Solution Brief
Multi-Level/Multi-Domain Platform Security
Public Sector Edge Computing

Multi-Layer Platform Security for the Public Sector

Intel security technologies provide a multi-layer computing platform security solution for the public sector.

Taking a Layered Approach to Security

One of the challenges in securing the public sector computing infrastructure is the attack surface can be exceptionally large. Hackers continuously look for ways to exploit vulnerabilities across a computing platform's diverse and complex stack.

Providing a comprehensive security approach, this paper describes several Intel security technologies that can significantly reduce the attack surface area of a computer's platform stack.

Challenge

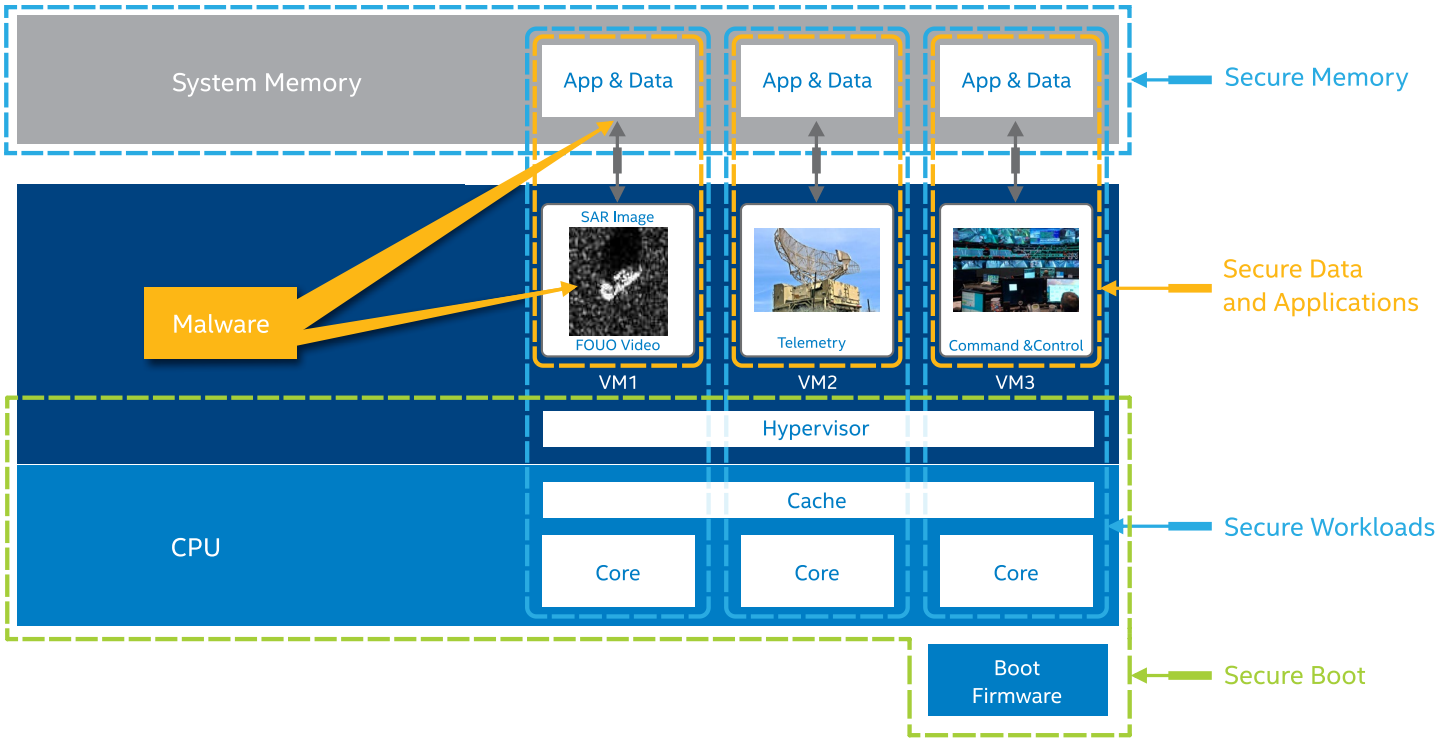
There is no single solution that can fully protect a computing system, which is why multiple technologies and controls working in concert need to be used – a layered approach to security. It is important that public sector computing systems secure the whole stack, including the firmware, operating system, hypervisor, applications, and other workloads.

Solution

A suite of Intel security technologies can increase computer security in the public sector by providing protection of the boot sequence, data, applications, and workloads. The technologies complement a multi-layer security approach needed to safeguard systems against malware.

Figure 1 illustrates an example of a multi-layer platform security approach. A synthetic-aperture radar (SAR) application is protected from a virtual machine (VM) rootkit attempting to intercept and manipulate a mission-critical "For Official Use Only" (FOUO) video stream collected by a drone. VM rootkit attacks attempt to subvert and then access and manipulate a legitimate VM's file system, application code, and data.

Figure 1. Multi-layer platform security protecting a synthetic-aperture radar (SAR) application



1. Secure boot

Threat: Attackers inject VM root malware into the firmware, which could load before the computer's security defenses are activated.

Solution: Combining Intel® Boot Guard and Intel® Trusted Execution Technology (Intel® TXT), Intel® Converged BootGuard and Intel TXT (Intel® CBnT) detects the firmware was modified, terminates the boot sequence, and provides attestation of the booted components and firmware preventing the malware from being loaded on the system and getting visibility into the boot flow and mitigation.

2. Secure memory

Threat: Attackers attempt to access and exfiltrate the FOUO VM's video data stream.

Solution: Intel® Total Memory Encryption (Intel® TME)[1] encrypts the FOUO video data, so it is incomprehensible to the malware.

3. Secure data and applications

Threat: Malware attempts to access and control the FOUO VM's video data application.

Solution: Intel® Software Guard Extensions (Intel® SGX)[2], encrypts the FOUO application and data, and places it in a highly protected memory address space that is not accessible to the malware.

4. Secure workloads

Threat: Malware attempts a cache side channel attack, which takes advantage of shared cache memory, to read the FOUO video data.

Solution: Intel® Resource Director Technology (Intel® RDT) provides cache isolation, preventing the malware from intercepting the FOUO application's cache contents.

Intel Security Technologies Summary

This solution brief features four Intel security technologies that are among many others available on Intel® processor-based computing platforms.

Intel® CBnT verifies the firmware booting the platform was not inappropriately modified and establishes a measured launch environment (MLE)

that compares all critical launch environment elements against a known good source.

Intel Total Memory Encryption encrypts the platform's entire physical external memory to ensure data privacy.

Intel Software Guard Extensions isolate and encrypt specific application code and data to create private regions in external memory, called enclaves. Enclaves are protected from malicious processes running at higher privilege levels, including rootkit malware and physical access threats.

Intel Resource Director Technology brings new levels of visibility and control over how shared resources cache and memory bandwidth are used by applications, VMs, and containers.

More Information

For more information about the security technologies presented in this white paper, please contact Intel at IOTG-PublicSector@intel.com

1. Baiju Patel, Intel website, "Intel Releases New Technology Specification for Memory Encryption," Dec 22, 2017, https://software.intel.com/en-us/blogs/2017/12/22/intel-releases-new-technology-specification-for-memory-encryption.
2. Intel® technology features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://www.intel.com.