OMAP™ platform security features

By Harini Sundaresan
Applications Engineer, OMAP Security Texas Instruments, Wireless Terminal Business Unit

This white paper introduces TI's OMAP application processors in the wireless and the embedded space and highlights their security features. The security architecture for TI's OMAP platform is a combination of hardware and software components that enforce the security policy and provide secure functionalities to the platform.

Table of contents

Table of figures

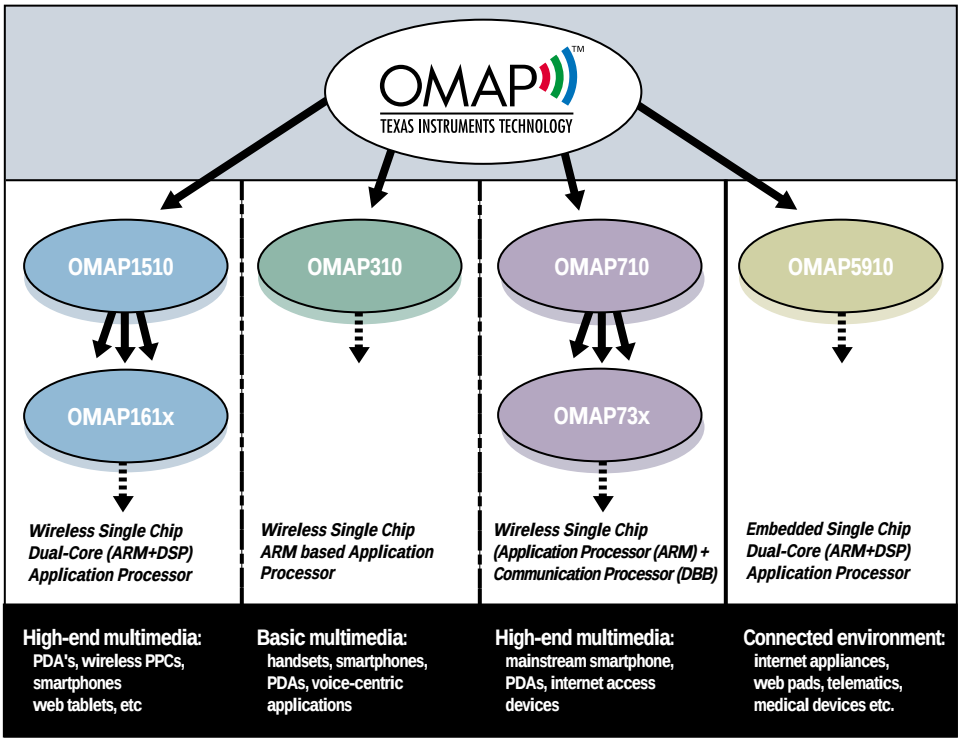
Glossary

AES	Advanced Encryption Standard
API	Application Programming Interface
DBB	Digital BaseBand
DES/3DES	Data Encryption Standard/ Triple-DES
DRM	Digital Rights Management
DSP	Digital Signal Processor
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HW	Hardware
MD5	Message Digest version 5
MPU	Main Processing Unit. The main processor used in computers (and phones).
NoVo	Non Volatile
OS	Operating System
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PPC	Microsoft® Windows ® Pocket PC
RAM	Random Access Memory – a writable memory.
RNG	Random Number Generator
ROM	Read Only Memory
SE	Secure Environment
SHA-1	Secure Hash Algorithm. Algorithm version 1. Algorithm used to calculate highly secure hash values
SSL	Secure Socket Layer
SW	Software

OMAP application processors

TI's OMAP™ application processors can be broadly classified into two categories focusing on different markets: 2.5G and 3G wireless handsets and embedded applications. Wireless OMAP processors address a wide range of market segments from traditional cost-sensitive, voice-centric handsets to multimedia-rich wireless handsets and PDAs with the best combination of high-performance and ultra-low power consumption. Embedded OMAP processors are ideal for designers working with devices that require embedded applications processing in a connected environment such as Internet appliances, web pads, telematics and medical devices.

Figure 1: OMAP application processors



The need for security

The need for strong security in the OMAP platform comes from the vulnerability of the wireless space to security risks such as viruses. The mobile phone has traditionally been a closed system. In Europe, security is mainly relying on the SIM card, which provides the user of the mobile phone with a unique network identity. Due to the closed nature of the system and to the robust smart card manufacturing process, the risk for the Network Operator to suffer from hackers was limited.

The introduction of packetized services, such as GPRS, and the move to 3G systems opens the wireless industry to a new range of services and a new vulnerability to hackers. The formerly closed nature of mobile phones is changing to a more open system offering rich content and applications available over the air. With this openness a new level of security is required to protect wireless networks and handsets. Open architectures require security not least because of the threat of viruses but also because malicious software can compromise the intended commercial use of the phone and the deployment of value added services.

