NO CHIP IS AN ISLAND

OmniShield Technology: Critical Security for Connected Systems-on-Chip Design

January 2016

Analyst: Mike Feibus

in association with

Imagination

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Every time you turn around, it seems, somebody is adding network connectivity to a piece of hardware that didn't used to have it. Lathes and light bulbs. Cordless drills and dog collars. Hardly a week goes by without someone introducing more connected stuff.

And for products that already connect to the Internet, designers are adding more connection options – and more systems and applications that make use of them. Consumer electronics suppliers, for example, have been adding services to smart TVs and set-top boxes – everything from Hulu and Netflix to Facebook and Skype – as well as Bluetooth and Wi-Fi to supplement the traditional Ethernet connection.

Architects of these increasingly complex and capable products are beginning to integrate all those apps and systems onto a single chip. You might say that they are evolving from system-on-chip (SoC) design methodologies to multiple systems-on-chips design.

With all this as a backdrop, it's becoming apparent that in the new paradigm, no system is an island. Indeed, not even on-chip systems are islands.

For those who work to keep those products safe from attacks, it means their challenge is blossoming. And it's not just the sheer number of connected devices they have to protect. Many of these devices are vulnerable to attack in ways that IT managers are unaccustomed to fighting. They're typically not behind locked doors like servers in the datacenter. Devices that monitor exhaust fan performance, for example, might be sitting outside, exposed to the elements. They might even be in a location where they're vulnerable to screwdriver attacks.

Attackers, on the other hand, see opportunity. They enjoy for fun and profit stealing valuable digital assets by probing for the easiest way into networks. So the more connected systems there are, the more potential pathways to the valuable data, content or records they're chasing.

As well, connected devices like smart door locks and garage door openers are attractive targets for burglars who want easy access to jewelry, keepsakes and other valuables inside homes. And to make things more difficult, there is a lack of interoperability standards in place for secure communication between these devices. It's just this type of vulnerability that enabled attackers to hack into a Jeep's entertainment system, take control of crucial systems and run the vehicle off the road.

Fortunately, system(s)-on-chip designers have a new and promising set of technologies to tackle this escalating problem. It's called OmniShield from Imagination Technologies. OmniShield is an on-chip security architecture comprised of hardware and software technologies from Imagination. It gives engineers the power to isolate systems, assign resources, and also to police communications between systems using a pool of hardware-enforced firewall features.

Those are critically important capabilities, because together they form a potent counter to attackers' practices. Despite all the work devoted to keeping cyber thieves at bay, hackers are still remarkably successful at finding ways in.

What OmniShield provides is a foundation to thwart attackers' ability to hop from their newly secured beachhead to the critical systems and storage centers they're trying to reach. So even if attackers successfully penetrate the on-chip container that houses the most vulnerable system on the network, it doesn't buy them much because they're stuck there. It's as if they're burglars who've broken in through a window in the laundry room only to find that it's sealed off from the rest of the house. In this example, OmniShield would act to isolate the laundry room, and also as the security system, sounding the alarm so that the intruders can be safely removed.

As we shall illustrate, the protection that OmniShield provides isn't just about security in the traditional sense. It provides security in other ways, as well.

CONTEXT

What is OmniShield?

OmniShield is a unique set of enabling technologies designed to protect SoC designs. The foundational technology is built into Imagination's hardware IP, including its PowerVR GPUs, MIPS CPUs, Ensigma RPUs, and other processing technologies. Instantiating the technology in hardware is key to its effectiveness. Building on top of Imagination's 'OmniShield-ready' processors are a range of solutions including a Trusted Element (TE), trusted operating systems and trusted hypervisors for OmniShield. These tools make it easy to take advantage of the powerful OmniShield technology.

OmniShield is a unique solution for embedded systems that can:

- Establish multiple domains, or containers, on a single SoC (from two all the way up to 255 containers)
- Authorize access to on-chip resources – everything from on-board microprocessors and graphics processors to audio and communications controllers – as well as prioritize use for shared resources
- Allocate and manage service interrupts from external processors and peripherals, securely routing them to individual containers
- Manage and enforce the solidity of secure hardware with the flexibility and scalability of trusted softwarehow bad will the capacity crunch get? Let's run through the math.

