Today's Computer Security Threats Require Hardware Solutions

Electronic Design

Sasa Marinkovic

Fri, 2014-08-22 11:12

Adding security features to computer hardware will be an effective and necessary step to mitigate security threats.

When exploits like Heartbleed sport their own custom graphic logos, you know the general public is paying attention. CIOs should take advantage.

Security and privacy have achieved top-of-mind public awareness, especially with the worldwide reaction to revelations of the National Security Agency's "snooping" into private, corporate, and government communications. CIOs can make good use of employees' desire to block online snoopers, including e-mail providers that use personal communications and online browsing history for "behavioral remarketing" targeted advertisements that reduce people to mere barcodes.

Security vendors are working on ways to increase privacy and stop the next Heartbleed bug. The ideal is that these technologies will not require users to remember dozens of unique and complex passwords for sites and applications. With millions of new Internet-connected devices hitting networks within the next few years, CIOs should be applying pressure, because the current model is failing.

For decades, IT has largely relied on username/password access and software-based antivirus and malware systems. However, the computing landscape has changed, along with user expectations. Employees are demanding greater individual control of social networking security and privacy, as well as protection from online harassment, theft, and misuse of personal information. They want to enjoy a free and open Internet, yet be protected by computing security technologies that are intuitive, interactive, and invisible.

Related

Developers Discuss IoT Security And Platforms Trends

Understanding The Protocols Behind The Internet Of Things

Can The Internet Of Things Be Secure?

Nice concept, but we can't wait. The rise of advanced persistent threats (APTs) is fueling a growing consensus that basic password-protection and software-based security measures are simply no longer enough.

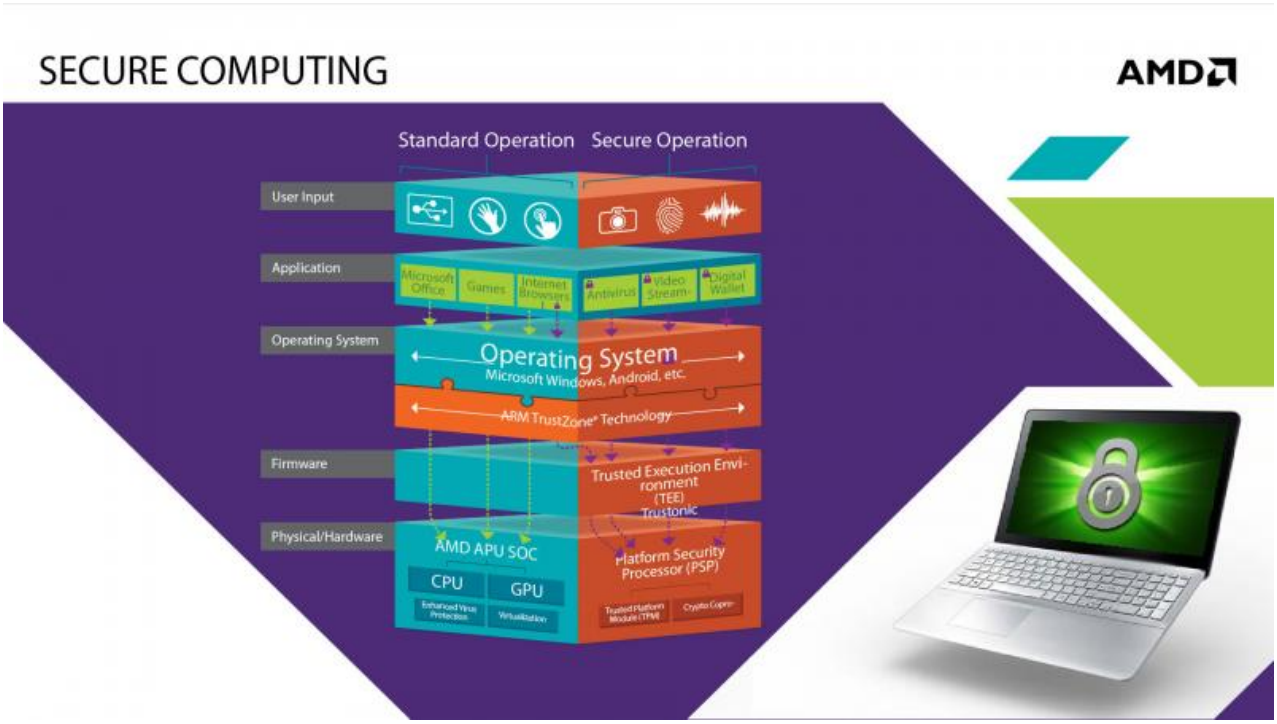
It's in the Chips

Hardware-based security, building security directly into the silicon, is a simple and cost-effective

approach. Many software-only security programs load as a background application after the device boots, detecting threats predominantly using blacklist checking and burning precious CPU cycles that can slow computer performance and hinder productivity.

