Decoupling Form from Function in Intelligent Devices

The End-User is the Winner

General Dynamics

Carl L Nerup, Vice President, Global Business Development

Dr. Daniel Potts, Vice President of Engineering

Kim Scott, Director of Secure Mobility Products

Citrix

Rich Persaud, Director, Program Management, Client Virtualization

Samantha Foster, Sr. Director, Market Development, Client Virtualization

Version 0.7.2

OCTOBER 2013

Table of Contents

Executive Summary

The Smartphone (R)evolution

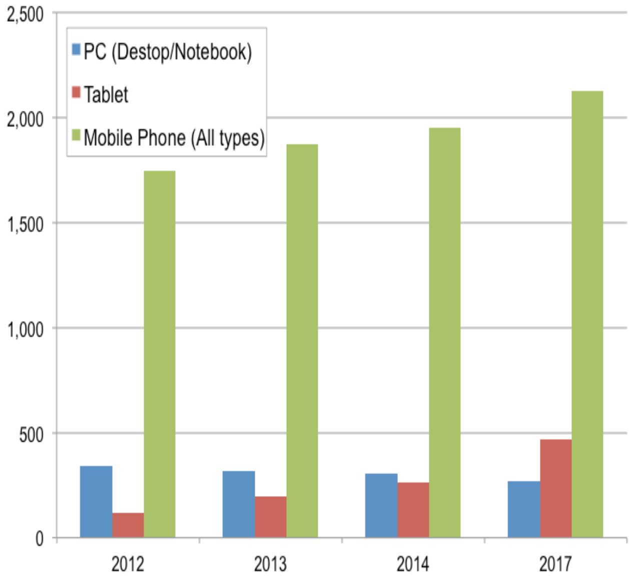

Figure 1. Shifting Device Shares 2012-1017
Gartner – April 2013 (millions of units)

Global smartphone penetration has climbed from under 35% in 2011 to topping 60% in 2013 (comScore). Total shipment volumes are expected to reach 865 million units, up 32% from 2012 (Digitimes Research). Global tablet growth is comparably aggressive, up 59% from 2012 to a projected high of 229 million units this year (IDC). By contrast, the PC market is in its fifth year of steady decline, down 11% for 2013 (Gartner).

These trends do not simply indicate a market shift from desktop to mobile devices. Rather, they point to a deeper paradigm shift away from a one-size-fits-all approach to personal and professional productivity, to one that reflects financial realities, personal preference, and ability of different types of devices to address real-world use cases.

In that vein, smartphones, tablets, notebooks, and other intelligent devices are converging into a broader definition of platforms. These platforms are defined less by visible form factor and more by the various missions they fulfill.

A key aspect of this convergence is the end of specialization: desktops and notebooks no longer “own” the domains of spreadsheets, presentations, development, gaming and other display-intensive applications; mobile phones continue to enable the core functions of voice and text messaging, but also join desktops and tablets in enabling the gamut of personal and professional use.

Decoupling Form and Function

Once upon a time, the function of a device dictated the form. If consumers wanted to take pictures, they bought cameras. When consumers wanted to talk on the go, they bought cell phones. If consumers wanted to play games, they bought gaming consoles. To be productive at work or at home, employers and consumers acquired desktop PCs and notebook computers.

Function followed form, clear across leisure and work activities, creating distinct product categories.

Today, form and function have been neatly teased apart. Mobile phones boast integrated picture taking with specs and capabilities that trump most point-and-shoot legacy cameras. Notebooks, tablets and smartphones let users play games on par with everything but high-end gaming

Who Should Read This White Paper

This white paper and the architecture it describes will be relevant to anyone with an interest in mobile system software. In particular, the information presented in the following chapters will benefit

- *C-level technologists and product / solutions architects*
- *Mobile software and hardware product managers*
- *Others with an active interest in building smarter, more secure and future-proof devices*

consoles. And workers are no longer tied to their desks, instead exchanging e-mail, composing documents and accessing apps from smartphones and tablets.

