White Paper

Security

Federal and Aerospace

Applying wolfBoot to 11th Gen Intel® Core™ Processors for Secure Boot

Authors

Lauri Minas - Intel
Christopher Conlon - wolfSSL

Table of Contents

Authors 1

Introduction...1

wolfBoot Secure Bootloader 1

11th Gen Intel® Core™ i7 Processors 2

Replacing Intel® Slim Bootloader with wolfBoots..2

Better Together: wolfBoot and Intel 3

Conclusion and Next Steps 4

Introduction

11th Gen Intel® Core™ i7 processors include security features out of the box that make them an ideal processor choice for a number of project designs [1]. Some of these include Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) , Intel® Advanced Vector Extensions (Intel® AVX2, Intel® AVX-512), and UEFI Secure Boot [2]. Given an excellent set of features offered by Intel processors, some users and Intel-based projects will benefit from extending the boot process using a second stage bootloader subsequent to Intel's UEFI. This paper will introduce the wolfBoot secure bootloader, 11th Gen Intel® Core™ i7 processors, and how wolfBoot can replace Intel® Slim Bootloader to provide certified and customized solutions such as securely unlocking a SATA drive using the trusted platform module version 2.0 (TPM 2.0) during boot.

wolfBoot Secure Bootloader

wolfBoot [3] is a portable secure bootloader solution that offers firmware authentication and firmware update mechanisms. Due to its minimalistic design and tiny Hardware Abstraction Layer (HAL) API, wolfBoot is completely independent from any operating system (OS) or bare-metal application.

wolfBoot can easily be ported and integrated in existing embedded software projects to provide a secure firmware update mechanism. Upon installing a verified update, wolfBoot creates a backup copy of the last firmware image known to work correctly. If the new version is not confirmed by the application, or if the image installed is somehow corrupted, the bootloader will restore the state of the system before the most recent update.

wolfBoot supports multi-slot partitioning of memory, integrity verification of firmware images using SHA2 or SHA3, and authenticity verification of firmware images using wolfCrypt's digital signature algorithms (ECDSA SECP256R1/SECP384R1, RSA 2048/3072/4096, and ED25519). It provides a highly reliable transport-agnostic firmware update mechanism with anti-rollback protections, hardware-assisted dual bank swapping, support for key storage and One-Time Programmable (OTP) memory. wolfBoot can utilize a variety of memory types and locations, including SPI/QSPI, NOR, NAND, eMMC, and SSD, among others.

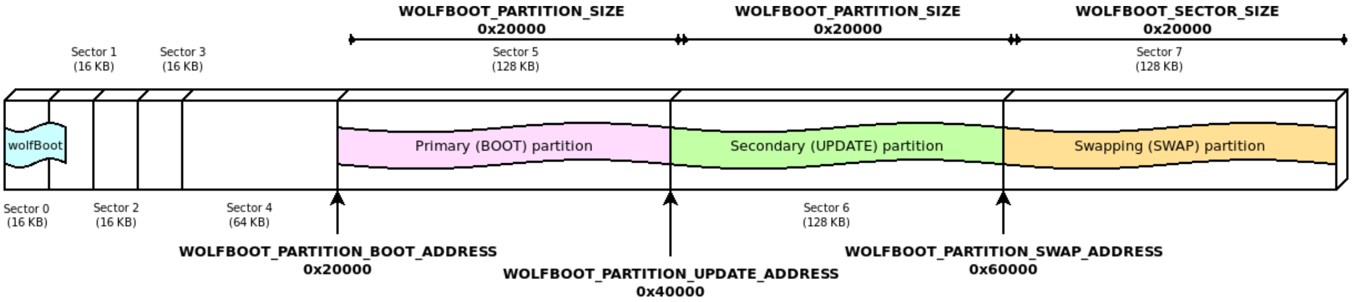

Figure 1: Example partitions in STM32F4

TPM 2.0 modules are becoming widely used for secure key generation and storage as well as cryptographic operations. wolfBoot supports the use of TPM 2.0 modules if available on the platform for hardened security.

For sensitive firmware images and use cases, wolfBoot supports encrypted firmware images. One of the frequent concerns when it comes to secure boot is the protection of data at rest when firmware updates are received and stored on unprotected non-volatile memory, such as external SPI FLASH devices or other customized forms of storage. With wolfBoot, each firmware update can be signed and encrypted to be distributed to the target and the application can set a decrypt key at runtime, using wolfBoot's API. Images stored in the update partition will always be encrypted when using this feature, including the backup copy of the previously running system during installation.