Japan was the setting for the first example of security weakness for current 2.5G and 3G mobile phones. There were a number of attacks with various consequences including:

- malicious e-mails to wireless handsets that unleashed malicious code which took control of the communications device and, in some cases, repeatedly called Japan's emergency response system
- placing long distance calls without the user's knowledge
- handset lockup, making it impossible for subscribers to use any of the arrier's services

Numerous incidents involving spamming, denial-of-service, virus attacks, content piracy and malevolent hacking are becoming rampant in the wireless field. The security breaches that have posed a constant threat to desktop computers over the last 10 years are migrating to the world of wireless communications where they will pose a threat to mobile phones, smartphones, personal digital assistants (PDAs), laptop computers and other yet-to-be-invented devices that capitalize on the convenience of wireless communications.

With over 12 years of wireless experience, TI has the depth of knowledge imperative for understanding how critically important security will be to the success of 2.5G and 3G. To meet the needs of the wireless market, in February of 2003 TI announced five new OMAP processors with on-chip hardware security.

OMAP security solutions

OMAP1510, OMAP710, OMAP310, OMAP5910 processors

The first generation of the OMAP processors includes the OMAP1510, the OMAP710, the OMAP310, and the OMAP5910. The security solution for the first generation of OMAP processors is software based. TI, working with industry leading security providers, Certicom and Safenet, has high-performance software crypto libraries available for high level operating systems (HLOS) like Linux®, Microsoft® Windows® CE, and Symbian OS™ that are optimized for the OMAP platform. Apart from core crypto functions, TI also offers Certicom's SSL toolkit and PKI toolkits that are optimized for the OMAP platform. These software crypto engines and toolkits have been tested with regressive tests and provide user friendly API guides and sample test frameworks enabling quick development.

Figure 2: OMAP platform security solutions

OMAP Security Features	OMAP 1510	OMAP 161x	OMAP 310	OMAP 710	OMAP 73x	OMAP 5910	Benefits to OEM
Crypto Engine **SW Crypto Library**	•	•	•	•	•	•	Optimized to enhance performance and efficiently use power
True HW-based RNG (Random Number Generator)		•			•		Enhanced security (versus SW-based pseudo RNG)
CyptoHW accelerators (DES/3DES, SHA1/MD5)		•			•		High throughput/Power efficient (VPN/SSL / FileEncrypt/ DRM etc.)
GSM/GPRS DBB Modem SDRAM Protection				•	•		Flash boot sector write protection and shared memory protection
Third Party applications	•	•	•	•	•	•	Optimized solutions offer fast time-to-market
Secure Boot/flash		•			•		Secure boot/flash process (prevent security attacks during device flashing and booting)
Secure Environment		•			•		Execution of authenticated code, secure crypto and management (VPN/SSL, DRM, e-wallet, etc.)

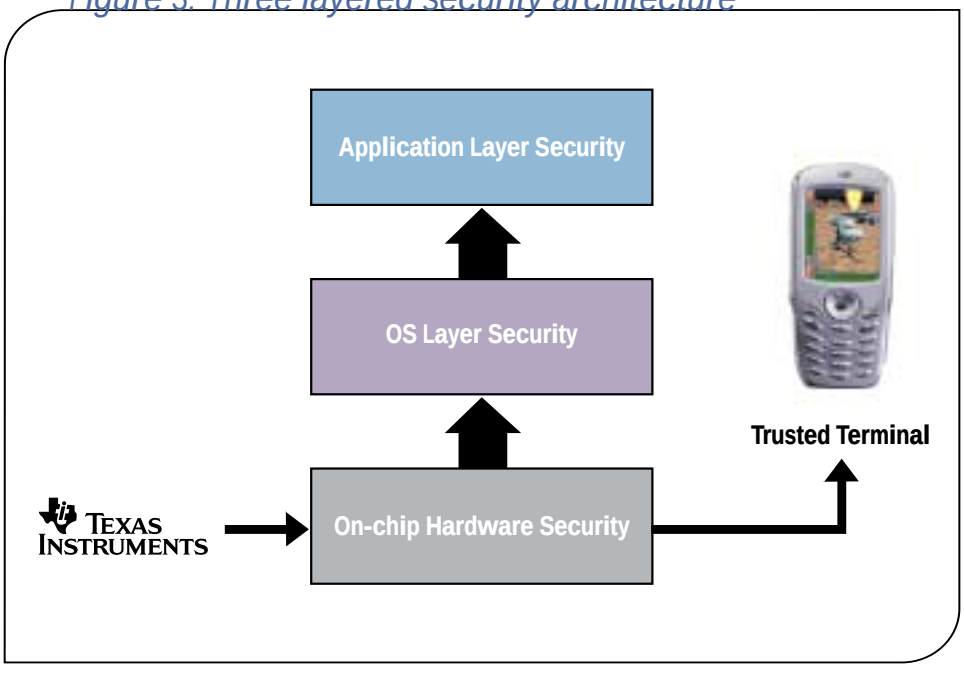
Apart from the SW core crypto library, the OMAP Developer Network offers additional Third party security applications. These applications are optimized for the OMAP platform and offer OEMs development cost savings and faster time-to-market. A few of the offerings from OMAP developers includes:

- Biometric fingerprint recognition from Authentec
- VPN application from Safenet and Certicom
- Virus protection from Network Associates
- Firewall, Content Filtering and mobile data security from WhiteCell
- Encrypted FAX capability from Snapshield

OMAP161x, OMAP73x processors

One of the distinguishing features of the second generation of OMAP processors, the OMAP161x and the OMAP73x devices, is the embedded on-chip security. This is described in detail in the next section. This security solution is a combination of hardware and software components used to create a "trusted device". Today, most devices include two layers of security: application layer security and operating system layer security. While these efforts reduce risk, stand-alone they are not sufficient. TI offers a third layer of protection that integrates embedded hardware security technology. By doing this, TI enables manufacturers to offer a new layer of defense at the chip level that is fast and serves as a security foundation for the applications and OS layers, thereby creating a "trusted" mobile device.

