WP429 (v1.0) May 20, 2014

TrustZone Technology Support in Zynq-7000 All Programmable SoCs

By: Yashu Gosain and Prushothaman Palanichamy

Embedded systems are becoming more and more vulnerable to unauthorized penetration, in many cases due to preventable weaknesses within the system kernel itself — often a simple lack of appropriate security features and protections that could have been designed in to safeguard the integrity of important data and processes. This dangerous situation is compounded by the fact that each device becomes potentially connectable to other devices outside its intended functional space, making use either of open Internet connectivity or other contrived digital transport strategies.

This white paper describes how the ARM® TrustZone® architecture and technology can be applied to protect custom IP created in Xilinx® Zynq®-7000 All Programmable SoCs.

Introduction

It is actually quite easy to invade and infect a standard, Internet-connected system with a malware payload. Search engines, making use of a variety of easily applied filters, can reveal the IP address of a machine running specific exploitable software; additional online tools can then be employed to identify vulnerable access points to the machine and deliver a target-specific malware payload directly to the platform.

As an example, smartphones have evolved into open platforms with the ability to download a variety of user applications from the Internet. These non-secure applications must often run side-by-side with high-value services like remote bank account management systems. Embedded system designers are being continually challenged to provide security for systems at low cost without compromising easy usability.

ARM, the industry's leading provider of embedded microprocessors, provides the TrustZone framework that designers can implement to protect the embedded system against potential security threats. System designers using TrustZone technology can configure a range of capabilities to provide specific functions and achieve specific goals within a secure environment. Through the creation of appropriately secured software running within a well-designed hardware system architecture, sensitive data remains safe, no matter how hostile the system's operating environment might be.

Xilinx has incorporated the ARM TrustZone technology into the Zynq-7000 All Programmable SoC (AP SoC), a processor-centric platform that provides software, hardware, and I/O programmability in a single device. Like traditional SoCs, the processor-centric approach allows the processor to boot first. At the same time, this approach also allows control and partial reconfiguration of the programmable logic by running software on the processor. This enables the user to optimize system performance and power management to meet varying operating environments.

The Zynq-7000 AP SoC architecture integrates a feature-rich dual-core ARM Cortex™-A9 MPCore™-based processing system (PS) along with Xilinx FPGA programmable logic (PL) in a single device, built on a state-of-the-art high performance–low power (HPL) 28 nm high-k metal gate (HKMG) process.

This white paper describes how developers can use TrustZone and TrustZone-related features available in the Zynq-7000 AP SoC processing system, programmable logic, and software ecosystem to improve security in custom embedded systems.

ARM TrustZone Architecture

The ARM TrustZone architecture makes trusted computing within the embedded world possible by establishing a trusted platform, a hardware architecture that extends the security infrastructure throughout the system design. Instead of protecting *all* assets in a single dedicated hardware block, the TrustZone architecture runs specific subsections of the system either in a "normal world" or a "secure world." Such an approach, when combined with software designed to leverage its advantages, enables creation of an end-to-end security solution that includes functional units as well as debug infrastructure.

In the Zynq-7000 AP SoC, a normal world is defined as a hardware subset consisting of memory regions, L2 cache regions, and specific AXI devices. In a normal world, non-trusted software can be limited to an environment that prohibits its access or even its awareness of the additional hardware dedicated to the support of the TrustZone architecture in the secure world. Trusted applications that run on a TrustZone-based system that implement a secure world (trusted execution environment) separated

from the main operating system (OS) protect the potentially vulnerable embedded system from software/malware based attacks.

Zynq-7000 AP SoC TrustZone

The Zynq-7000 AP SoC provides enhanced system-wide security by integrating the TrustZone framework into the ARM processor, interconnects, and system peripherals in the processing system (PS). The Zynq-7000 AP SoC's programmable logic (PL) is tightly integrated with the processing system and provides AXI interconnect soft IP that can be used to configure the PL IP for a Secure or Non-Secure mode.

When using TrustZone technology, the system designer must carefully consider all hardware security options early in the initial design phase so that protection can be built into the system from the outset. Figure 1 shows a trusted application and a non-trusted application residing on the same Zynq-7000 AP SoC device. The system uses the Zynq-7000 AP SoC TrustZone implementation to isolate these two applications.

