Securing the Future

Albert Chiang
MIPS Technologies, Inc.
November 2006

A system is only as secure as its weakest link, and security becomes ever more important as more equipment moves to a system-on-chip (SoC) approach, Albert Chiang, strategic marketing manager at MIPS Technologies, looks at the security options available to SoC designers.

In addition to performance, SoC designers have become increasingly aware of the need for security functionality in consumer devices. Security has emerged in the last year, especially, as an increasingly important consideration, protecting both the device and its content from tampering and copying.

Designing a secure system takes a chip-wide approach. Any system is only as secure as its weakest element, and retro-fitting elements for security to a system that has not been designed with security in mind is only a temporary fix. The protection of a device's "secret key", content, and understanding the basic requirements of a secure SoC is vital in a system designer's ability to provide leading edge products.

Coming from the server market, the MIPS® architecture has been designed from the beginning to be secure. Servers handling millions of credit card transactions every hour need to be as secure as possible, and MIPS Technologies has been supplying silicon for these systems for 20 years.

With more and more e-commerce applications running on phone handsets today, mobile systems are only now looking to adopt security for the same reasons. While mobile processors have previously relied on SIM cards as the secure element, the processor architecture and integration architecture are now critical to the security of the whole system as more and more of the peripherals are being integrated into a single chip.

There are three elements that are vital to a secure system in silicon:

- Secure peripherals that prevent unauthorized access, ideally with multiple levels of access
- A trusted environment to run trusted software and store sensitive data in a secure area
- Cryptographic acceleration, which is more than a secure peripheral

Hypervisor

One way to provide multiple levels of security to peripherals is to create a Hypervisor, a thin layer of software that has greater priority than the supervisor in a system. Supplied by companies such as TRANGO Systems in Grenoble, France, the tiny 20Kbytes of the Hypervisor creates virtual processors that allow multiple operating systems run on one CPU. This works because the Hypervisor guarantees separation and time-slicing among the virtual CPUs.

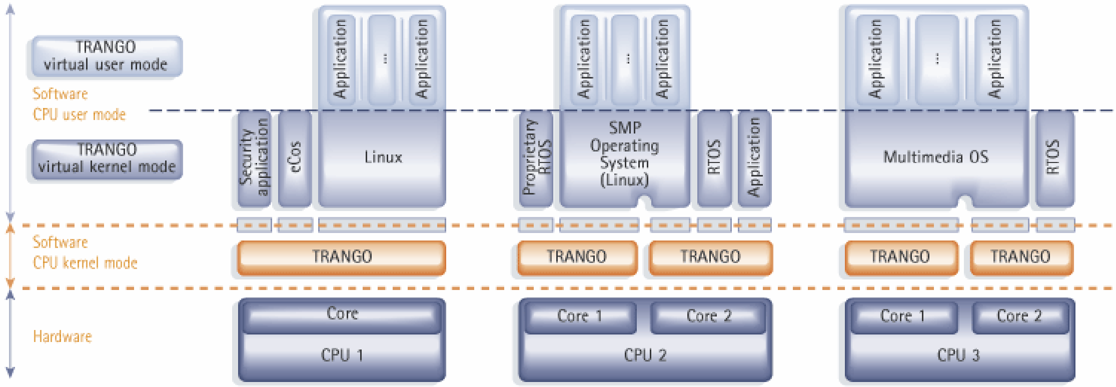


Figure 1: The virtual machines set up by software from TRANGO Systems

This approach provides an efficient thin layer of code that allows system designers greater flexibility to extend the functionality of an existing system or to use only one CPU to handle multiple OSes, for example. Some system designers choose to use a dual CPU approach when performing secure operations in a trusted environment. One CPU handles the open OS where application(s) run and the other CPU to handle a secure OS for key management, for instance. With the Hypervisor product provided by TRANGO systems, only a single CPU is then needed to keep the OS and multiple environments separate. This means that a system designer working with an existing system can create trusted areas where secure processes like key management or secure boot can run without adding another CPU, Or, in systems where there is more than one CPU, the Hypervisor can extend functionality without major hardware changes.

This approach is applicable to a wide range of systems including DVD players, printers, cable and DSL modems, routers, medical equipment, electronic payment systems, video and data processing, set-top boxes and digital televisions.