Security Through Separation

The notion of isolation as a tool for mitigating damage and risk is not new. Shipbuilders, for example, have leveraged the concept for hundreds of years as a way to ensure that ships remain seaworthy throughout the toughest of storms and conditions. By dividing the ship's hulls into watertight sections, any water breaches will be contained to just one section. And the ship can sail on.

Likewise, firefighters construct fire breaks – strips of land that are free of trees, brush, leaves and anything else that might feed the flames – to help containerize brush fires. Manufacturers build firewalls in everything from automobiles to factories to cordon off flammable materials and operations. And the networking industry has adopted the network firewall concept - as well as the name – as a means to secure the network layer.

In fact, the computer industry has been containerizing network assets in the enterprise since the 1990s, when internal network installations and internet connectivity first became commonplace. At the time, IT deployed dedicated servers for all of the major services it provided, including email, data storage and web hosting. Eventually, the enterprise virtualized those physical containers onto a single server.

There is a similar consolidation underway in myriad other environments, where services and information are being consolidated into a smaller number of devices. In many areas this is happening at the chip level. In the automobile industry, for example, designers are pulling the dashboard, GPS and infotainment systems onto a single SoC. And OmniShield is central to enabling isolation of safety-critical functionality and services in such environments.

Today's embedded hardware-enforced IP alternatives offer a maximum of two containers: one for trusted applications and sensitive data, and one for everything else. But this means that all of the trusted applications and services reside in the same place – which, as we will illustrate, does not provide the level of isolation needed for next generation applications. Early OmniShield design activity centers on the three- to seven-container range. And with up to 255 containers available, designers have plenty of headroom now and into the future.

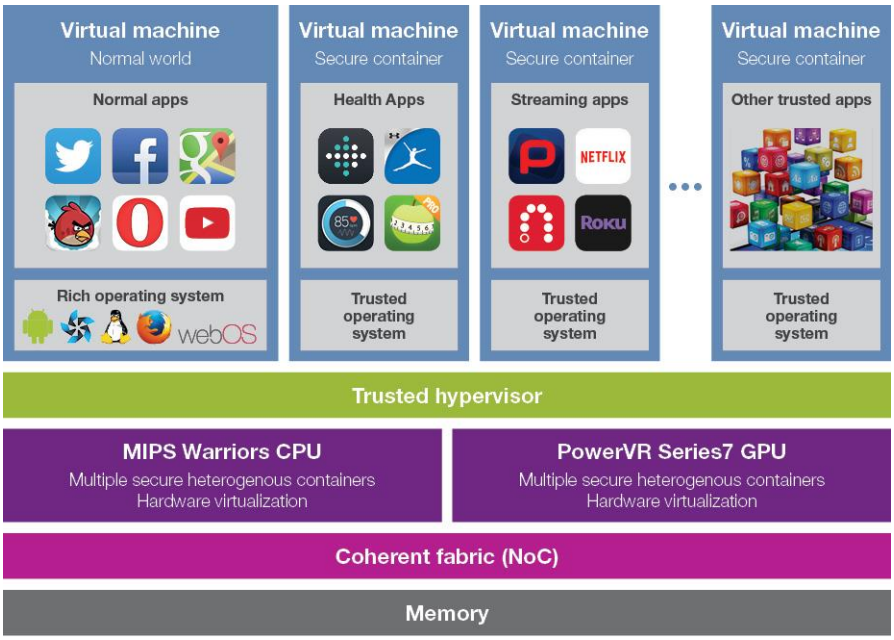
Resource Allocation

Through a piece of software known as the trusted hypervisor, OmniShield can assign exclusive permissions and rights to the CPU cores, graphics cores, other processors in an SoC.

In this process, it is essential to ensure that mission-critical systems or applications always have access to the on-chip resources they need to continue operating. The OmniShield-enabled hypervisor prioritizes access of shared on-chip resources to ensure that mission-critical systems operate as intended.

One of the most commonly-shared system resources is memory. It also happens to be one of the most vulnerable to attack. OmniShield is engineered to securely manage system memory access. The OmniShield-enabled hypervisor dynamically allocates memory between the containers, giving precedence to higher-priority services. It also polices demands from those containers, which is a powerful tool in identifying and neutralizing attacks. For example, OmniShield can detect when one container is trying to hog memory, which could mean that hackers are launching a denial-of-service attack. It could also mean that poorly managed software in one container is trying to take more than its share of memory, which would impact performance and cause application resource starvation in the other containers.