As end-users become accustomed to choosing form and function(s) of devices to enable their professional and personal lives, it creates both opportunities and challenges for the consumer electronics and information technology industries.

The Long Tail of Convergence

Building PCs and mobile devices began as comparable exercises, but time and commoditization led the two in very different directions. At the birth of the PC marketplace, a select set of manufacturers (led by IBM) ruled the day, defining the hardware and software, and owning the entire value chain, from design to delivery. Over time, the PC itself became commoditized, with value migrating to the supply of core components (OS, CPU, memory, storage, etc.) and to brand, channel, and an independent software ecosystem.

Until recently, mobile devices represented a comparable concentration of added value: handset OEMs designed and built their wares with proprietary hardware and software, presuming to add value through careful integration of miniaturized physical devices with their own operating systems and applications. Ironically, the challenge of building high-end devices – smart phones and tablets – is leading to mobile commoditization comparable to white-box PCs. To build these high-margin, high functionality devices, mobile OEMs have turned to third parties for silicon, displays, storage, and most recently for operating systems and application software.

Unlike the PC market, integration is still the measure of mobile added-value. But similar to PCs, it is increasingly difficult to use traditional design and development techniques to deliver devices that satisfy even a single segment, let alone meet the needs of entire markets.

Meeting this “long-tailed” challenge requires rethinking device architecture to embrace this convergence.

Enabling Platform Convergence

This purpose of this white paper is to introduce the reader to design techniques and a system software architecture that acknowledges these truths and helps device manufacturers and their ecosystem partners define, design, build and deliver converged devices.

A few basic truths underlie and drive today’s convergence of computing platforms and form factors:

- Size matters, but not like it used to
- Complexity is in the eye of the beholder
- Operating systems are enablers, not universes unto themselves
- Functionality is increasingly determined by end users, not by manufacturers

Size

Today’s smartphones and tablets boast computing power only found in desktops and servers just a few years ago. Mobile devices also defy conventional wisdom that limits certain applications to particular form factors – end users expect voice communications from their PCs and notebooks and increasingly compose documents, edit images and run financial software on mobile devices.

Complexity

Growth in software complexity long ago outstripped comparable hardware evolution. Mobile software now boasts tens of millions of lines of code (MLoCs) at all levels, from firmware to OS to applications. The best way to tame complexity is through abstraction, not by making it someone else's problem but by letting appropriate ecosystem participants each apply their hard-won expertise in a multi-layered hardware and software "stack."

Operating Systems

The OS wars are over. It turns out that nobody really won. Instead, each OS has its fans along with a set of functions and a portfolio of applications. And thanks to technologies like virtualization, device makers needn't place their bets on a single OS any more.

Functionality

End users will always surprise suppliers by finding novel ends and purposes for devices. Instead of endlessly sub-segmenting the mobile marketplace and nervously gazing into crystal balls, device manufacturers should strive to build flexible and configurable devices to accommodate the long and growing tail of real-world applications.

The Evolving Device Marketplace

General Dynamics and Citrix address a marketplace that is rife with contradictions. On one hand, device OEMs – manufacturers of mobile handsets, tablets, automotive systems and other intelligent devices – invest hundreds of millions of dollars annually in research and development of new mobile and embedded technologies. Today's devices feature brighter, denser displays, and faster, lower-power multi-core CPUs. These new higher bandwidth wireless interfaces and dedicated multimedia engines, and software applications are critical to enable end-users enjoy those features and the ecosystems surrounding them to monetize them. On the other hand, system software architecture reflects design thinking that's decades old, that accommodates but barely leverages the capabilities of underlying hardware and in many cases holds back and adds complexity to the applications and enabling software that truly determines the user experience.

Function Still Drives Device Design

To accommodate the decoupling of form and function, device manufacturers continue to strive to integrate capabilities in demand from a dynamic marketplace while also optimizing the costs associated with the BOM (Bill of Material) to preserve profitability.

In a historical analogy to the PC business, mobile devices (smartphones, tablets, etc.) are trending towards commoditization. The nexus of commoditization, instead of the PC motherboard, is the SoC (System on a Chip).