For mobile phone applications this allows multimedia, real-time and trusted applications to be easily integrated, reducing production and development costs and enhancing the security and integrity of users' personal data. In networking equipment, the Hypervisor allows the secure integration of Linux and market standards into existing embedded systems, supporting symmetric multi-processing (SMP) operating systems, high-availability, and OS redundancy policies.

In summary, regardless of configuration, the Hypervisor keeps all the multiple environments separate, all without having the different parts of the system interact without permission, with full predictability, and with high performance.

Secure peripherals

Looking to the future, a new generation of standards is enabling a wide range of secure peripherals with individualized access levels, avoiding the problems that can occur with a single trusted environment. In that situation, if one peripheral is breached, it can be used to access all the others. With multiple levels of access, the peripherals and assets that need to be most secure, such as those handling certificates and credit card numbers, can still be kept secure from other peripherals.

The OCP-IP specification (Open Core Protocol International Partnership) is defining a standard way of building secure peripherals based on a signal on the bus that can be defined by an arbitrary number of bits to set different levels of access.

This will allow processor cores to build in capabilities similar to that of Secure Machines and chip designers to use a wide range of peripherals and easily build more secure systems. MIPS Technologies has been a strong supporter of OCP-IP as it builds the ecosystem of peripherals and software that can be combined to create secure systems.

This is different from recent moves to create standard specifications to provide secure communication links between separate devices in a system. These are aimed largely at conditional access systems and protecting the content in Pay TV systems. This becomes less relevant as the functions are integrated into a single chip and use the Secure Machines approach or OCP-IP specification to provide a secure interface.

Trusted environment

So far, trusted environments have been built with proprietary technology as closed systems, and only on new processor cores, so that new applications are time-consuming to develop and verify and are not backwards compatible. There are better ways forward.

The MIPS32® 4KSd™ core augments the 4KEc™ embedded core with a secure MMU that scrambles the cache interface and adds cryptographic acceleration through the SmartMIPS™ instruction extensions, as well as designed with anti-analysis features. This mix of hardware and software adds less than 10% to the size of the core but provides a secure system that has already been used in smartcards.

The SmartMIPS Application Specific Extensions (ASE) are extra instructions for the MIPS32 architecture optimized to help cryptography and secure applications. They were jointly defined with Gemplus (now Gemalto)—the world's number one provider of smart cards—to combine cryptography enhancements, secure memory spaces, code compression and virtual machine performance enhancements. Among other applications, the SmartMIPS ASE serves to enable an inexpensive, low-power and complete smart card processor solution.

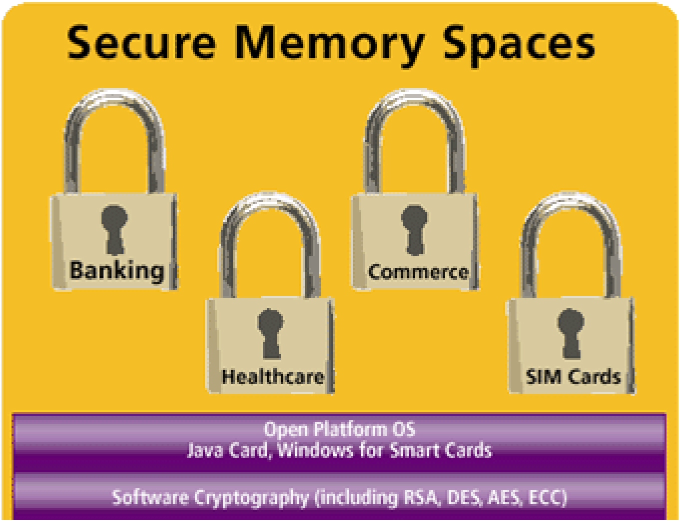

Secure Memory Spaces
Banking
Healthcare
Commerce
SIM Cards
Open Platform OS
Java Card, Windows for Smart Cards
Software Cryptography (including RSA, DES, AES, ECC)

Figure 2: The SmartMIPS™ extensions are optimized for cryptography and secure applications

The cryptography enhancements speed public-key data security algorithms, providing three to ten times the speed of a software-only implementation. Secret-key operations also gain, but to a lesser extent.