Figure 3: Three layered security architecture



OMAP platform security features

Secure Environment

The Secure Environment is a feature available, where critical code and data can be executed securely and sensitive information can be hidden from the outside world with the help of the following security components:

- Secure Mode (Secure Execution Environment): Can be viewed as a 3rd privilege level allowing secure execution of “trusted” code via on-chip authentication. Its activation relies on the presence of special–purpose hardware creating an environment for protecting sensitive information from access by non-trusted software. The secure mode is set with the assertion of a dedicated security signal after a set of pre-determined security conditions are met. This signal propagates across the system and creates a boundary between resources that only trusted software can access and those resources available to any software.
- Secure Keys: OEM specific one-time programmable keys accessible only in secure mode used for authentication and encryption in a secure environment.
- Secure ROM: Accessible only in secure mode and contains security services such as secure storage mechanism using secure keys, key management and cryptographic libraries.
- Secure RAM: Accessible only in secure mode and used for running OEM specific “trusted/authenticated code”.

Secure Boot/Secure Flash

The foundation of a secure platform is the authentication of the software installed on the platform. The authentication process must guarantee the origin and the integrity of the software stored in the external NoVo memory.

In security-enabled production devices, secure flash and secure boot is enforced to achieve high level of security. Secure flash ensures that the OEM’s OS image is correctly and securely programmed into flash memory at the factory. Secure Boot ensures that the “authorized” OEM’s SW (signed by the OEM) and optionally the OS image (optionally signed by the OEM) is authenticated prior to execution. This prevents the code from being modified by unauthorized entities or the external memory NoVo from being tampered with. It also prevents the execution of any forged or spoofed software code. The authentication of a software module is based on a certificate associated with this module*[1].

Run-time Security

The OMAP platform secure environment can be extended to OS applications during run-time for relatively short security critical tasks such as key encryption/decryption, authentication and managing other highly secure data. Such operations often require maximum security in DRM, VPN and banking applications. The run-time services require the presence of software interface components like the APIs and drivers designed to integrate the secure environment into the OS.

Crypto Engine

The OMAP161x and OMAP73x processors have HW crypto engines to achieve higher throughput and enhance security. The HW crypto engines available are DES/3DES, SHA1/MD5 and RNG. These HW crypto engines can be either configured as secure mode access only or both user mode and secure mode access based on the OEM's preference.

1. HW Accelerators in Secure Mode: For security applications that are short and/or require high level of security (e.g.: M-wallet application, DRM key management, Point Of Sale terminal verification), the secure mode only access configuration is desirable.
2. HW Accelerators in User Mode: For security applications that are long and/or require medium or low level security (which does not require the secure mode services) but desire higher throughput (e.g.: VPN, WLAN, bulk data encryption), the user mode access configuration is the preferable choice.

The OMAP SW crypto libraries from TI's security providers Certicom and Safenet have an added feature allowing developers to seamlessly access the HW accelerators in user mode from their crypto libraries. Developers simply need to use the IPSec toolkit, SSL toolkit and/or the PKI toolkit running on the top of the SW crypto libraries to take advantage of the HW Accelerators. The ease of development is a great benefit to OEMs and offers faster time-to-market since TI and its security providers offer the complete, integrated, optimized solution.

Conclusion

The security architecture offered by the OMAP platform is a combination of hardware and software mechanisms for safe execution of secure services:

- On-chip security hardware offers the necessary robustness for tamper resistance
- Software security provides the modularity and scalability to support numerous cryptographic standards and security protocols for confidently running any value added application

Thus, building a security foundation on the OMAP platform, manufacturers that choose TI will meet the "trusted security" challenges of 2.5 and 3G wireless and embedded devices. The thirst for security can never be quenched completely; however strong we build a fortress, new threats will always appear. TI is determined to continue its leadership in building robust wireless/embedded security solutions for its customers for all future generations of the OMAP processors.

References

1. www.omap.com
2. *Reducing the Security Threats to 2.5G and 3G Wireless Applications* – www.omap.com
3. *Wireless Security: from the inside out* – www.omap.com

*[1] Note: There are other types of devices where secure boot and secure flash is not enforced. It is not in the scope of this white paper to discuss them in detail.

Special thanks

Special thanks to the following Texas Instruments WTBU members for their contribution to this white paper either in the form of review, feedback or internal reference materials: Erdal Paksoy, Jerome Azema, Sunil Hattangady and Jason Vorel.