The Hidden Potential Within Video Game Consoles

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY-SA 4.0

SUBMISSION DATE / POSTED DATE

09-10-2020 / 27-01-2021

CITATION

Mattioli, Michael; Lahtiranta, Atte (2020): The Hidden Potential Within Video Game Consoles. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.13075694.v4>

DOI

[10.36227/techrxiv.13075694.v4](https://doi.org/10.36227/techrxiv.13075694.v4)

The Hidden Potential Within Video Game Consoles

Michael Mattioli and Atte Lahtiranta
Goldman Sachs & Co.

Abstract—Video game consoles share many of the characteristics of an ideal device for use in enterprise deployments. In comparison to many desktop and notebook PCs available in the market, modern video game consoles are actually quite powerful and capable. They provide an excellent user experience with simple and intuitive setup and operation. At the heart of the design of many modern video game consoles is security; they are remarkably resilient against very sophisticated hardware and software attacks. They are also rather cost-effective in comparison to modern PCs.

I. INTRODUCTION

Video game consoles are ideal devices for enterprise deployments; they're powerful, versatile, easy to use, cost-effective, and extremely secure. Systems suitable for use in an enterprise must be able to handle a variety of workloads to ensure that users remain productive; such workloads include, but are not limited to, video conferencing, web browsing, content creation (e.g. spreadsheets, presentations, documents, audio, video, etc.), and audio/video streaming. Security is equally as important, if not more important, than user productivity; enterprise systems routinely process sensitive information which is critical to the organization's success. Of course, all enterprise systems strive to reduce overall total cost of ownership (TCO); this can be achieved by simply reducing the cost of the hardware itself as well as reducing the operational expenses (OpEx) incurred by managing and maintaining the systems (e.g. patching, updates, user training/support, etc.).

The purpose of this paper is to describe the ideal characteristics of a device suitable for use in enterprise deployments and demonstrate how video game consoles are designed with these characteristics and traits in mind which, therefore, makes

them an excellent fit. It is extremely important to understand that while this paper may use specific consoles as *examples* of such devices many of the points being made apply to almost all modern video game consoles including, but not limited to, the Nintendo Switch, the Sony PlayStation 4, the Sony PlayStation 5, and the Microsoft Xbox Series S.

II. PERFORMANCE

Relative to desktop and notebook PCs available at their time of release, modern video game consoles are quite powerful in comparison. As shown in Table I, video game consoles feature the latest technologies available at their respective times of release. Unsurprisingly, performance is critical when considering devices for use in the enterprise. It is fairly common for enterprise users to be working across multiple applications and contexts at once; high-performance devices aid user workflow and productivity.

The Microsoft Xbox One X features a semi-custom system on a chip (SoC) developed in partnership with Microsoft and Advanced Micro Devices (AMD) [1]. The SoC is implemented using Taiwan Semiconductor Manufacturing Company's (TSMC) 16nm Fin Field-effect transistor (FinFET) Plus (16FF+) technology; it features a CPU composed of 8x 64-bit x86 cores operating at 2.3 GHz and a GPU composed of 40x compute units operating at 1.172 GHz. The SoC uses a unified memory pool, shared by both the CPU and the GPU, which consists of 12 GB of GDDR5 DRAM; the total memory bandwidth is 326.4 GB/s. The console supports HDMI 2.0b display output with high-bandwidth digital content protection (HDCP) 2.2, 10-bit HDR, and a resolution of 3840 x 2160 at 60Hz. The GPU is further optimized for a version

TABLE I
HARDWARE DETAILS OF VARIOUS VIDEO GAME CONSOLES RELEASED OVER SEVERAL YEARS.

System	Release Date	CPU Cores	Memory	Process Tech.	CPU Microarch.	GPU Microarch.
Microsoft Xbox One	November 2013	8x x86-64	8GB DDR3	TSMC 28nm	AMD Jaguar	AMD GCN 2
Sony PlayStation 4	November 2013	8x x86-64	8GB GDDR5	TSMC 28nm	AMD Jaguar	AMD GCN 2
Microsoft Xbox One S	August 2016	8x x86-64	8GB DDR3	TSMC 28nm	AMD Jaguar	AMD GCN 2
Sony PlayStation 4 Pro	November 2016	8x x86-64	8GB GDDR5	TSMC 28nm	AMD Jaguar	AMD GCN 4
Nintendo Switch	March 2017	4x ARMv8	4GB LPDDR4	TSMC 20nm	ARM Cortex-A57	NVIDIA Maxwell
Microsoft Xbox One X	November 2017	8x x86-64	12GB GDDR5	TSMC 16FF+	AMD Jaguar	AMD GCN 4
Microsoft Xbox Series X	November 2020	8x x86-64	16GB GDDR6	TSMC N7e	AMD Zen 2	AMD RDNA 2
Microsoft Xbox Series S	November 2020	8x x86-64	10GB GDDR6	TSMC N7e	AMD Zen 2	AMD RDNA 2
Sony PlayStation 5	November 2020	8x x86-64	16GB GDDR6	TSMC N7e	AMD Zen 2	AMD RDNA 2

of Microsoft's DirectX 12 graphics API specific to the system.