Next-generation platforms across many applications require heterogeneous operation of dissimilar processing elements (CPU, GPU, codecs, etc.) sharing a common memory subsystem. This means that a system must manage memory effectively, controlling access to not only the on-board host processor, but all processing elements in the system. OmniShield was built for managing memory and other resources in these heterogeneous systems.



Hardware Root of Trust

Attackers are always looking for the weakest link to penetrate a network. And once they gain access, they work their way toward critical systems and information.

The best way to guard against this type of attack is to anchor the platform in hardware. Indeed, the finest security schemes invariably pair soft authorization with a form of validation from the physical world. An example of this is needing to use a password and pass an iris scan in order to gain access to a building. Or swiping your credit card and entering your zip code in order to pump gas.

OmniShield not only controls access to the on-chip compute resources; it is also designed to control communication between the containers and will alert if a container with low-level authorization is behaving outside the expected boundary conditions.

Let's say, for example, that hackers gain access to a system through the Bluetooth connection to the FM radio app in your smartphone. Now that they control the radio, they might try to disguise it as an app with higher-level privileges to get closer to the data they want.

Use Cases

OmniShield offers the best combination of flexibility, security and control for a broad array of applications. Let's take a look at how designers in three market segments are deploying OmniShield-enabled solutions, though they are by no means the only areas that are developing with the technology.

Automotive

Electronics in vehicles are changing rapidly as designers are migrating several in-vehicle systems onto the same SoC, incorporating new systems in several distinct areas, including:

- Advanced Driver Assist Systems, or ADAS: automakers are integrating a host of new capabilities into this rapidly advancing arena. A growing number of vehicles already include backup cameras and lane-line detection. Newer features include blind-spot monitors, drowsiness detection, and obstacle recognition.
- Infotainment systems: In-system entertainment systems are multiplying, so that each passenger in the vehicle has their own. Each personal system needs connectivity, of course, along with the ability to sign on to passengers' accounts and download their personal information.
- Smart City data exchange: Metropolitan areas are gearing up to make use of real-time traffic conditions to help improve a number of services, including traffic light control, multi-directional rush-hour lane management and city-light administration.

Today cars have multiple different wireless connections. And with all the new systems that automakers are proliferating, the number is only destined to climb higher.

Automobile designers, who've already been migrating discrete in-vehicle electrical control units to SoCs, must cordon off the functionality of those systems into their own on-chip containers – ensuring separation from the ones that house mission-critical dashboard functions, driving controls and GPS navigation.

And as the auto industry moves more and more toward autonomous driving, managing communications between the containers is going to become far more complicated because critical systems will need to interact with each other. A hands-free driving feature, for example, will need real-time information from containers housing the GPS, municipal traffic services, on-board cameras and the dashboard so it can safely steer, brake, accelerate and avoid collisions. A hacker who managed to gain access to the hands-free driving container from, say, the

entertainment system, would have the power to cripple traffic, causing great damage to people and property.

In the summer of 2015, two researchers proved why it's so important to police communications between containers housing the various in-vehicle systems. In a demonstration for Wired magazine, they wirelessly hacked into a Jeep Cherokee's entertainment system, and then proceeded to take control of the vehicle's climate control, dashboard, transmission and brakes. With a laptop miles away, they were able to change the radio station and turn on the AC. Eventually, they took control of the critical systems and ran the Jeep off the road.

The demonstration sparked a recall by Chrysler of 1.4 million vehicles to patch up the vulnerability.

Of course, a system built with OmniShield-based technology could have isolated the attacker from entering the mission-critical controls of the vehicle, preventing the entertainment system from sending commands to containers with the vehicle's driving functions. In fact, an OmniShield-enabled SoC can be configured to raise a flag in such an event and let a higher-level trusted application clean up the compromised container by re-initializing the application and possibly reporting the intrusion.

Protecting against attackers is a top priority for automakers because the potential for lost lives and property damage is so high. Some are looking to OmniShield technology as a basis for creating containers for isolating systems, managing memory and other shared resources as well as watching over communication between the containers.

In fact, auto designers may one day find that they need to deploy the technologies that underpin OmniShield to be in compliance with the law. As a result of the Jeep hack, two US senators introduced a new bill requiring automakers to isolate critical systems from the rest of the in-vehicle network. With all the concern about the coming age of connected automobiles, the US law could be first of many globally.