Software cryptography allows easy field upgrades of cryptography algorithms. Therefore, a potential breach in the security algorithm doesn't require a recall of the actual cards, and the accelerated software cryptography enables choice of algorithm (such as RSA, DES, AES, and elliptic curve cryptography—ECC) on a per-application basis.

The Secure Memory Spaces protect sensitive consumer data by application, preventing unauthorized data access by rogue applications. Built-in code-compression minimizes memory use, preserving scarce memory resources.

As the core is synthesizable and has a high maximum frequency, the SoC designer has many options when it comes to floor planning. This is important as some analysis can determine the activity patterns of particular execution units and deduce some of the code activity, so avoiding noticeable hotspots is a standard technique in secure processor design.

The 4KSd core can be used as a secure second core alongside a 24K® core as host, providing digital rights management and certificate handling. As this requires minimal caches, the core can be a negligible 1.5mm^2.

Host controller

Another option is to use the 4KSd core as a secure system controller. This can save area in the SoC, but requires secure applications to have a higher level of privilege than the operating system. As most operating systems running kernel mode it means that the OS has to be ported to run in supervisor mode, leaving the secure applications to run in the kernel mode.

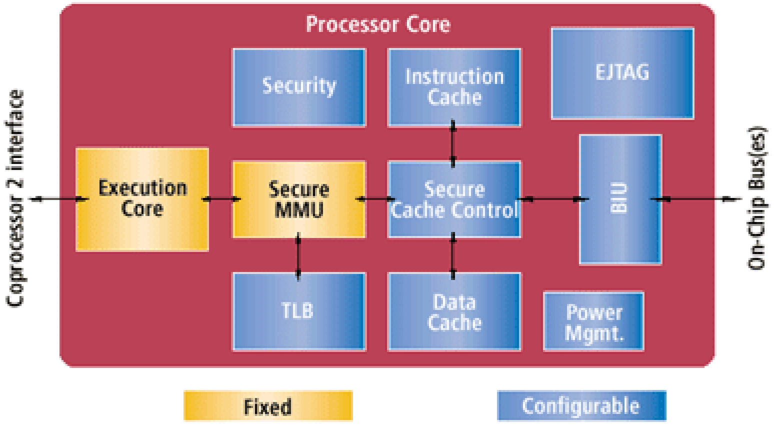


Figure 3: The MIPS 4KSd core

This allows the same core to be used for non-secure functions, for example in a point of sale terminal, and then use the kernel mode for a secure application to handle the payment.

The virtualization approach from TRANGO Systems can be used on the 4KSd or on any MIPS core. This creates a secure virtual second CPU that runs in kernel mode while the main operating system runs in a “virtual kernel” mode, which is instantiated in user mode.

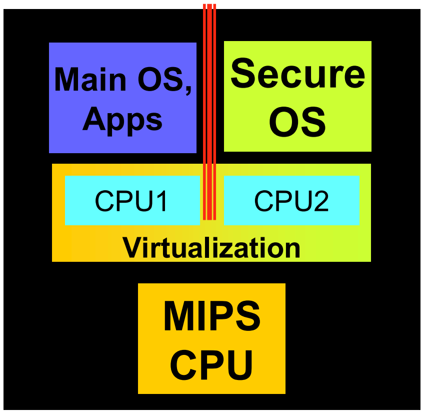


Figure 4. Virtualization technology (Hypervisor) provided by TRANGO Systems can set up a separate and secure OS needed in a trusted environment

The core then switches contexts between the two environments, with the Hypervisor virtualization layer handling address protection, interrupt vectors and exception handling to keep the system secure. The additional load required for this approach is nominal, with the context switch taking no more than 60 cycles, and typically 16 cycles.

Such a system has been demonstrated running Linux concurrently with two real-time operating systems on a single MIPS core. This approach provides the system designer with much needed flexibility in integrating new functionality, including adding security to the existing system while preserving the software or hardware investment.