The real shift then is from fully custom handset and tablet design methods to platform based concepts that enable multiple functions irrespective of the form factor. This shift, in both hardware and software domains, enables re-use and also enables OEMs and ecosystems around them to act with increasing degrees of agility critical for success in markets with shrinking product life- and deployment cycles. The mobile mantra is no longer to "build a better mousetrap," but instead to build one that serves today's and tomorrow's applications, across regions and industry verticals.

Designing to Meet Technology Roadmaps

One aspect of maximizing functionality independent of form is enabling devices to run two (or more) different operating systems, across a range of chipsets. In current-generation devices, a device might deploy one or more instances of Linux and/or Android; in a future generation, a different set of operating systems.

Comparably, a device shipping today might embed an available chipset, but would benefit from migrating to more powerful CPUs and higher integration in future derived product line SKUs.

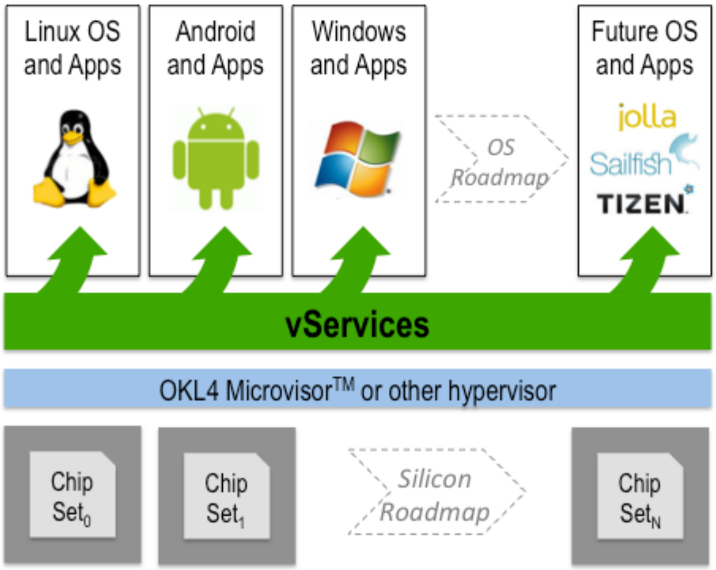

Figure 2. – Designing devices to meet future tech roadmaps

Virtualization, a Ubiquitous Technology

In the past 2-3 years, embedded chipset suppliers have begun to integrate IP and capabilities previously only found in datacenters and robust desktop systems: multicore CPUs, GPUs, sophisticated memory management and hardware support for virtualization.

When most readers encounter the term “virtualization”, they think of:

- Datacenter and cloud-based technology for enabling provisioning and resource scaling
- Desktop software to let Windows users run legacy operating systems or to let Mac OS users run Windows or to run other operating systems (Linux, BSD, etc.) and applications on top of them

However, CPUs found today in smartphones and tablets are every bit as capable of supporting virtualization as PC-based equivalents, with analogous applications in mobile and embedded systems.

Who Needs Virtualization?

Mobile / embedded virtualization may seem like overkill, but real-world requirements drove development of embedded hypervisors and the integration of virtualization support into embedded CPU architectures. These requirements include needs for:

- Stronger isolation among software components for secure and certifiable devices
- Support for in-place re-hosting of existing embedded software, especially legacy RTOS-based software stacks and pre-certified baseband stacks
- Consolidation of multiple CPUs and disparate software stacks onto a single multi-core SoC, to cut costs, improve performance, and optimize energy consumption
- Simultaneous hosting of multiple operating systems and multiple instances of one OS for “multi-persona” devices and to support trusted computing and enterprise mobility

Impact on and Support from Silicon Architectures

These and other requirements have led to new trends in silicon sourcing and chipset design:

- Deployment of desktop/datacenter CPUs in embedded applications, e.g., x86/IA silicon in automotive designs, leveraging software interoperability and Intel ® Virtualization Technology (VT)
- Reinvention of the Intel® Architecture, embodied in Intel® Atom™ family CPUs, to address energy and thermal requirements of mobile and embedded applications
- Integration of hardware support into the leading mobile/embedded ARM architecture, starting with ARM Cortex-A15
- Introduction of comparable virtualization support in other embedded processor families, e.g., Power Architecture, MIPS, Xtensa, et al.