The Microsoft Xbox Series X, shown in Figure 1, features a semi-custom (SoC) developed in partnership with Microsoft and Advanced Micro Devices (AMD) [2]. The SoC is implemented using TSMC's 7nm FinFET Enhanced (N7e) technology; it features a CPU composed of 8x 64-bit x86 cores operating at 3.8GHz, or 3.6GHz with simultaneous multithreading (SMT) enabled, and a GPU composed of 52 compute units operating at 1.825GHz. The SoC uses a unified memory pool, shared by both the CPU and the GPU, which consists of 16 GB of GDDR6 DRAM; 10GB, reserved for the GPU, operate at 560 GB/s and 6GB, reserved for the CPU, operate at 336GB/s. The console supports HDMI 2.1 display output with the same features as the Xbox One X SoC in addition to fixed rate link (FRL), variable refresh rate (VRR), display stream compression (DSC), 4:4:4 chrome subsampling, and a resolution of either 3840 x 2160 at 120Hz or 7680 x 4320 at 60Hz. The GPU is further optimized for a version of Microsoft's DirectX 12 Ultimate graphics API specific to the system.

For comparison, the Intel Core i5-8600T, an Intel eighth-generation desktop SoC released several months after the Xbox One X, features a CPU

Fig. 1. Microsoft Xbox Series X video game console and controller [3].

composed of 6x 64-bit x86 cores operating at a base frequency of 2.3 GHz and a GPU operating at 1.15GHz; this SoC is implemented using Intel's third-generation 14nm++ technology [4]. It supports HDMI display output with a resolution of 4096 x 2304 at 24Hz; it also supports the mainstream version of Microsoft's DirectX 12 graphics API.

It is important to understand that while these SoCs differ *drastically* in regards to cost, intended use, process technology, thermal design power (TDP), instructions per cycle (IPC), and various other aspects of SoC and CPU and GPU design, the intent here is to highlight that video game consoles are powerful and feature-rich in comparison to mainstream compute devices available at the time of their release.

III. USER EXPERIENCE

Video game consoles provide an elegant and engaging experience for all ages and skill levels. This characteristic is ideal for enterprises because it enables all of its users to be functional and productive without requiring additional training, learning, etc.

A. Ease of use

Content (games) aside, the systems are designed for both children and adults with limited experience or understanding of technology. Only two cables are required to use the system: power and display (usually HDMI). User input and haptic feedback is performed through an ergonomically designed controller; however, modern systems also supports traditional keyboard and mouse input [5]. System and software (game) updates and purchases are obtained through a single source (e.g. Microsoft Store, Nintendo eShop, Sony PlayStation Store, etc.) which is tightly integrated into the system making it easy and intuitive to find, purchase, and download software.

B. Versatility

The systems are also rather versatile; developers can write and release a variety of different software titles. Aside from the obvious (games), this includes, but is not limited to, video streaming

applications, music streaming applications, video conferencing applications, web browsers, and cloud storage applications. For example, Hulu is available on the Nintendo Switch via the Nintendo eShop and Spotify is available on the PlayStation consoles via the Sony PlayStation Store. Enterprises have the ability to write their own custom internal applications and independent software vendors (ISVs) can also develop and distribute applications for public consumption.

IV. SECURITY

At the heart of their design is thoughtful and practical defense against a wide range of threats. Without question, security is paramount in enterprise contexts. It is common for users to access and store sensitive information which is crucial to the success and well-being of the organization and its stakeholders (e.g. employees, customers, clients, shareholders, etc.).

A. Identity and access management

Centralized identity and access management (IAM) is used throughout the entire ecosystem. The Microsoft consoles require users authenticate using a Microsoft account; similarly, the Sony consoles require a Sony account and the Nintendo consoles require a Nintendo account. These identities are then used for access and privilege management. Identity is required to associate and maintain licenses for software (games and applications) and subscription services. It is also used to control communication and interaction with other users; access to user information (e.g. online status, currently running software, etc.) and interactions (e.g. text messages, voice messages, in-game chat, etc.) can be explicitly granted to or revoked from other users.

