Securing the Datacenter with FlexVer™

Raptor Engineering, LLC
https://www.raptorengineering.com

Overview

In this document we explore the revolutionary FlexVer™ security technology introduced on our Talos™ mainboards, and answer the most frequently asked questions regarding usage of this technology.

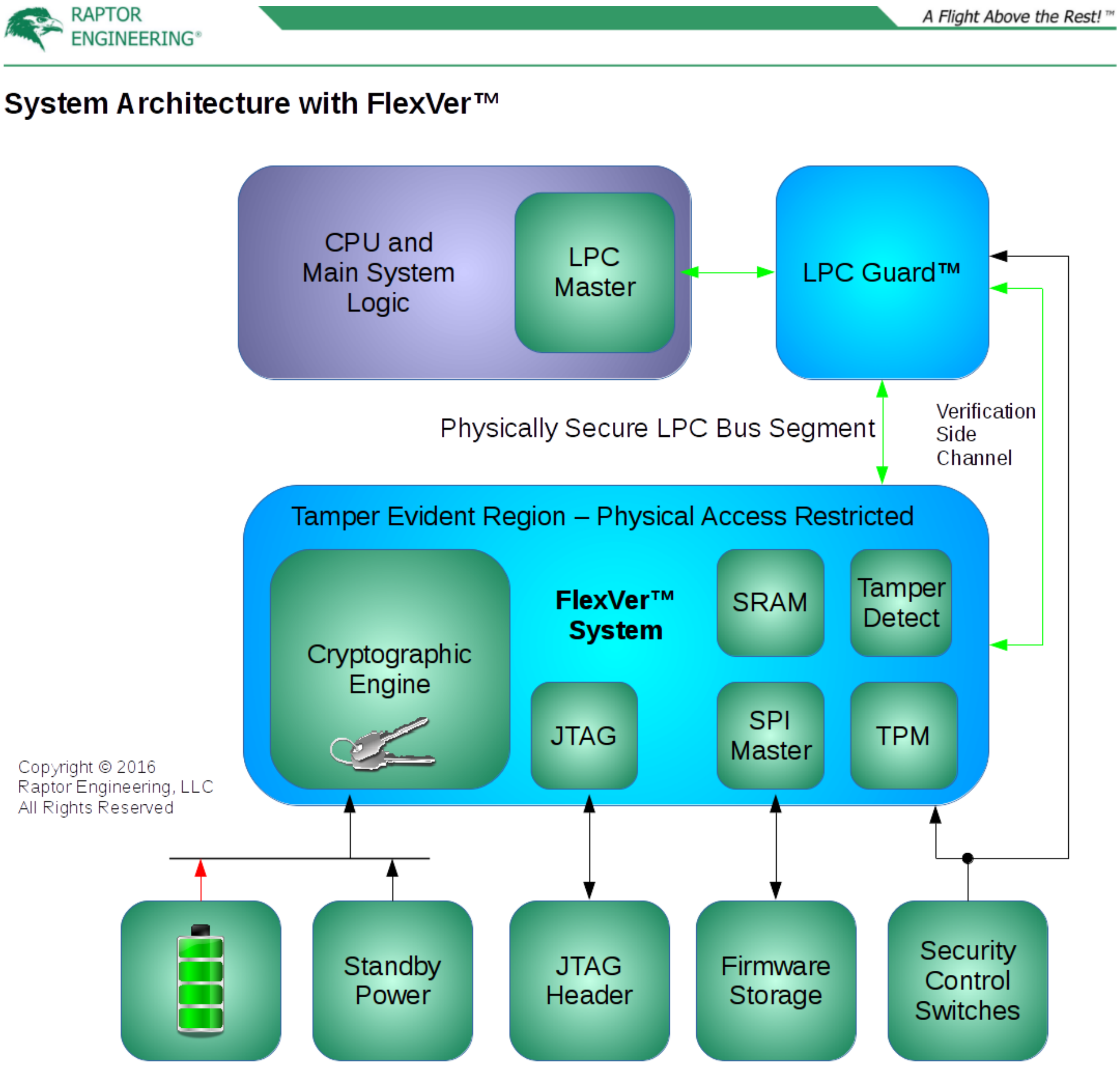
What is FlexVer™?

FlexVer™ is a new, owner-controlled security technology designed to safeguard critical data and applications in the event of software or hardware tampering. FlexVer™ allows a system to be provisioned in a trusted physical environment, then deployed to an untrustworthy physical location while retaining system integrity. Provided that OS-level attack avenues are properly mitigated, for example through the use of TRESOR and similar technologies, FlexVer™ allows deployment of provisioned systems without concern of hardware and/or software tampering and subsequent extraction of sensitive material -- a provisioned system can be guaranteed to be answering only to its previously configured owner, not the owner of the physical space in which the system resides. This is a major departure from prevailing security models, which largely assume that either the possibility of physical access by a malicious actor must result in loss of trust of the affected system, or that trust must be delegated to the system vendor in all situations.

How is FlexVer™ different than Intel® Boot Guard™ and related technologies?

Unlike existing security technologies, FlexVer™ does not depend on a fully trustworthy vendor for the root of system trust. Recent events have shown that this trustworthy vendor assumption is not valid, and in fact there is strong pressure on all vendors to compromise their root of trust for financial gain, warrant-related data extraction, industrial espionage, and related purposes. Any given security technology is only as secure as the weakest link in the chain; Boot Guard™ and related technologies operate by permanently locking the hardware to a vendor-controlled signing key, not only keeping the vendor in complete control of the hardware at all times, but also creating a single point of failure by which millions of systems could potentially be compromised with a single hack or leaked key. Effectively, the vendor and their partners' software, data security processes, and key handlers have become the weakest link in the chain, offering a large attack surface and severely weakening all systems based on this security model.