GD Connect™ for Next-Generation Smart Devices

Part of General Dynamics' GD Protected™ family of software and applications for securing mobile communications devices, GD Connect services help manufacturers (OEMs) and integrators rapidly architect and build high assurance mobile phones, tablets and other intelligent devices. In particular, GD Connect services support creating virtualized devices that deploy multiple operating systems in an architecture promoting isolation, controlled sharing and policy-based management of resources.

GD Connect is provided as a set of reusable software components, offering a rich framework for virtual machine-hosted software to communicate and share resources (memory, peripherals, etc.) in a controlled and secure manner, based upon well-defined management policies.

Devices deploying GD Connect services deliver a range of capabilities and benefits to device OEMs and end-users alike:

- Support for ARM and Intel CPU architectures
- Transparent hosting of both industry-standard and specialty operating systems – Linux, Android, Windows and popular embedded RTOS platforms
- Independence from guest operating systems and the ability to work with lightweight execution environments (no OS)
- Interoperability with General Dynamics' OKL4 Microvisor, Xen and other Type I hypervisor implementations.
- Strong isolation among execution environments for high assurance and security
- Architecture for abstracting and sharing peripherals across virtual machines
- Mandatory APIs for fine-grained policy control over access to shared resources – memory, peripherals, IPCs, etc.

Virtualization Landscape

Even as leading silicon architectures integrate support for virtualization in hardware, the role of the hypervisor remains central to the success of converged device design. Let's look at two virtualization platforms: the OKL4 Microvisor from General Dynamics and the XenClient client virtualization solution from Citrix:

OKL4 Microvisor

General Dynamics offers designers of converged systems the OKL4 Microvisor, designed from the ground up as a mobile virtualization platform. A microkernel-based embedded hypervisor - called a microvisor, OKL4 imposes a very small footprint and the right combination of performance and CPU support to target mobile telephony.

The OKL4 Microvisor is distinguished by supporting mobile virtualization, componentization, and security, enabling a new generation of applications and capabilities with impact across the mobile ecosystem.

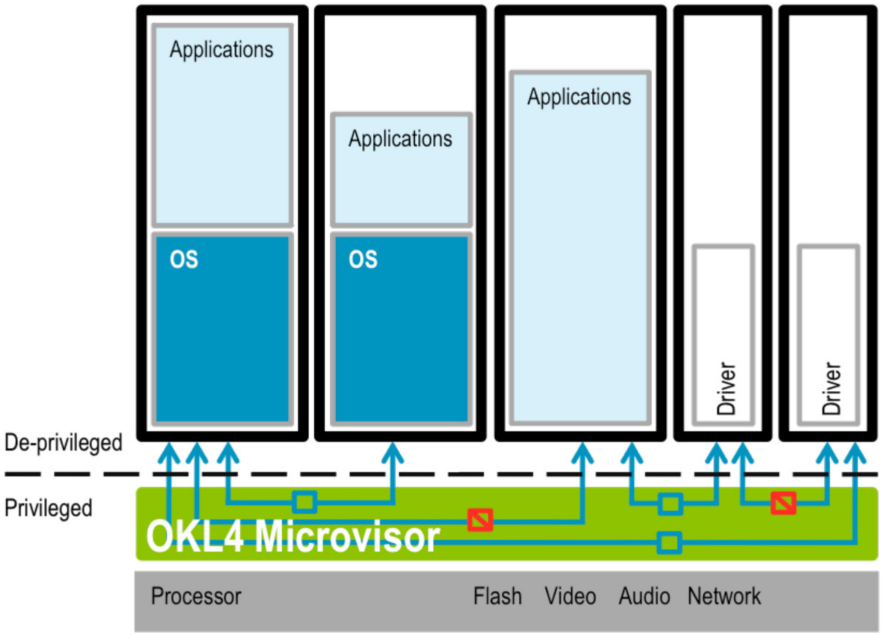

Figure 3. OKL4 Microvisor Architecture

Learn more about OKL4 at http://www.ok-labs.com/products/okl4-microvisor.