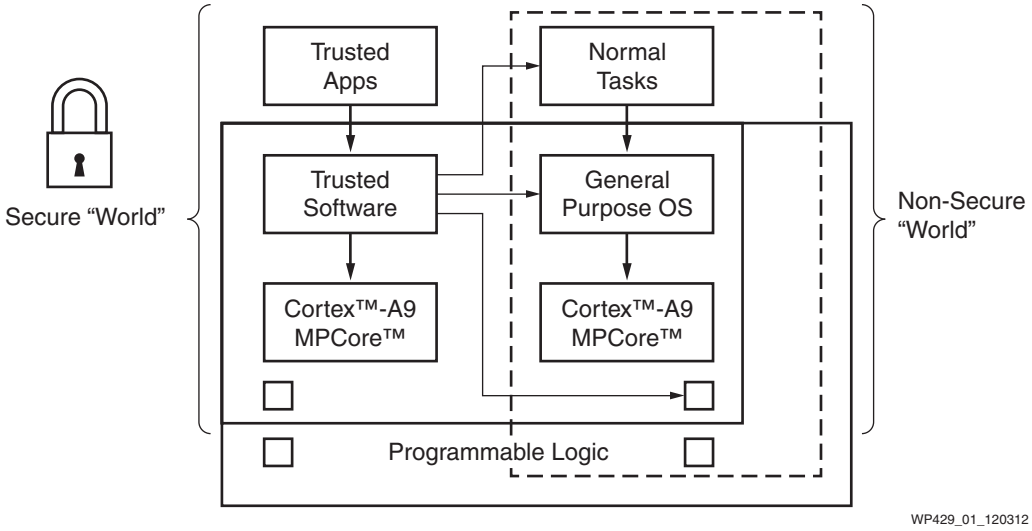

Figure 1: **Trusted and Non-Trusted Applications on a Zynq-7000 AP SoC**

For detailed information on Zynq-7000 AP SoC architecture, refer to UG585, *Zynq-7000 AP SoC Technical Reference Manual*.

AMBA AXI TrustZone Technology

Within complex embedded system designs, both data interconnect and system components are often combined to provide the mechanisms that protect against illegal access attacks.

For ARM-based, TrustZone-enabled systems, the AMBA® AXI interface specification includes an additional control bit for each of the read and write channels on the main system interconnect. These bits are known as Non-Secure (NS) bits (see Figure 2).

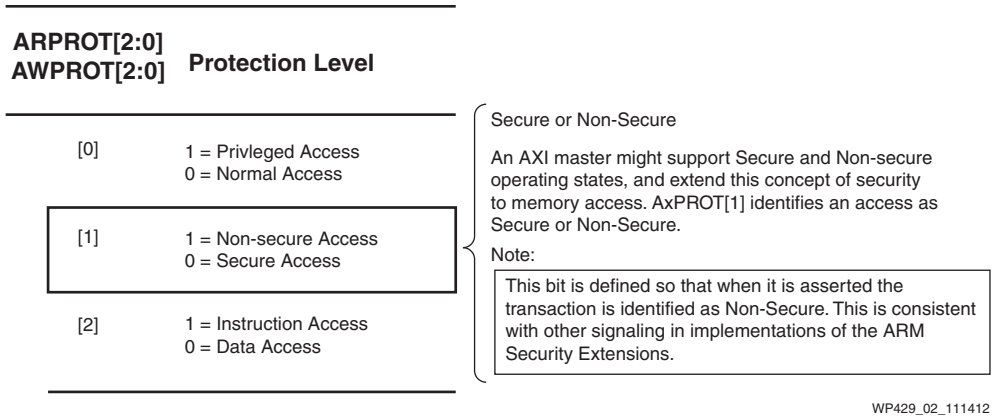

Figure 2: **Secure/Non-Secure Bit: ARPROT[2:0] (Read) and AWPROT[2:0] (Write), Bit [1]**

During a transaction, all masters assign an appropriate value to these signals, and the interconnect or slave decode logic must interpret them to ensure that the required security separation is not violated. All Non-Secure masters must have their NS bits set High in the hardware, which makes it impossible for them to access Secure slaves.

If a Non-Secure master attempts to access a Secure slave, the implementation defines whether the operation fails silently or generates an error. An error can be raised by the slave or the bus, depending on the hardware peripheral design and bus configuration. Consequently, a slave error (SLVERR) or a decode error (DECERR) can occur.

For more details, refer to UG761, *AXI Reference Guide*.