B. Patching and updates

The systems are designed such that only fully patched and updated systems and software can access protected resources (e.g. Xbox LIVE, Nintendo Online, game servers, etc.) and interact with other compliant (patched and updated) systems and users.

Upon boot, the system attempts to connect to single, trusted authority (e.g. Xbox LIVE, PlayStation Network, etc.). Upon connection, it then checks

for any system updates and prompts the user to download and install them. If the user chooses to skip/decline any pending updates or if a connection to the trusted authority cannot be made (for whatever reason), they can continue to use the system offline and use software (games) that is already installed. Very simply, the system will not allow a user to connect to the trusted authority (e.g. to play games, to chat with friends, etc.) unless the system is fully patched and updated.

If the system is fully patched and updated but the software (game) the user wishes to launch is not fully updated, the user is prompted to download and install any pending updates. If the user chooses to skip/decline any pending updates, they can continue to use the software offline; in other words, they cannot interact (play) with other users online using that software unless it is fully patched and updated.

C. Hardware security

Video game consoles are designed to be remarkably resilient against various hardware and software attacks. The entire business model of a modern video game console is centered around software sales, not hardware sales. They are designed around the premise that the end-user cannot be trusted; an end-user's motivation is to play games for free (piracy) and/or modify the game to achieve an unfair advantage over other players (cheat). Therefore, extreme measures must be taken to prevent physical attacks against the system. However, the end-user isn't the only untrusted entity.

The Xbox One X is an excellent example of such design [6]; many of these security features have been carried forward to the Xbox Series X. Quite literally, the only trusted entity of the entire Xbox One X system is the SoC itself; the internal storage, DRAM, optical drive, etc. are considered untrusted. Therefore, all information which leaves the SoC must be encrypted and all information which enters the SoC must be decrypted and integrity checked.

All data is stored in non-volatile memory using a format known as the Xbox Virtual Disk (XVD). As illustrated in Figure 2, all data is stored in an NT File System (NTFS) virtual disk and then encrypted and hashed (for both confidentiality and integrity); finally, the root digest of the hash tree is signed

Fig. 2. High-level depiction of an Xbox Virtual Disk (XVD) structure [6].

Fig. 3. High-level depiction of the Xbox One X SoC architecture [6].

using Microsoft RSA (for integrity of the hash tree itself).

The system SoC, illustrated in Figure 3, features a custom-designed element referred to as the Streaming Crypto Engine (SCE) which is able to decrypt information loaded from the internal storage as fast as it can be read from the underlying I/O bus (SATA III in Xbox One X and NVMe in the Xbox Series X). Keys used to decrypt information are fed into the SCE through a dedicated hardware pin connecting it to the Crypto Engine inside of another custom-designed element within the SoC referred to as the Security Complex; this ensures that the keys are never exposed to software at any point in time. This Security Complex also closely monitors the system clock, voltage, temperature,

Fig. 4. High-level depiction of the Xbox One X three-OS architecture [6].

and reset; these are commonly manipulated to attack a system.

One of the core tenets of the console’s security design is defense in depth; in other words, an attacker must break through multiple layers of security. In addition to encrypting and integrity checking all information which passes through the SoC, the system uses a three-OS architecture [7] as illustrated in Figure 4. The Host Operating System (OS) contains all of the drivers and necessary components for interacting with and communicating with the underlying hardware. The Software OS contains the game or application that is running in the foreground. The System OS is responsible for everything outside of the software title itself such as networking communication and drawing any user interface elements outside of the software. As illustrated in Figure 4, the majority of the system memory is allocated to the Software OS. The Hypervisor is responsible for enforcement of signed code. Using the stage-2 CPU MMU, it will verify that every page of memory which is marked for execution is signed by Microsoft; if it is not signed, it will not be executed. This architecture not only allows developers to create more engaging experiences, it further strengthens the overall security of the system by layering and separating software components.

V. COST

As shown in Table II, video game consoles, at the time of their respective times of release, have been priced at or below USD 499 for the last several years. For comparison, USD 499 spent today can buy a Lenovo ThinkCentre M720q which includes 128 GB of internal storage, an Intel Pentium Gold G5400T SoC, and 4 GB of DDR4 DRAM [8]. Clearly, the consoles are rather competitively priced compared to modern PCs. However, the true cost of any hardware deployment in the enterprise extends far beyond the device itself. One must consider patching, maintenance, and management of the device throughout its entire lifecycle. Considering that patches and software are released and distributed directly through the trusted authority (e.g. Microsoft via Xbox LIVE, Nintendo via Nintendo Online, etc.), there is less operational overhead for an enterprise which would otherwise have to build its own infrastructure to do so.

