, but the opportunity for pervasive wireless connectivity, such as offered by Bluetooth™ and other similar standards, presents a potentially more widespread security challenge. With truly mobile computing, computers are no longer restricted to equipment that users or administrators manage themselves. Consequently, security must be considered in many devices as a fundamental implementation issue.

Economic Value in Security Issues

Practically every security issue can be related back to economic value, touching every point in the industry value chain. This includes content owners and providers who need to be able to protect and charge for their content and services, and be able to take advantage of new business models; service providers who must protect their networks against malicious use and provide efficient channels to reach end users; and the end users themselves who want privacy, protection from street and cyber crime, but with convenience and the freedom to choose their source of service.

Fraud of any kind has an economic cost, often in lost revenues as a result of counterfeiting or abuse of digital media rights. For example, telecommunication frauds are estimated to cost the industry more than a billion dollars yearly.[2] One of the biggest contributors to that cost is the cloning of cellular handsets.

For end users, there may be loss of personal funds as a result of electronic theft. In the wider context, research has demonstrated that enabling easy and secure payment systems can boost consumer spending on credit by up to 20 percent.

Better security will enable new revenue streams and different business models for some industries. For example, the current use of credit cards for web-based transactions can be an expensive overhead when used for very small transactions, or 'micro-payments'. Better security measures will reduce the risk of using credit cards for micro-payments, thus reducing the transaction cost. The likely outcome is the generation of new revenue streams for industries such as online gaming, where endusers will be able to buy resources to enhance their game-playing experience.

For manufacturers, security will become an issue of competitive differentiation. Handset devices with inappropriate levels of security will be left on the shelves.

At a corporate level, the adoption of mobile information appliances will be limited by the ability to demonstrate protection for company assets. The use of smartphones and wireless networks in the corporate environment brings a new range of vulnerabilities. Unsurprisingly, companies have demonstrated a willingness to pay for more robust security in mobile systems.

Open Industry Issues

There are a number of possible approaches to building security measures into embedded systems.

Much of the effort towards implementing embedded security solutions to date has been focused on building security features into operating systems (OS). However, the fact that OS are by definition open, and extremely complex software systems, makes it difficult to provide robust security solutions based on the OS alone.

The lack of common security elements across different platforms is obstructing the development of integrated security solutions. With no standards in place, implementation of embedded security measures has been fragmented, costly and consequently adoption has been slow. Up to now, many OEMs have developed their own software modules based on the execution of a secure execution mode outside the CPU or OS. Inevitably this approach will be less safe than a solution that integrates hardware, OS and application measures.

The implementation of security measures requires the application of techniques that can inhibit the development and debug process. Currently, some manufacturers provide special pre-production debuggable handsets to developers to help accelerate the application development process. However, this can compromise security measures if these handsets become available within the public domain. What is really required is a solution that enables debug without compromising security.

The successful deployment of trusted computing within portable and wireless equipment depends on being able to address these key open issues.

The Options for Security

There are a number of possible approaches to building security measures into embedded systems.

One option is to add a hardware security module to the design. This approach suffers from all of the restrictions inherent in any pure hardware solution. Pure hardware solutions are inflexible; they cannot easily be adapted to cater for new security functions. Obviously if an error is discovered it cannot easily be fixed without a costly design re-spin. Additionally, adding hardware IP adds manufacturing cost to the design and can have an adverse affect on power consumption.

Off-chip hardware, such as co-processors and storage, offer another approach to embedded security, enabling the acceleration of demanding cryptography algorithms, for example. However, adding a second processor to the system adds to the cost, complexity and power budget. Additionally, this approach may not provide the fundamental level of security required in the CPU processing and operating systems. The nature of the physical implementation means that traffic may be exposed between the core processor and the off-chip device, and it may not be possible for the CPU device to ascertain the integrity of the off-chip device – it may be removed and interfered with. Performance may be an issue, as with any off-chip processing.

SIM cards have a role to play in securing wireless embedded systems. The strength of the traditional SIM card in enabling security within the handset is predominantly in guarding against physical attacks. There are two opposing trends in SIM card development. One trend is towards more functionally capable SIM cards, or 'Super SIMs', containing larger memory and having more processing power.

The other trend suggests a move towards smaller SIMs with more compact form fac-

[1] http://news.bbc.co.uk/1/hi/uk/3326171.stm

[2] http://www.secretservice.gov/Telecommunications