Video Game Consoles in the Enterprise

Michael Mattioli and Atte Lahtiranta
Goldman Sachs & Co.

Fig. 1. Microsoft Xbox One X video game console [1].

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 the ideal device for enterprise deployments; they're powerful, versatile, easy to use, cost-effective, and extremely secure. The Microsoft Xbox One X, released in 2017, is an excellent example of a modern video game console which embodies many these attributes.

II. PERFORMANCE

Relative to desktop and notebook PCs available at its time of release, the Xbox One X is quite powerful in comparison.

The Xbox One X features a semi-custom system on a chip (SoC) developed in partnership with Microsoft and Advanced Micro Devices (AMD) [2]. 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 of Microsoft's DirectX 12 graphics API specific to the system.

For comparison, the Intel Core i5-8600T, an Intel eighth-generation desktop CPU released several months after the Xbox One X, features a CPU 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 [3]. 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's important to understand that while these two 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 the Xbox Series X is powerful and feature-rich in comparison to mainstream compute devices available at the time of its release.

III. USER EXPERIENCE

The Xbox One X provides an elegant and engaging experience for all ages and skill levels.

A. Ease of use

Content (games) aside, the system is designed for both children and adults with limited experience or understanding of technology. Only two cables are required to use the system: power and HDMI (to connect it to a display). User input and haptic feedback is performed through an ergonomically designed controller; however, the system also supports traditional keyboard and mouse input [4]. System and software (game) updates and purchases are obtained through a single source, the Microsoft Store, which is tightly integrated into the system making it easy and intuitive to find, purchase, and download software.

B. Versatility

The system is also rather versatile. The console can support applications developed using the Universal Windows Platform (UWP) [5]. 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.

IV. SECURITY

At the heart of the system's design is thoughtful and practical defense against a wide range of threats.

A. Identity and access management

Centralized identity and access management (IAM) is used throughout the entire ecosystem.

Users of the system are required to authenticate using a Microsoft account; this identity is 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 system is designed such that only fully patched and updated systems and software can access protected resources (Xbox LIVE, game servers, etc.) and interact with other compliant (patched and updated) systems and users.

Upon boot, the system attempts to connect to Xbox LIVE. 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 Xbox LIVE 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 Xbox LIVE (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

The Xbox One X was designed to be remarkably resilient against various hardware and software attacks [6]. 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. 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.

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].

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 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 (in the case of the Xbox One X, SATA III). Keys used to decrypt information are fed into the SCE through a dedicated hardware pin connecting

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

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, 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

At release in 2017, the Xbox One X was sold for USD 499; the system included 1 TB of electro-mechanical internal storage and a controller. For comparison, the same USD 499 spent today can buy a Lenovo ThinkCentre M720q which includes 128 GB of solid-state internal storage, an Intel Pentium Gold G5400T SoC, and 4 GB of DDR4 DRAM [8]. Clearly, the console is 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 Microsoft via Xbox LIVE, 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. The Xbox One X is just one example; other modern consoles such as the Sony PlayStation 4 and the Nintendo Switch share the same characteristics. Upcoming consoles such as the Microsoft Xbox Series X and S and the Sony PlayStation 5 are expected to carry these traits forward; performance is expected to improve with

adoption of NVM Express (NVMe) internal storage and semi-custom variants of AMD's Zen2 CPU cores and RDNA2 GPU cores while security is expected to improve simply because threats (piracy and cheating) and attacks will only become more advanced over time.

REFERENCES

- [1] W. Commons, "File:xbox one x gamescom (36042607743).jpg," [https://commons.wikimedia.org/wiki/File:XBOX_ONE_X_Gamescom_\(36042607743\).jpg](https://commons.wikimedia.org/wiki/File:XBOX_ONE_X_Gamescom_(36042607743).jpg), Aug 2017, accessed: 2020-09-26.
- [2] J. Sell, "The xbox one x scorpio engine," *IEEE Micro*, vol. 38, no. 2, pp. 53–60, 2018.
- [3] 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.
- [4] Microsoft, "Mouse and keyboard support on xbox one," <https://support.xbox.com/help/hardware-network/accessories/mouse-keyboard>, accessed: 2020-09-27.
- [5] Microsoft, "Uwp on xbox one," <https://docs.microsoft.com/en-us/windows/uwp/xbox-apps/>, Oct 2017, 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.

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.