Citrix XenClient

Citrix XenClient is an advanced client virtualization platform that provides high levels of security, isolation and performance. It is a secure local virtual desktop solution which is based off the open source Xen Project™ hypervisor. XenClient is able to secure, optimize, and evolve with ever-changing device hardware through a next generation architecture, hardware-assisted security features, and an open, extensible development platform.

XenClient is designed from the ground up for ever-changing hardware with an open source, modular architecture. This next generation architecture (seen in Figure 4) disaggregates and de-privileges components such as networking and VPNs into separate, completely isolated modules to abstract the physical hardware and reduce the device-wide impact from any single component. XenClient uses a hardened Type-1 client hypervisor, which runs on bare metal to maximize both security and performance. It is based on the mature, market-proven Xen Project™ open source hypervisor that has been battle-tested in public clouds and datacenters and open for inspection from third-parties. The hypervisor has been enhanced with a thin footprint that reduces the attack surface and adds additional access control mechanisms using SELinux and Xen Project Security Modules (XSM). Finally, XenClient client endpoints are centrally managed with the Synchronizer, which manages platform updates and controls granular policies of network, VPN, and isolation.

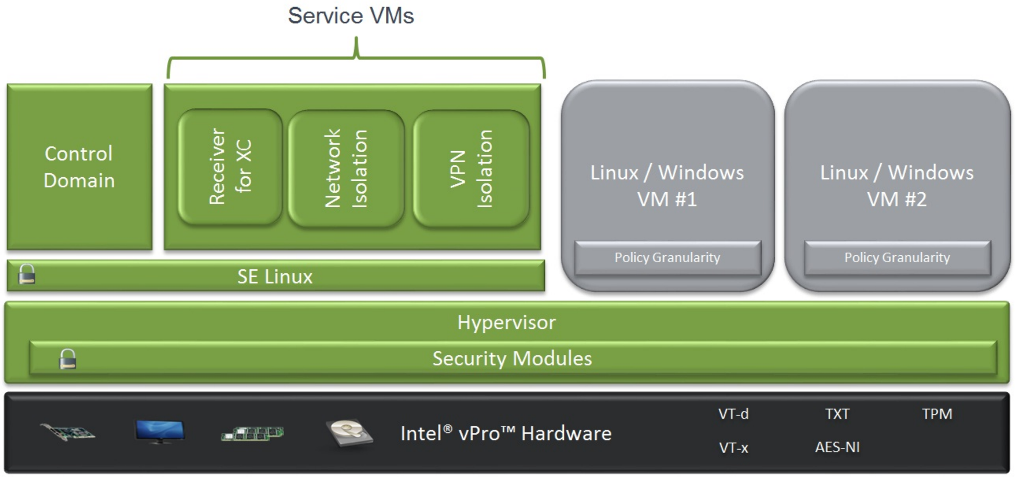

Figure 4. Citrix XenClient Architecture

XenClient has hardware-assisted security capabilities such as trusted boot and disk encryption that ensure only authorized users have access to critical data. It provides the ability to boot to a trusted and verified platform every time with Intel Trusted Execution Technology (TXT) technology, which validates that the system has not been compromised by verifying the integrity of the platform at boot time using the system’s Trusted Platform Module or TPM. This gives XenClient the ability to boot to a trusted and verified system every time. XenClient also uses Intel AES-NI technology for hardware accelerated disk encryption to protect confidential data. Most importantly, it leverages Intel Directed I/O Virtualization Technology or VT-d to get full control over access to I/O resources obtain greater levels of isolation by isolating components including networking and physical devices. This enables further abstraction of physical hardware by virtualizing devices and assigning them directly to specific virtual machines.