Support for TrustZone Technology in the Zynq-7000 AP SoC

The Zynq-7000 AP SoC is divided into two domains, a processing system (PS) and a programmable logic (PL) domain. The PS consists of a dual-core ARM Cortex™-A9 MPCore microprocessors, its peripherals, and its interconnect resources, which are provided as hard custom blocks in silicon; the PL consists of programmable FPGA fabric. The Zynq-7000 AP SoC supports ARM TrustZone technology in both the PS and PL domains of the device.

The PS provides a set of configuration registers related to TrustZone support for all hard custom blocks. These configuration registers can be dynamically programmed by the software during execution.

In the PL, a security-checking feature is provided for each master interface (MI) slot in the AXI interconnect IP. Using the Xilinx XPS tool, AXI interconnect MI slots can be assigned a static Secure or Non-Secure status.

All slave IP cores instantiated in the logic can be individually assigned a Secure or Non-Secure designation. For Xilinx slave IP cores, Secure/Non-Secure configuration can be designated at the AXI interconnect level because AWPROT[1] and ARPROT[1] bit checking can be enabled/disabled. For third-party slave IP cores, security bit checking can be performed in the IP core itself, or it can be statically done at the Xilinx AXI interconnect level.

Xilinx master IP cores instantiated in logic initiate only Secure transactions, as these IP cores drive AWPROT/ARPROT signals to logic zero.

TrustZone Support in the Zynq-7000 AP SoC Processing System

Each of the ARM processor cores in the Zynq-7000 AP SoC PS domain provides separate NS bit configuration for Secure/Non-Secure mode selection. The NS bit is defined in the Secure Configuration Register (SCR) in coprocessor CP15. By default, the NS bit for each processor core is set to zero, which means that both cores are in Secure mode. To change the processor mode, software should modify the NS bit. Although all Secure privileged modes can access the NS bit, it is strongly recommended to only use the Secure Monitor to change the NS bit.

Software can enter "Secure Monitor" mode by executing the SMC (Secure Monitor Call) instruction.

Secure Monitor mode is a privileged mode and is always Secure regardless of the state of the NS bit. The Secure Monitor is code that runs in Secure Monitor mode and processes switches to and from the Secure world. The overall security of the software relies on the security of this code along with the Secure boot code. All other modes of the processor core except the Secure Monitor can operate in either the Secure or Non-Secure worlds; therefore, both Secure and Non-Secure user modes can exist, as well as Secure and Non-Secure privileged modes.

In software terminology, the NS bit determines whether software execution is in the Secure world or the Non-Secure world.

In addition to the ARM Cortex-A9 core, the Zynq-7000 AP SoC PS also provides a Secure/Non-Secure configurable option for all the hard I/O peripherals and AXI interconnects. The TrustZone control registers defined in the PS can be used to configure the Secure or Non-Secure mode for the following PS devices:

- All I/O Peripherals (IOP)
- OCM RAM
- DMA Controller and Interrupts
- DDR Controller
- All PS Interconnects to PL:
  - General-Purpose (GP) Master/Slave Interconnects
  - High-Performance (HP) Slaves
  - Accelerator Coherency Ports

All these registers are dynamically configurable by the software during execution. By default, all hard I/O peripherals and AXI interconnects are set to Secure mode. As Secure devices, they have access to all Zynq-7000 AP SoC hardware and effectively operate as if the TrustZone architecture were not present. Boot software can configure them during initialization, or they can be modified at any time during software execution.

For example, each bit in the TZ_DDR_RAM Register defines a specific 64 MB region of memory space in DDR as Secure or Non-Secure. Similarly, all other devices have registers that can be used to define the security mode.

Refer to UG585, *Zynq-7000 AP SoC Technical Reference Manual* for a detailed description of the different PS blocks. In addition, Xilinx FAEs can provide TrustZone specific register information.

TrustZone Support in Zynq-7000 AP SoC Programmable Logic

In addition to the PS, the Zynq-7000 AP SoC includes FPGA programmable logic (PL). Designers can program the PL with Xilinx soft IP or with custom IP; these IP cores are typically connected via a memory-mapped AXI interface. This section covers Xilinx soft IP support for TrustZone technology at the AXI interconnect level as well as at the master/slave IP level.

Xilinx AXI Interconnect IP Support for TrustZone Technology

All Xilinx soft IP cores are AXI4 compliant, and Zynq-7000 AP SoC PS AXI interfaces to PL are AXI3 compliant. The designer must instantiate an AXI interconnect IP core in the PL to connect any of the soft IP cores in the PL with any of the PS interfaces.