For minimizing the size of firmware transferring to a device, wolfBoot supports delta updates. With delta updates, only a comparison between the old and new firmware images needs to be signed and sent to the device. This can reduce both transfer time and cost (if a per-byte fee is applicable) by reducing total update size.

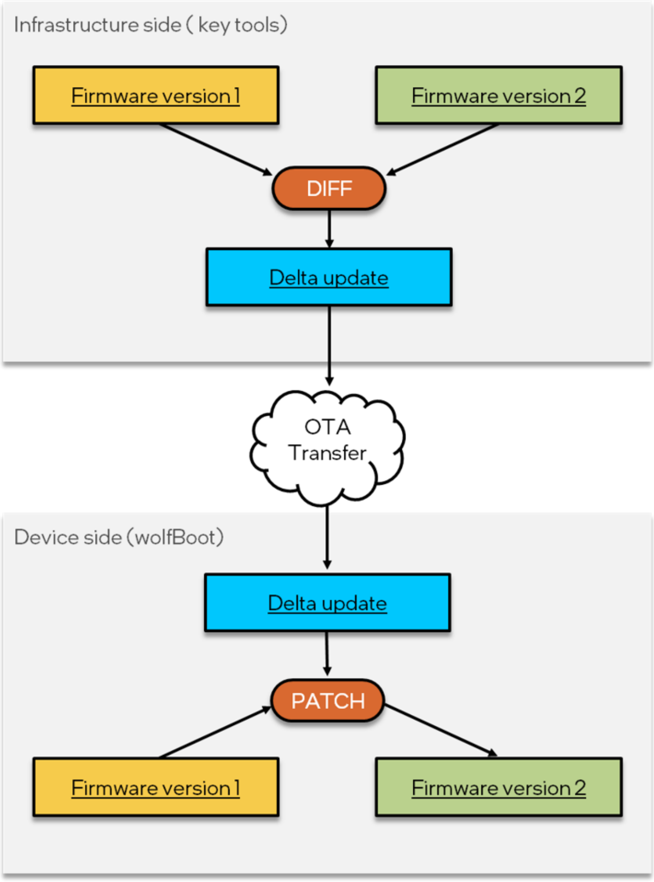

Figure 2: Delta updates are signed to reduce size of firmware

wolfBoot is also an excellent solution for users requiring certified code. The wolfCrypt cryptography library which provides cryptographic services to wolfBoot has been FIPS 140-2 validated [4] and DO-178C DAL-A certified [5]. wolfBoot uses safe coding practices with no dynamic memory use, a feature useful in safety-critical applications as well.

11th Gen Intel® Core™ i7 Processors

11th Gen Intel® Core™ processors transform hardware and software efficiencies and takes advantage of Intel® Deep Learning Boost to accelerate AI performance. Key platform improvements include memory support up to DDR4-3200, Intel® Iris® Xe Graphics, up to 20 CPU PCIe 4.0 lanes, integrated USB 3.2 Gen 2x2 (20G), Intel® Optane™ memory H20 with SSD support, and hardware-based security.

The hardware-based security features on 11th Gen Intel® Core™ processors include: Intel® AES New Instructions (Intel® AES-NI), Intel® AVX2, Intel® BIOS Guard, Intel® Boot Guard, Intel® Control Flow Enforcement Technology (CET), Intel® Platform Trust Technology (Intel® PTT), Intel® Runtime BIOS Resilience, Intel® Total Memory Encryption (Intel® TME), and Intel® Trusted Execution Technology (Intel® TXT).

Replacing Intel® Slim Bootloader with wolfBoots

a) Intel® Slim Bootloader

The Intel® Slim Bootloader (Intel® SBL) is designed to be small, fast, secure, extensible, and configurable [6]. It is an open source boot firmware designed to be secure and optimized on Intel x86 architectures. Intel maintains Intel® SBL as open-source code on GitHub [7]. It uses a linear staged boot flow to initialize the platform and launch the operating system, consisting of the following four stages [8]:

Stage	Description
Stage 1A	Pre-memory initialization
Stage 1B	Initialize main memory
Stage 2	Post memory initialization: initialize CPU, I/O controllers, devices, etc.
Payload	Load, verify and launch OS images; or perform firmware update.