XenClient also provides an open platform to allow third-parties to build on top of it. One example of this is developing and distributing extension packs with Service Virtual Machines (VMs). Service VMs are separate VMs used to offload and de-privilege services such as networking, VPN and security scanning from the hypervisor. For instance, XenClient provides network device isolation by putting network cards and VPNs into different Service VMs to protect the rest of the platform from network-based attacks. These extension packs allow organizations to meet local business and certification requirements with custom functionality, including networking, display, and security-related features. They also turn XenClient into a future-proof security platform that can quickly adapt and evolve with continuously changing device hardware.

Furthermore, Citrix XenClient has been optimized to deliver a rich user experience. For instance, it works on a variety of form factors through Commercial Off the Shelf (COTS) vPro hardware. This allows it to work on everything from desktops to laptops, to even Ultrabooks, tablets, and 2 in 1 convertible devices. XenClient can also run the most demanding workloads and graphic intensive 2D & 3D applications with near-native performance for an enhanced user experience. Additionally, it provides support for both Linux and Windows guest operating systems.

By providing high-assurance security and isolation while delivering a rich user experience, XenClient is able to satisfy both IT and end-users with a single solution. It satisfies IT by centrally managing endpoints and protecting critical assets and sensitive information. At the same time, it pleases end-users with a rich user experience since it can run even the most demanding workloads on bare metal. XenClient also helps organizations to execute on organizational initiatives such as mobility and reducing costs. For example, it helps support mobility for organizations by safeguarding and isolating data on mobile devices such as laptops, Ultrabooks, tablets, and 2 in 1 convertible devices. Furthermore, it reduces the Total Cost of Ownership (TCO) for IT by consolidating workloads and applications on multilevel desktops and thin clients onto a single physical system. The modular Citrix XenClient architecture is compatible with multiple open-source and proprietary drivers for virtual devices, including General Dynamics' GD Connect services.

Differentiation, Open Innovation, and Intellectual Property

Innovations in electronics, storage, manufacturing process, chipset and form factor continue to dissolve boundaries in the evolving PC ecosystem. As performance-per-watt increases, devices can support new hybrid forms. Phone form factors blend into tablets that can be docked with a keyboard. Notebooks shrink and can be detached into a separate tablet and keyboard.

Customers now face many form factors when selecting a device, but they face even more choices when using their adopted device: physical configurations, accessories, applications, cloud services and telecom operators. Further, the business priorities driving customer use cases and purchase decisions may not be the same in a few quarters, as new applications, services and device types alter the business landscape.

Client virtualization provides customers with a software platform for resilience against change in application and service ecosystems. Customers can take advantage of new innovations without losing their operational investment in existing services and applications. Citrix XenClient makes emerging and mature ecosystems available to customers on a single device, with centralized remote management.

For device manufacturers and system integrators, Citrix XenClient offers multiple architectural options for software components that integrate device hardware into a differentiated user experience. The XenClient SDK was used by the US Air Force Research Laboratory to create the ground-breaking SecureView multi-domain software appliance. XenClient's modular architecture provided high-assurance composition of open-source and proprietary components from multiple vendors, on an enterprise-grade foundation.

The Citrix XenClient platform provides developers with the efficiency of reusable commercial components along with APIs and extensible interfaces to modify system behavior for specialized use cases. This gives OEMs and system integrators both the business scalability of a horizontal solution and the integrated user experience of a vertical solution, with clear separation of proprietary extensions from the base platform.

Beyond Virtualization

Mobile/embedded virtualization is a truly strategic technology that is enjoying increasing adoption across industry segments, highlighted by the wide adoption and deployment of the General Dynamics OKL4 Microvisor and the Xen Project™ hypervisor. But real-world needs go beyond containers and foreign execution environments.

Virtual machines hosting multiple and diverse guest software stacks do not exist in a vacuum. System development methods need to acknowledge that while intentionally isolated, virtual machines need to communicate with the “real world” and with one another, need to share resources, coordinate operations – “play well” together. And they must do so securely and efficiently.

Real-World Example – High Assurance Solutions

Many real-world design domains include requirements for mobile/embedded virtualization. One such domain is High Assurance, where requirements include and also surpass virtualization alone.