Connected Home

Nowhere is the connectivity explosion more evident today than in the home. More services are coming in from the internet – everything from streaming content to home security and remote management. And on the other side of the home gateway, the number of connected devices exchanging data with cloud services is increasing significantly, both in number and in type. Consumers today are connecting more than just their PCs, tablets and smartphones. They're also hooking up set-top boxes, smart TVs, connected thermostats, webcams, motion detectors, lights and air conditioners.

Cable companies, telephone operators and other internet service providers who see all that data flowing into and out of the home gateway understand that they need a better way to isolate and protect the diverse interests of content providers, financial institutions and, of course, the consumers themselves. You might say that security is in the eyes of the beholder. Consider that:

- Consumers want privacy. Among other things, they fear that information from connected security systems and comfort controls, for example, could alert burglars when they're out of town.
- Content providers like NetFlix and Hulu need assurances that their audio and video streams are digitally protected.
- Financial institutions that enable consumers to pay for services in the connected home (and beyond) electronically demand that account and password data be secured.

Containerization on an OmniShield-enabled SoC can be a powerful tool for designers to isolate services and barricade sensitive data. If the systems have a root of trust anchored in the hardware that they can rely on to help identify and defeat attacks, then the permissions for those containers can't be changed.

There have been several widely-publicized attacks on connected home devices of late. And it's easy to understand why they are prime targets for attackers as they poke around the edges of a network to find the easiest way inside. These IoT edge devices can be attractive attack targets because many of them:

- Are comparatively simple devices, designed without much thought for security
- Have credentials to get deeper into the network
- Run with firmware that can be updated remotely

For connected devices like garage door openers and surveillance cameras, the need for security is obvious. But for devices like light bulbs and microwave ovens, the need may not be so apparent. But it's important to understand that all connected devices, simple or no, are all part of the attack surface. So they must be secured.

One method for protecting against an attack from a connected light bulb, for example, would be for the service provider to use an OmniShield-enabled system to set up a lighting services container on the gateway. Another way would be for the light bulb manufacturer to establish an identity container on the light bulb that OmniShield can use to monitor.

OmniShield can be used in ways that extend beyond traditional security, as well. For example, internet service providers can add containers to their home gateways for add-on services like home automation, security and cable TV. Rather than installing discrete security control hardware, they can add the capability remotely to a container in the gateway. Adding further containers allows a portfolio of differentiated services to be deployed and managed on the existing gateway hardware, enabling the customer to freely pick and choose which services they want, which in turn derives revenue for the operator.

Such an implementation would also eliminate the need to integrate and test large software stacks and disparate code bases, since the essential networking and routing functions of the gateway can be maintained separately.

Providers can also improve flexibility and mitigate risk by adding another container for new internet capabilities. That way, they can add state-of-the-art connectivity features into that container without the risk of destabilizing tried-and-true capabilities, which are in their own container. This is a great way to minimize returns and recalls as well as extend the life of deployed units.

Internet of Things

Internet of Things, or IoT, is a term applied to a broad set of products with built-in connectivity. Just to name a few: street lights, traffic lights, climate controls, security cameras, coffee makers, escalators, automated teller machines, shop lathes and air conditioners.

In addition, businesses and governments are deploying countless sensors to detect and measure real-world variables like motion, temperature, pressure and humidity, with multiple disparate systems beginning to tap into the so-called edge devices for information they can use to make decisions.

Security systems, for example, can allow access to in-building assets by comparing data from the edge devices with employee records. The devices can also feed predictive models that energy management systems can use to manage heating and cooling more economically. And factory-floor management systems can use the devices to help identify deteriorating parts before they fail.

From a systems design viewpoint, it is far more economical to integrate these and other management systems onto a single device. Of course, the systems must be isolated from one another. Imagine if hackers broke in through the HVAC system, and then migrated to systems that are more central to the business. They might try to infiltrate the security system and employee records. Or they might try to work their way into the electronic payments systems to steal credit-card numbers, passwords and other customer records.

To help safeguard against such attacks, designers can leverage OmniShield to build an SoC for in-building command-and-control separate containers to house the different systems, and then anchor credentials in hardware.