In contrast, hardware-based security is the first to boot and operates independently even after the boot process. Software protected by hardware-based security is shielded from potential malware and other threats that may have infected the main operating system. The dedicated security hardware also operates without burdening the host processor, avoiding computer slowdowns or lost productivity.

Hardware-based security is not a new concept, and previous efforts saw limited success because they were designed as proprietary closed systems, eliminating the possibility of third-party audits to detect security flaws. A better bet is a comprehensive "security platform" approach to hardware-based security based on open-source and standards-based architecture, including a programmable operating environment.



A prominent example of this approach is the TrustZone technology developed by ARM *(see the figure)*. This open platform includes programmable software components and applications that enable computer hardware designers to create customized security solutions or counter specific security threats.

Homegrown technology solutions are generally preferable, but the open-source and standards-based TrustZone approach was so appealing that we partnered with ARM. The idea is to create a broad-based "security ecosystem" spanning the ARM processor architectures running today's tablets and smartphones, in addition to the x86 processor architecture running most of today's notebooks, desktop PCs, and servers. Unlike proprietary closed-architecture hardware security solutions, an open-platform standards-based approach to computer security will allow for transparent and collaborative solutions, rapid response to emerging threats, and the potential for broad industry acceptance and long-term success.

We envision "platform security processors" that will include hardware-level protection to monitor and help protect against malicious access to sensitive data and operations. These security processors will complement existing security offerings including no-execute, virtualization, and manageability engines. Targeting a "code-once-use-everywhere" development goal, the fully programmable development

environment will enable the creation of applications that simultaneously support both x86 and ARM computing platforms.

Goodbye Passwords, Hello Logins

The goal is to deliver seamless security measures designed to enhance the security and privacy of everyday end-user transactions and invisibly protect against viruses, phishing, and persistent threats. Using the same security features and applications across personal devices ranging from cell phones to desktop PCs, users could benefit from secured PIN entry for mobile payments and banking, cloud-based document access control, software license management, digital rights management, loyalty-based applications, secure ticketing, mobile TV, and more.

Intuitive and interactive security measures could include secure login features using face recognition and voice authentication technologies. Imagine a powerful and sophisticated "security processor" enabling enhanced low-light facial recognition along with additional layers of voice authentication and identity verification. Online personal banking could become almost risk-free using double-authentication applications for additional system access security, randomly generated one-time passwords, and advanced transaction-level security with industry-wide compatibility with thousands of banks.

Multiple Devices, One Great Experience

Simultaneously supporting the two most commonly used computing platforms, the TrustZone security ecosystem aims to enable practically identical user experiences across almost all computing and communications devices. Security features and applications should be virtually indistinguishable for all supported devices, whether accessed using a smartphone, tablet, mobile device, 2-in-1 PC, ultrathin notebook, desktop gaming computer, or home server.

Open and industry-standard security frameworks enable more secure computing experiences for businesses, organizations, governments, and greater individual privacy and safety with everyday transactions in computing experiences. For example, most of the vulnerable content on computing devices utilizing the TrustZone security processor would have been protected from the Heartbleed bug. The best part of this approach: the freedom to use any computing device, anywhere, while enjoying the peace of mind enabled by best-in-class security.

Sasa Marinkovic *is head of technology and ISV marketing, responsible for identifying and evangelizing upcoming industry trends and technologies critical to AMD's success. He was responsible for the successful launch of several generations of disruptive products (IGPs, dGPUs, and APUs) and technologies (including HSA) and holds a number of patents, including PowerXpress, a technology that has been implemented in most of today's notebooks. He joined ATI Technologies in 1996 and came to AMD via AMD's acquisition of ATI. He graduated from the University of Toronto where he received a bachelor's degree in electrical engineering. He lives in Toronto. He can be reached at* sasa.markinovic@amd.com.

Source URL: http://electronicdesign.com/embedded/today-s-computer-security-threats-require-hardware-solutions