Figure 3: Four Stages of boot flow to launch platform and OS

Intel® SBL uses the Intel® Firmware Support Package (Intel® FSP) to provide programming information for initializing Intel platforms, using Intel® FSP Specification v2.x [9]. It can be easily integrated into boot loaders and includes CPU, memory controller, and Intel chipset initialization.

Intel® SBL can boot a Unified Extensible Firmware Interface (UEFI) payload, including support for multiple payloads. UEFI is a specification that describes an interface between the operating system (OS) and the platform firmware, and acts as a replacement for previous BIOS-like firmware. With similarities to Intel® SBL, wolfBoot has also been designed to be a lightweight, secure, and portable bootloader solution. wolfBoot can run inside the UEFI environment on Intel x86_64 machines then be used to load and verify other EFI applications. This includes verifying Linux on a UEFI machine (Linux supports booting as an EFI application).

b) Why Replace Intel® Slim Bootloader with wolfBoot?

Depending on application and use case, several scenarios might necessitate the replacement of the Intel® SBL with the wolfBoot Secure Bootloader. One such example is the application of wolfBoot in avionics systems. Avionics software commonly requires DO-178C certification meeting a specified Design Assurance Level (DAL). Intel® SBL does not directly provide DO-178C certification or a path to certification, making this a timely and costly endeavor for avionics vendors. Contrarily, wolfBoot can be taken through the certification process by wolfSSL Inc. with certification evidence delivered to meet the avionics application requirements. Line count can be minimized through feature configuration and code tuning, reducing cost and total time to market.

wolfBoot is flexible and customizable in its use of hardware-based cryptography and secure key storage solutions. This includes support for calling Intel-specific hardware optimizations (Intel® AES-NI, Intel® AVX2) and secure key storage solutions such as TPM 2.0 if available. A specific example of one wolfBoot use case required a DO-178C certified codebase in addition to utilization of a TPM 2.0 module by wolfBoot to unlock a Serial-Attached SCSI (SAS) hard disk using keying material stored in the TPM 2.0 module during device boot.

Other scenarios can also necessitate a replacement of Intel® Slim Bootloader with wolfBoot, including but not limited to requirements to use FIPS 140-2 or FIPS 140-3 validated cryptography as part of the secure boot solution, or use of a CAVP or an ACVP validated cryptography.

c) wolfBoot Modifications

To allow for easy replacement of Intel® Slim Bootloader, several changes and additions were made to wolfBoot. Changes included adding support for calling Intel® FSP microcode API's, adding a Stage 1 loader similar to mentioned above for memory initialization, adding drivers for Watchdog (CPLD)/UART/SPI, adding support for multiple signed partitions, adding support for multiboot and ELF32, adding support for calling Power-On Built-in Tests (PBIT) tests, adding support for a TPM-based root of trust and measured boot, and adding support for SATA drive unlocking.

Part of replacing an existing solution is doing extensive testing to ensure a robust replacement solution has been installed. With these modifications, wolfBoot was tested on a Quick EMUlator (QEMU) and with 11th Gen Intel® Core™ processors. Boot failure case testing ensured expected behaviors are manifested in failure conditions, complementing successful boot testing.

Better Together: wolfBoot and Intel

Hardware and software must work together in a reliable, performant and secure manner to provide a cohesive solution. 11th Gen Intel® Core™ processors provide a foundation on which secure software can be written and deployed. But, hardware itself doesn't meet the full requirements of applications and projects without the right software running on top.

When wolfBoot is running on 11th Gen Intel® Core™ processors, the wolfCrypt cryptography library can take advantage of Intel® AVX2's instructions to accelerate SHA2-256 and SHA2-384 algorithms used for verifying firmware integrity. If encrypted firmware images are used with AES-128 or AES-256, wolfBoot can leverage the Intel® AES-NI instructions to accelerate encryption and decryption operations.

The table below shows the performance improvement when using wolfCrypt with Intel® AES-NI and Intel® AVX2 instructions. This was measured using the wolfCrypt benchmark application, which is distributed as part of the wolfSSL 5.5.3 download.