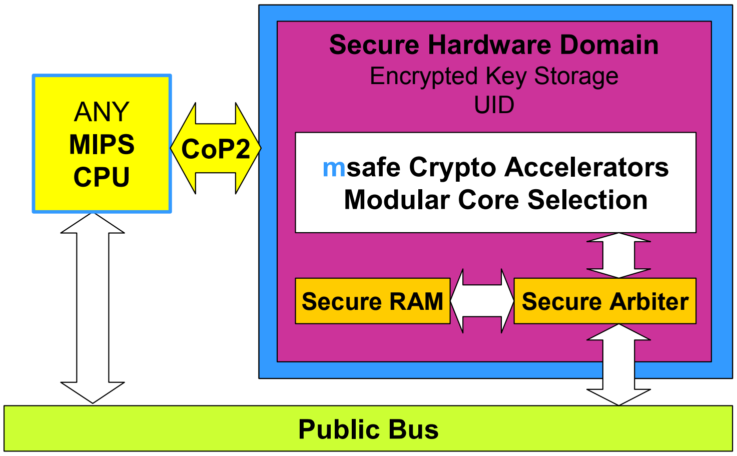
Safe-SOC™ Platform

MIPS recognizes that security and content protection is becoming increasingly important not only in enterprise networking devices but in a variety of devices in the consumer home that MIPS-Based devices have a dominant share. Safe-SOC™ is a platform where providers of software – such as TRANGO Systems, as well as hardware IP such as cryptographic cores from Israel-based msystems integrate their technology to provide the basics of a secure SoC, for instance. A secure SoC should provide these basic attributes:

- ➔ Trusted execution - Secure boot verify code integrity before booting
- ➔ Protection of the secrets during storage and execution - Secure storage hidden area for expiration date of content/constraints
- ➔ Key Protection – prevent read access of keys (used to decrypt and signatures)
- ➔ Cloning Protection – prevents attacker from cloning the SoC

msystems is an important Safe-SOC Platform alliance partner. msystems (now a wholly-owned subsidiary of SanDisk) has created a tightly coupled, modular, and configurable secure hardware domain based on msystem's mSafe™ cores. The secure hardware domain is directly connected to the MIPS® coprocessor interface (COP2) with direct access to any MIPS core. The secure hardware domain is protected by the MIPS CPU. COP2 is a dedicated interface that every MIPS core has and is not shared by other peripherals or traffic. This means physical isolation from access by potentially malicious software and hardware attacks. This isolation also results in higher throughput and less latency than those provided by a shared bus interface.

The crypto functions provided by msystems include the required implementation of secured memory (CryptoRAM) where secret system assets can be stored and protected during algorithm execution. The crypto cores, such as hardware-based AES (Advanced Encryption Standard) provide a fast, yet power efficient solution that is based on the highly robust and silicon proven mSafe cores from msystems. When compared to competing software-based solutions, it provides better than an order of magnitude improvement in response time, a significant saving in power, and a much higher level of resilience to analysis and other attacks. These advantages are particularly effective in portable products.



Another key advantage of this approach is its configurability. Cryptographic functionality and performance levels can be selected based on specific requirements, giving the minimum layout and cost for the application, as opposed to the larger area and silicon cost of a general purpose encryption coprocessor. This is vitally important in consumer applications where every square millimeter of silicon contributes to the cost of the end unit.

msystems provides industry-recognized crypto algorithms, such as AES, 3DES, SHA-1 and MD5 as well as the full range of PKI algorithms required for authentication and verification using public/private keys. The coprocessor can also include a completely digital and compact Random Number Generator (RNG). For example, a 3DES engine takes up only 8K gates and operates at 100 to 200Mbit/s. If the SuperMAP core is also included, authentication operations (which are essential to financial and DRM transactions, among others), are reduced from seconds to milliseconds.

This capability is provided by both MIPS Technologies and msystems and supported by msystems as part of the MIPS Ecosystem. Importantly, the solution is available with any MIPS CPU cores.

Conclusion

Security requires a system-wide approach and is all about the ecosystem. A system is only as secure as its weakest link. With secure SoC software and hardware provided by MIPS Technologies, msystems, and TRANGO Systems, respectively, SoC devices can be made as secure as possible without the need for redesigning and rewriting code and introducing more costs. This collection of superior technologies is presented to the SoC designer in an integrated fashion, for simplicity and “out of the box” ease of use.

A core designed from the ground up for security provides the best platform for these additional technologies and enables the design of secure systems-on-a-chip capable of running backward- and forward-compatible applications. Only a system-wide approach can make the next generation of devices truly secure.

For more information:
Albert Chiang
650-567-7088
albert@mips.com