The Xilinx AXI interconnect IP provides an (optional) Secure bit-checking feature that is used to facilitate support for TrustZone technology in the PL. This feature is present in the `axi_interconnect_v1.xx.a` version of AXI interconnect IP in the XPS tool. By default, Secure bit-checking is disabled. In this case, the AXI interconnect ignores the AWPROT [1] and ARPROT [1] bits generated by the master IP in PL and passes the transaction to the slave IP.

During system creation, the system designer can statically enable or disable the Secure bit-checking feature for each of the master interfaces in the AXI interconnect. When the Secure feature is enabled on an AXI interconnect master interface (MI), the AXI4 interconnect IP issues a DECERR as a response when a master IP connected to it initiates a Non-Secure read/write transaction. In such a configuration, the AXI interconnect will not propagate any Non-Secure transactions.

Figure 3 illustrates a system with the Secure feature enabled or disabled at the AXI interconnect level.

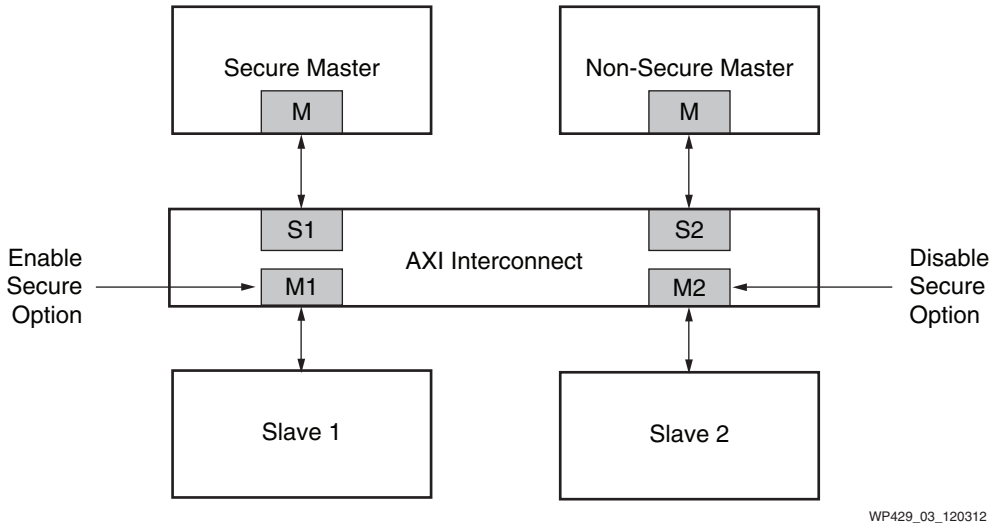

Figure 3: **Enabling/Disabling the Secure Feature at the AXI Interconnect Level**

By enabling the Secure option at interconnect master interface M1, any Non-Secure transaction from a Non-Secure master is blocked by issuing a DECERR response, and the Secure transaction from the Secure master passes through to Slave 1.

In addition, by disabling the Secure option at interconnect master interface M2, Secure as well as Non-Secure transactions to the slave are passed through. Both a Secure master and a Non-Secure master can access Slave 2.

Xilinx AXI-Compliant Master IP Support for TrustZone Technology

The Xilinx AXI-compliant master IP cores for the Zynq-7000 AP SoC drive AWPROT[2:0] and ARPROT[2:0] to zero internally. This means that any transaction from a Xilinx master IP core is a normal Secure data-access transaction. Designers must be aware that the Xilinx master soft IP cores provide no option to configure the AWPROT and ARPROT bits, either statically or dynamically, for Secure/Non-Secure modes. In practice, however, this can have minimal or no impact on the system design because it only affects the Xilinx MicroBlaze™ processor IP and different type of Xilinx DMA IPs cores.

Xilinx AXI-Compliant Slave IP Support for TrustZone Technology

All Xilinx AXI-compliant slave IP cores ignore AWPROT[1] and ARPROT[1] bit-checking during a transaction. Whether a transaction is Secure or Non-Secure, Xilinx slave IP cores respond to the transaction irrespective of the state of AWPROT[1] and ARPROT[1].

To provide TrustZone features to a system using Xilinx slave IPs, the system designer must set the Secure bit-checking feature on the AXI interconnect appropriately. By doing so, the interconnect can block any illegal access transactions generated by a master to a slave and respond back to the master with a DECERR on the bus. Only legal transactions from master to slave IP are passed through.

Zynq-7000 AP SoC TrustZone Hardware Architecture

Figure 4 shows a block diagram of a conceptual system using Zynq-7000 AP SoC TrustZone technology.