Beginning in the 1980s, procurement policies of the U.S. government shifted from specifying highly customized technologies to solutions built from commercial off-the-shelf (COTS) components. Today, COTS software and hardware is routinely specified to meet the needs of federal, military and civilian programs, and mobile devices are no exception.

As in many conventional enterprise settings, government organizations need to:

- Accommodate workers’ desires to carry a single communications device
- Enjoy the economics of COTS devices built on the popular and fast-growing Android platform
- Secure critical communications, data and applications on a device platform that is a highly visible target for malware and other cyber-threats

Building on the OKL4 Microvisor, General Dynamics evolved a vision for a High Assurance Framework (HAF) to foster implementation of high assurance platforms across the commercial mobile devices ecosystem. Starting with OKL4, the HAF integrates and accommodates best-in-class off-the-shelf components from commercial software suppliers (ISVs) and also free and open source software (FOSS) projects.

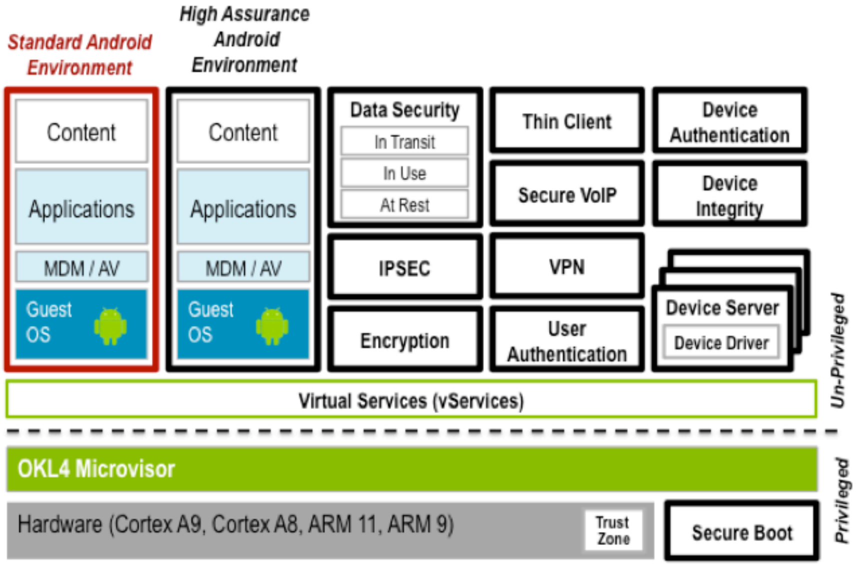

Figure 5 – General Dynamics High Assurance Framework

At the foundation of the High Assurance Framework lies the OKL4 Microvisor, with HAF functional blocks residing in individual fully isolated virtual machines--and the “plumbing” that connects the functional blocks is built from GD Connect services.

Deploying Type I Virtualization

Deploying a Type I hypervisor in today’s consumer electronics (CE) environment carries its share of challenges. Foremost are time-to-deployment and time-to-volume, success-critical metrics directly related to the complexity of modern consumer electronics device designs.

In the “old days” of the PC business, all systems fielded one OS running over one chipset design. The major players – OS and silicon vendors – collaborated to deliver a bootable system and enable core peripheral interfaces.

In today’s dynamic consumer device marketplace, OEMs develop and deploy with myriad chipset types and designs, and face requirements for two, three or more different operating systems to handle system and application-level chores. Instead of the “PC-AT virtual machine,” designers can now avail themselves of Type I hypervisors to normalize and abstract the OS-silicon interface. But the complexity of embedded peripherals, multiple CPU cores, diverse software stacks and communications among them easily outstrips the capabilities of hypervisors alone, especially in the compressed life-cycles endemic to the CE marketplace.

To meet the complex demands of the CE market for rich capabilities and accelerated product delivery, General Dynamics offers GD Connect services.

Industry Use Cases

This approach to Dual OS deployment approach is not without meaningful proof points in the industry today. It is a proven approach deployed by real companies to meet design challenges across multiple industry segments.