VI. CONCLUSION

The notion of using a video game console in the enterprise may seem laughable at first glance. However, as discussed, video game consoles actually embody many of the characteristics of an ideal device for use in the enterprise: high performance, excellent user experience, versatility, cost-effective, and secure at its core. Technologies from video game consoles are already trickling into the enterprise. Security technologies found in some of the latest AMD CPUs such as Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV) originated in the design of the Xbox One X [9]. Hypervisor-Protected Code Integrity (HVCI), a feature now generally available in Hyper-V for Windows, originated in the design of the hypervisor signed code enforcement technology previously discussed. Microsoft’s recently announced Pluton security processor originated in the SoC previously discussed [10]. Other recently released consoles such as the Microsoft Xbox Series S and the Sony PlayStation 5 share the same characteristics and carry these traits forward; performance has improved with adoption of NVMe internal storage [11] and semi-custom variants of AMD’s Zen 2 CPU cores and RDNA 2 GPU cores while security has improved simply because threats (piracy and

TABLE II
COST COMPARISON OF VARIOUS VIDEO GAME CONSOLES AT THEIR TIME OF RELEASE.

System	Release Date	Internal Storage	Cost (USD)
Microsoft Xbox One	November 2013	500GB	499
Sony PlayStation 4	November 2013	500GB	399
Microsoft Xbox One S	August 2016	500GB	299
Sony PlayStation 4 Pro	November 2016	1TB	399
Nintendo Switch	March 2017	32GB	299
Microsoft Xbox One X	November 2017	500GB	499
Microsoft Xbox Series X	November 2020	1TB	499
Microsoft Xbox Series S	November 2020	512GB	299
Sony PlayStation 5 w/o optical drive	November 2020	825GB	399
Sony PlayStation 5 w/optical drive	November 2020	825GB	499

cheating) and attacks only become more advanced over time.

[11] M. Mattioli, "History of video game distribution," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2020.

REFERENCES

- [1] J. Sell, "The xbox one x scorpio engine," *IEEE Micro*, vol. 38, no. 2, pp. 53–60, 2018.
- [2] J. Andrews and M. Grossman, "Xbox series x system architecture," https://hotchips.org/assets/program/conference/day1/HotChips2020_GPU_Microsoft_Jeff_Andrews_v2.pdf, Aug 2020, accessed: 2021-01-24.
- [3] W. Commons, "File:xbox series x 2.jpg," https://commons.wikimedia.org/wiki/File:Xbox_Series_X_2.jpg, Dec 2020, accessed: 2021-01-24.
- [4] Intel, "Intel core i5-8600t processor," <https://ark.intel.com/content/www/us/en/ark/products/129938/intel-core-i5-8600t-processor-9m-cache-up-to-3-70-ghz.html>, accessed: 2020-09-27.
- [5] Microsoft, "Mouse and keyboard support on xbox one," <https://support.xbox.com/help/hardware-network/accessories/mouse-keyboard>, accessed: 2020-09-27.
- [6] T. Chen, "Guarding against physical attacks: The xbox one story," <https://www.platformsecuritysummit.com/2019/speaker/chen/>, Oct 2019, accessed: 2020-09-27.
- [7] E. Brechner, "Getting diagonal on the xbox one trifecta," *Computer*, vol. 46, no. 8, pp. 77–78, 2013.
- [8] Newegg, "Lenovo thinkcentre m720q 10t8sdj900 desktop computer - pentium gold g5400t - 4 gb ram - 128 gb ssd - tiny - black," <https://www.newegg.com/p/N82E16883994324>, accessed: 2020-09-26.
- [9] CRN, "Amd's xbox, playstation work led to a big security feature in epyc," <https://www.crn.com/news/components-peripherals/amd-s-xbox-playstation-work-led-to-a-big-security-feature-in-epyc>, Aug 2019, accessed: 2020-09-27.
- [10] Microsoft, "Meet the microsoft pluton processor - the security chip designed for the future of windows pcs," <https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/>, Nov 2020, accessed: 2020-11-23.

Michael Mattioli leads the Hardware Engineering team within Goldman Sachs. He is responsible for the design and engineering of the firm's digital experiences and technologies. He is also responsible for the overall strategy and execution of hardware innovation both within the firm and within the broader technology industry. Contact him at michael.mattioli@gs.com.

Atte Lahtiranta is Chief Technology Officer and head of Core Engineering at Goldman Sachs. Contact him at atte.lahtiranta@gs.com.