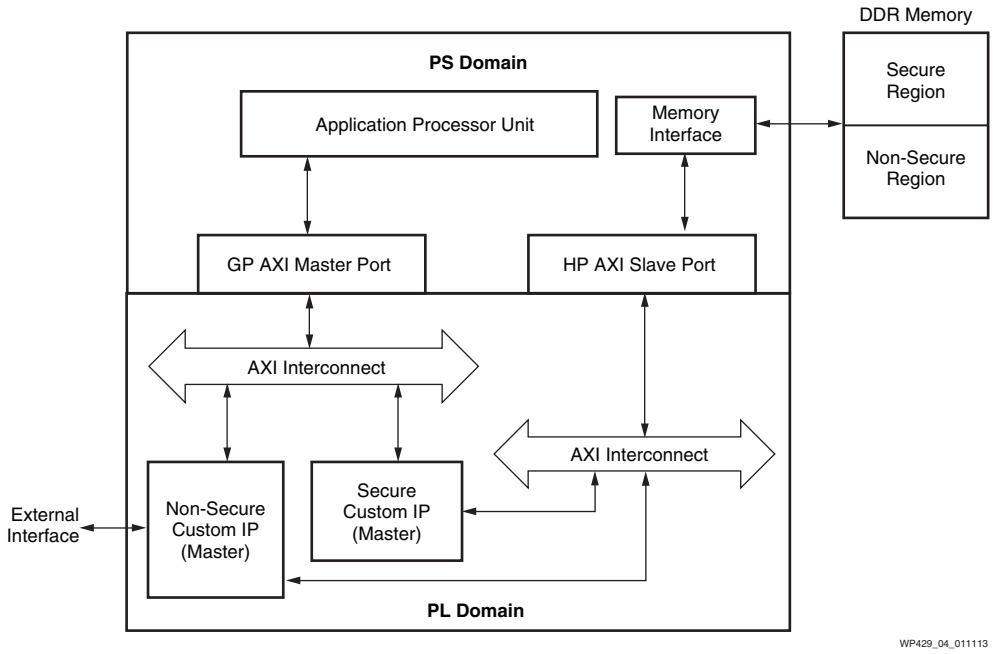

Figure 4: **Conceptual System using Zynq-7000 AP Soc Technology**

This is a conceptual system showing how to secure private or sensitive data in the system from illegal hardware access by using Zynq-7000 AP SoC TrustZone technology.

In this system, the PL domain uses two custom master IP cores:

- **Secure Custom IP:** This performs Secure read/write transactions to DDR using the HP slave port in the PS. It is also connected to the Application Processor Unit (APU) via a GP master port for register configuration.
- **Non-Secure Custom IP:** This is used to perform read/write transactions from/to the PS DDR upon requests from the "external world." It performs Non-Secure read transactions to DDR using an HP slave port. Configuration of this IP is done by the PS processor through a GP master port.

Upon power-on, the PS processor initializes both custom IPs, configures registers to establish Secure and Non-Secure regions in DDR memory, and transfers private data/instructions to the Secure DDR region.

After initialization and upon receiving a data request from the external interface, the Non-Secure custom IP first copies the data from the external interface to the Non-Secure region of DDR memory. It then interrupts the PS processor, which commands the Secure custom IP to perform the appropriate data computations using its private data/instructions in conjunction with the data just copied to the Non-Secure region of DDR memory. After computation is completed, Secure custom IP puts the computed data into the Non-Secure DDR region and interrupts the PS processor to command the Non-Secure custom IP to start transferring data from the requested location.

If an illegal data request from the external interface attempts to access the DDR Secure region through a Non-Secure custom IP read/write transaction, an AXI BUS error response is generated.

Zynq-7000 AP SoC TrustZone Software Architecture

In a complex embedded system, software is partitioned into two different worlds: the Secure world and the Non-Secure world. The system developer usually differentiates these two worlds according to the sensitivity of the components in the system. Critical components — for example, components vulnerable to security breach or containing private or secret information — are placed in the Secure world; components having no critical impact on the security of the system are placed in the Non-Secure world. Differentiation is totally dependent upon the design choices made by the system developer. This architecture is shown in Figure 5.