Mobile / Wireless

GD Connect services and virtualization platforms such as the OKL4 Microvisor and Citrix XenClient first found deployment in mobile devices such as laptops, smartphones and feature-phone wireless handsets. The technology fulfilled multiple missions: managing baseband communications, supporting chipset consolidation for cost-reduction in mass market devices, providing military-grade isolation and security in “superphones” and other certifiable systems for defense of government communications, and providing containerization for multi-persona handsets and tablets for enterprise mobility.

Mobile/wireless OEMs, network operators and integrators look to GD Connect services to both simplify virtualization of legacy designs and software stacks, and as a toolbox for accelerating design of next-generation smartphones and tablets. For certified/legacy systems, these services help carry forward existing software investments by abstracting hardware and reducing/eliminating requirements to recode, rebuild and recertify. For new designs, GD Connect services help developers “future proof” both platform and value-added software in anticipation of innovation on their own and silicon supplier roadmaps.

Automotive / In-Vehicle Infotainment

The automotive industry is investing in consolidation of diverse in-car subsystems into single “head units” with a goal of reducing costs, improving reliability and enhancing the driver and passenger user experience. This integration of in-vehicle infotainment (IVI) systems with dashboard displays, rear-view cameras and other control systems builds on virtualization capabilities embodied in modern embedded CPUs and realized by system software like the General Dynamics OKL4 Microvisor.

General Dynamics’ GD Connect services provide automotive device manufacturers (OEMs and Tier II suppliers) with a valuable tool to streamline integration of diverse legacy systems into a single head unit. GD Connect services provide the ideal method of secure and controlled communications among virtual machines hosting entertainment, informational and safety-critical software stacks on a single hardware platform. Building on GD Connect services’ transport abstraction and support for I/O device virtualization, these isolated software stacks have better options for communication and sharing when hosted on a single CPU, and can leverage industry-specific transport mechanisms (e.g., CAN bus) when distributed over multiple hosts in a single vehicle.

Trusted and Certified Computing

Several years ago, the National Security Agency (NSA) launched its High Assurance Platform® Program (HAP), an initiative to define a framework for development of "next generation" secure computing platforms, leveraging Trusted Computing technologies to improve protection for data, applications and networks. The NSA program demonstrated that commercial-off-the-shelf (COTS) Trusted Computing technologies can create secure, assured, manageable and usable computing platforms and components.

The NSA HAP was well received by U.S. federal, state and local government agencies (including the NSA itself and more broadly, the Department of Defense and U.S. allies), civilian organizations, and the ecosystem of contractors and suppliers that serves them.

General Dynamics, in conversation with these ecosystem partners, evolved the High Assurance Framework (HAF) to foster implementation of the NSA platform across the commercial mobile devices ecosystem. Today, the HAF forms the foundation of multiple shipping secure devices from key global device OEMs.

Conclusion

Today's device hardware and software ecosystem is more vibrant and varied than ever. It is populated by a menagerie of mobile and embedded operating systems, multiple hardware architectures and chipsets, different hypervisors, and players that develop and deploy combinations thereof. This diversity emanates not from positioning by silicon suppliers and ISVs – it arises from the varied and dynamic real-world requirements of device manufacturers and end-users.

Meeting those requirements with off-the-shelf hardware and software is upending long-held beliefs and design principles. Key attributes of intelligent devices are becoming increasingly mutable – form factor, mission, CPU, OS, software stack – you name it.

In particular, OS wars are over.   Who won? The end user.

Instead of being locked into one OS and a monolithic user experience, embedded/mobile virtualization lets intelligent devices have multiple personalities, running different operating systems for different missions and use cases, separately and at the same time.

Building this new generation of devices doesn't have to be rocket science. Citrix and General Dynamics now give device developers and integrators a powerful toolbox for building and deploying modular, componentized and re-usable device software, rapid and efficiently.

To learn more about General Dynamics' GD Connect services, visit the GD Protected website.

For more information about Citrix XenClient, please see the XenClient website.

References

Nerup, Carl [2011]. *A High Assurance Framework for Mobile/Wireless Device Applications.* An OK Labs White Paper