In contrast, FlexVer™ abandons this centralised security model, using a distributed, locally-verified model instead. FlexVer™ becomes the local root of trust for each protected system, removing the possibilty of a single data breach compromising all systems simultaneously and eliminating the capability for a vendor or its affiliates to access protected data on your system. Under the FlexVer™ security model, each system is provisioned in a secure, trusted physical environment by trusted members of an organization. The FlexVer™ hardware definition files and resultant bitstream are verified to be trustworthy, and this trusted bitstream is then loaded into the FlexVer™ hardware. Immediately upon FlexVer™ startup, a unique internal key is generated to protect the system from any form of tampering; this key allows FlexVer™ to operate in conjunction with a standard TPM, and to only allow the TPM to unseal if the FlexVer™ hardware and system firmware have not been modified. Critical data, such as disk or application encryption keys, are then loaded into the TPM, completing the provisioning process. FlexVer™ continues to guard against any unauthorised modification to hardware, firmware, or software, and will render all data stored withing the TPM permanently inaccessible if the FlexVer™ hardware is tampered with in any way.



RAPTOR ENGINEERING®

A Flight Above the Rest!™

System Architecture with FlexVer™

CPU and Main System Logic
LPC Master
LPC Guard™
Physically Secure LPC Bus Segment
Verification Side Channel
Tamper Evident Region – Physical Access Restricted
Cryptographic Engine
FlexVer™ System
SRAM
Tamper Detect
JTAG
SPI Master
TPM
Standby Power
JTAG Header
Firmware Storage
Security Control Switches

Copyright © 2016 Raptor Engineering, LLC All Rights Reserved

Figure 1: FlexVer™ Architecture

How does FlexVer™ protect my data against physical attack?

FlexVer™ introduces a shielded area onto the system board; this shielded area contains the main FlexVer™ control FPGA, temporary storage (SRAM), and the system's root TPM. This shielded area is highly resistant to physical attack, and any attempt to physically penetrate this area will result in key destruction and immediate loss of the sensitive data stored within the TPM. Unlike existing solutions, the logic used to implement FlexVer™ inside the shielded area is completely open; not only can FlexVer be completely audited, but if any flaw is found within the FlexVer™ system, all affected systems may be reprovisioned using an updated copy of FlexVer™.

Placement of the root TPM within the shielded area is vital. A standard TPM is generally secure against offline (cold) attack; if a TPM is powered down and removed from the mainboard extraction of key material is nearly impossible. However, the same TPM is not secure against online (warm) attack; there are multiple attack vectors that rely on hardware access to extract key material, override the TPM, hijack the root of trust, and otherwise compromise the integrity of the secure platform.

Finally, the internal storage is critical to preventing timing attacks on the system firmware. By loading the CRTM from the external firmware storage device prior to cryptographic validation, it is not possible to bypass verification with an authorised copy of the firmware, then substitute an unauthorised version at runtime. All three devices within the shielded area handle highly sensitive data vital to assuring the integrity of the system platform, therefore FlexVer™ has been designed to "fail safe" and erase its internal key at the first sign of trouble. It is far easier to physically pull, verify, and reprovision a system than it is to clean up after a data breach or rebuild a compromised system!

What systems is FlexVer™ available for?

Our Talos™ system comes with FlexVer™ and LPC Guard™ integrated directly onto the mainboard. FlexVer™ will also be available for the ASUS KGPE-D16 in 2017 as an add-on module, and we hope to see our FlexVer™ technology integrated into other systems in the future. If you or your company would like to integrate FlexVer™ into an upcoming product or use FlexVer™ internally on custom hardware, please contact us directly; we welcome all interested parties from small organizations to large corporations.

How do I provision FlexVer™?

FlexVer™ is provisioned in several stages to ensure full integrity. Depending on the value of the stored data, steps may be skipped or bypassed based on a given organization or individual's requirements. Provisioning should always start with the machine powered down in a physically trusted environment, and a previously validated FlexVer™ bitstream, platform firmware image(s), and operating system. The machine should be physically inspected, focusing on the FlexVer™ shielded area and looking for any signs of damage or tampering. The system CMOS battery should also be checked at this time and replaced if necessary. If physical inspection passes, the FlexVer™ bitstream should be loaded into the FlexVer™ control FPGA, and the platform firmware image(s) should be loaded into the appropriate Flash storage device(s). At this point the system can be powered on, and the operating system installed. After installation, the TPM may be provisioned, and sensitive data stored within the TPM via the appropriate standard utilities. Once this process is complete, the system is fully provisioned, and is ready for deployment outside of the physically trusted provisioning environment. This provisioning process may be repeated at any time if desired.

What happens if FlexVer™ detects tampering?

FlexVer™ immediately deletes its internal key and issues a system reset, rendering all data previously stored within the TPM permanently inaccessible. If a tampering event is detected in error, for instance if the system is unplugged with a discharged CMOS battery, the system may be inspected, reprovisioned, and put back into service. If the FlexVer™ shielded area was in fact physically tampered with, as evident during visual inspection, that particular system should no longer be used for secure purposes.

Where can I find more information on the design of FlexVer?

A whitepaper detailing the security features of Talos™, including FlexVer™, is available at https://www.raptorengineering.com/TALOS/security_features.php

© 2016 Raptor Engineering, LLC, All Rights Reserved
FlexVer™ and related technologies may be covered by one or more U.S. patent(s) or patent application(s)
For licensing information, please contact Raptor Engineering at sales@raptorengineering.com