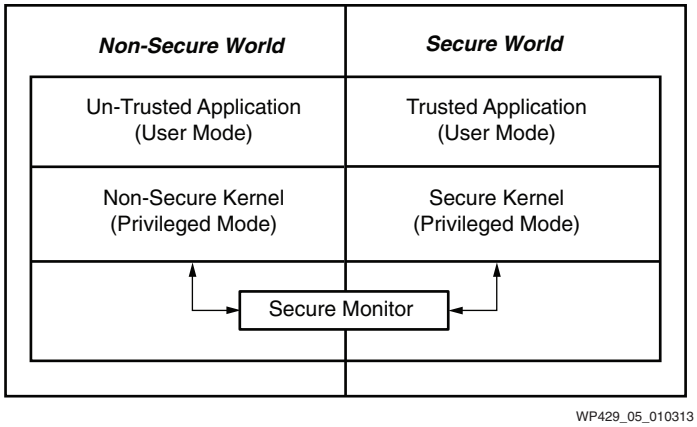

Figure 5: **Secure / Non-Secure System Partitioning**

Software in the Non-Secure world runs ordinary applications whose trust level is not designated through the Non-Secure kernel. The application is forced to run only in a Non-Secure hardware subset of the Zynq-7000 AP SoC and is physically prevented from accessing memory, cache, or devices that are located in the Secure world. By contrast, software in the Secure world runs trusted applications through the Secure kernel and is able to access *all* Zynq-7000 AP SoC system resources, essentially ignoring the Secure or Non-Secure designation of any hardware component. Non-Secure world software can access *only* system resources that have been designated as Non-Secure.

When a user process running in the Non-Secure world requires Secure execution, it makes a request to the Non-Secure kernel to enable the TrustZone Secure Monitor to transfer execution of the process to the Secure world. The Secure Monitor mode links the two zones and acts as a gatekeeper to manage program flow between them. Secure Monitor mode is a privileged mode and is always Secure, regardless of the state of the processor's NS bits.

As described earlier, when a user process in the Non-Secure zone tries to directly access Secure resources, an AXI BUS exception error is generated.

Secure Boot Flow

System security starts with the boot process. The on-chip BootROM code is highly critical because it must start the system in the Trusted state. The BootROM code starts the whole security chain by ensuring that first-stage boot loader (FSBL) is signed and verified.

Designers can select the asymmetric RSA and the symmetric AES/HMAC algorithm to authenticate the image. If the BootROM code fails to authenticate the image, the device executes a Secure system lock-down. The Secure Boot and TrustZone technologies complement each other: the first is responsible for the start of the Secure process, and the second maintains security on the running system by isolating Non-Secure applications.

For more information on Secure Boot, refer to UG585, *Zynq-7000 AP SoC Technical Reference Manual* (see the "Device Secure Boot" chapter).

Multi-OS and Software Stack Support on Zynq-7000 AP SoCs

The hardware security extension of the ARM TrustZone can be leveraged to create a hypervisor. Such a system can host multiple guest operating systems in addition to a Trusted Execution Environment (TEE). The TEE can be used to execute point-specific application stacks and is completely segregated from the regular software stack.

Complementing the support for ARM TrustZone on the Zynq-7000 AP SoC, Xilinx and its partners provide several other solutions that enable the concurrent execution of multiple software stacks, including: Linux + Bare metal AMP; Bare metal + Bare metal AMP, Linux + FreeRTOS AMP; Linux + GlobalPlatform Trusted Execution Environment, RTOS + General purpose OS combinations, and more. Xilinx Sales offices can be contacted for additional information related to specific product requirements.

Conclusion

The Zynq-7000 AP SoC provides a system security solution by integrating the TrustZone framework with the ARM processor, interconnects, and system I/O peripherals in the PS. It provides dynamically controllable TrustZone registers for all hard blocks inside the PS. Software can configure them during initialization, or they can be modified at any time during software execution.

On the PL side, Xilinx soft IPs provides static TrustZone frameworks at the AXI interconnect level. Depending on the system security requirements chosen, a system developer at the hardware level can assign appropriate security configurations to the PL AXI interconnect and execute the Security setting of the PS block at the software level. The Zynq-7000 AP SoC provides to the user with a flexible security solution for developing a robust and secure embedded system by using the TrustZone features provided on both the PS and PL sides. Xilinx also works with corporate partners to provide a comprehensive ecosystem for customers wishing to develop their own secure embedded systems using the TrustZone technology.

Related Reading

PRD29-GENC-009492C, *ARM Security Technology: Building a Secure System using TrustZone Technology,* white paper.

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
05/20/2014	1.0	Initial Xilinx release.

Notice of Disclaimer

Automotive Applications Disclaimer