Designers have a strong incentive to establish multiple containers for security in even the simplest, single-function devices like light bulbs. For designers who build more complex products like command centers, employing an OmniShield-enabled system helps reduce risk for them in other ways, as well.

Designers working on products lines that have been around for years understand how dicey it can be to strike a balance between the safety of older, battle-tested firmware and riskier code for leading-edge features that keep the product line competitive. Long-time brands for everything from washing machines to mass-transit ticketing units appreciate how difficult it can be to strike a balance to ensure both reliability and performance.

With OmniShield, designers get the best of both worlds in their future devices. Rather than scrapping the legacy software for a more modern package, designers can play it safe by deploying additional containers to house the latest features. That way, designers can maintain reliability by keeping the legacy code in their own containers.

Designing products this way can help cut costs by decreasing the need for in-field updates and repairs. For products with features that are developing quickly, deploying multiple containers for your service would enable over-the-air updates with much lower risk. That, in turn, could extend the practical life of the device.

Using OmniShield to establish containers for optional features as well as code that's unique to specific countries' regulations will dramatically lower the cost and hassle of certifying systems. With OmniShield, control system vendors would only need to submit one box for approval. That's far cheaper and less time-consuming than submitting boxes for every possible combination of features.

RECOMMENDATIONS

The number and type of connected devices is exploding, and with that comes the promise for a world that is much more convenient, efficient and fun than it is today. At home, our connected devices and clothing might help us spot early signs of health conditions before they become problems. And at work, sensors on the factory floor can alert us to changes in sound, vibration and temperature – all signs that production-line equipment needs service to avoid a failure.

Hand in hand with all that promise is a world that is more exposed to attack than ever before. Indeed, security in the connected age is about protecting far more than valuable data like credit-card numbers and passwords. As if that isn't difficult enough to guard against. Hardly a week goes by without reports of a new highly-publicized data breach, each of which costs the victim-companies hundreds of millions of dollars or more to clean up.

Indeed, attackers see newly-connected devices as potential portals into all aspects of our lives and our livelihoods. If compromised, for example, smart door locks and garage door openers can help burglars break into our homes. As well, connected appliances and security systems can tell them when we're away.

Attackers also have more ways to attack, because these devices aren't typically under lock and key like corporate servers. And someone doesn't typically have a hold on them like we do with our laptops, tablets and smartphones. Smart water meters and surveillance cameras, for example, may be attached to a wall outside, accessible from the street. So attackers who want to inject malware, for example, can physically break into the devices.

The best way to protect against all these types of attacks is with a security system that is built into embedded hardware at the SoC level. And OmniShield is uniquely qualified to provide this level of security.

Indeed, OmniShield isn't just another technology for on-chip security. It's an architecture that enables this revolution in chip design for the connected world. OmniShield is the best solution to protect against attackers because it gives designers:

- The ability to establish multiple containers on-chip
- Enforce access to shared heterogeneous resources, like memory, graphics and communications
- Manage and enforce it all with an anchored root of trust

OmniShield's capabilities give designers security in other ways as well. For example, they can reduce risk by adding additional containers to their SoC designs. That way, they can avoid costly in-field replacements by employing the containers to add security updates or improve performance. They can also use containers to add new services as they become available, which can help reduce risk by extending the life of their designs.

As well, designers can use containers to help reduce inventory risks. Rather than stocking three models in a product family, for example, an internet service provider could carry a single device, and charge more when they populate containers with advanced features like channel bonding or support for Multimedia over Cable Alliance (MoCA) technology.

It should be apparent by now that the new paradigm that a connected world brings also requires a new paradigm for security. Chip-level security is an absolute must for connected devices deployed in the field. And OmniShield is an SoC security architecture that is uniquely able to protect multiple systems-on-chip for connected devices.

How Do I Access OmniShield?

If you're a SoC designer, contact Imagination to find out more about its Omnishield-enabled hardware and software technologies. If you're a systems OEM, chips leveraging OmniShield technology are already in the market from Imagination licensees.

https://imgtec.com/platforms/omnishield/

Mike Feibus is Principal Analyst at TechKnowledge Strategies, Inc., a market research and consulting firm that provides clear, critical and independent insight to technology buyers and suppliers. Reach him at mikef@feibustech.com.

TechKnowledge Strategies, Inc.

P.O. Box 25685

Scottsdale, AZ 85255

www.feibustech.com

+1-480-922-3244