System Configuration for Measurement

Processor: 11th Gen Intel® Core(TM) i7-1165G7 @ 2.80GHz, 2803 Mhz, 4 Core(s), 8 Logical Processor(s)

Graphics: Intel(R) Iris(R) Xe Graphics

Memory: 32.0 GB (31.8 GB usable)

OS: Windows 10 Version 21H2 64-bit operating system, x64-based processor

Storage: NVMe__WDS100T1X0E-00AF0

BIOS: INSYDE Corp. 03.10, 7/19/2022

Boot Loader: wolfSSL 5.5.3; wolfCrypt 5.5.3; wolfBoot 5.5.3

Intel does not control or audit third-party data. You should consult other sources too.

Algorithm	Software Throughput (MiB/s)	Intel® AES-NI + Intel® AVX2 Throughput (MiB/s)	Percent Increase
AES-128-CBC-enc	315	1903	503%
AES-128-CBC-dec	353	12203	3359%
AES-256-CBC-enc	237	1398	490%
AES-256-CBC-dec	249	8931	3488%
SHA2-256	255	465	82%
SHA2-384	441	721	63%

Table 1: Performance improvement using wolfCrypt with Intel® AES-NI and Intel® AVX2 instructions

Using Intel® AES-NI and Intel® AVX2 also reduces cycles per byte for these operations, which can reduce the power and energy used by cryptography operations. This is shown by the percent reduction in cycles per byte in the table below.

Algorithm	Software Cycles Per Byte	Intel® AES-NI + Intel® AVX2 Cycles Per Bytes	Percent Decrease
AES-128-CBC-enc	8.48	1.41	83%
AES-128-CBC-dec	7.58	0.22	97%
AES-256-CBC-enc	11.29	1.92	83%
AES-256-CBC-dec	10.85	0.30	97%
SHA2-256	10.47	5.78	44%
SHA2-384	6.06	3.71	38%

Table 2: Percent reduction in cycles per byte using wolfCrypt

As can be seen by these numbers, using wolfCrypt and wolfBoot together on 11th Generation Intel® Core™ processors provides a substantial improvement over using one or the other separately. With Intel's focus on processor and platform security, there is also room for wolfBoot to be extended to support other features as well.

Conclusion

The 11th Gen Intel® Core™ processors provide a foundation with reliability and security on which to build a secure boot solution. The Intel® Slim Bootloader meets the needs of many applications and projects, but for cases requiring custom use of security modules, custom workflows, DO-178C certification, or FIPS 140-2 / FIPS 140-3 validated cryptography, replacing Intel® Slim Bootloader with wolfBoot provides better performance of security encryption algorithms.

Learn more

To learn more about wolfBoot and using it on Intel processors, contact wolfSSL at facts@wolfssl.com. wolfSSL Inc.

wolfSSL focuses on providing lightweight and embedded security solutions with an emphasis on speed, size, portability, features, and standards compliance. Our products are Open Source giving customers the freedom to look under the hood. wolfSSL provides embedded security products utilizing cryptography. wolfSSL products are built completely from the ground up, written in native C code, modular, customizable, on average ten times smaller than OpenSSL, and see 1/10th of the Common Vulnerabilities and Exposures. wolfSSL has a mean time to release a fix for vulnerabilities of less than 36 hours, offers commercial support up to 24/7, and has the best tested cryptography and the largest team of software engineers dedicated to crypto in the market today.

Learn more about 11th Gen Intel® Core™ processors

11th Generation Intel® Core™ processors redefine Intel® CPU performance for laptop and desktop PCs. New core and graphics architectures, AI-based performance boosts, best-in-class wireless and wired connectivity, and advanced tuning features deliver higher levels of power and flow to support your aspirations.

References

[1] https://www.intel.com/content/dam/www/central-libraries/us/en/documents/white-paper-11th-gen-intel-core-processor-security.pdf

[2] https://builders.intel.com/docs/networkbuilders/secure- the-network-infrastructure-secure-boot-methodologies.pdf

[3] https://www.wolfssl.com/products/wolfboot/

[4] https://www.wolfssl.com/license/fips/

[5] https://www.wolfssl.com/wolfssl-support-178-dal/

[6] https://slimbootloader.github.io/introduction/index.html

[7] https://github.com/slimbootloader/slimbootloader

[8] https://slimbootloader.github.io/developer-guides/boot-flow.html

[9] https://www.intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

No product or component can be absolutely secure. Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.