CONCURRENT TECHNOLOGIES

Step by Step Instructions for creating Signed Secure Bootable VxWorks 7 UEFI Boot Loader and Signed Final Images

Contents

Summary

To understand why the associated application note is of value, we must first establish why VxWorks is being used, and the relevance it has within the current embedded systems market. This short publication aims to give a brief overview of VxWorks, UEFI Secure Boot and why they are used in Concurrent Technologies' Embedded Solutions.

Definitions

According to Search Networking, Tech Targets (2007)[i] "VxWorks is a real-time operating system (RTOS) that can be used in embedded systems." Use of the system allows the user to "control network and communication devices, test and measurement equipment, computer peripherals, automotive systems, avionics (aeronautics and astronautics) equipment and diverse consumer products."

As explained by the Microsoft (2019)[ii] "Secure boot is a security standard developed by members of the PC industry to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM)."

How they Work? And why Concurrent Technologies use them?

In an era where security is paramount in many systems, it is intrinsic for users to be able to boot and load software that is guaranteed to be as secure by using a trust-based mechanism. Using UEFI Secure Boot allows the user to have confidence in their systems functioning as intended, without the possibility of any tampering or altering of the operating system and associated drivers. UEFI Secure Boot ensures successful boot up by verifying each stage – this ensures that only the correct Software is loaded and run so that malicious code cannot be executed at this stage of the boot process. This is one of the key characteristics about Secure Boot, and the main reason Concurrent Technologies choose to incorporate it into their embedded systems.

VxWorks, as previously mentioned is a real-time operating system, this means users can control their application in the correct time frame. Operating systems are categorized based on their latency; the lower the latency a system allows, the better it is for real-time operation and the more effective and efficient it is for typical applications within the defense industry. Latency, in layman's term, is how responsive a system is and for VxWorks the interrupt latency is typically around 100µs.

Other operating systems, such as Windows, may appear real-time due to their perceived speedy response times to a user request, however the latency is likely to be in the order of ms rather than µs. In addition, due to the fact the user is not in control of what is happening/processing when using Windows, there are inconsistencies in response time that are a barrier to it being used for real-time solutions. Applications within the defense industry require a deterministic response, so that processes complete within a consistent time frame. Using VxWorks ensures applications and products are working within tight latency in a deterministic fashion to enable complete control of the operating system for the user.

Advantages and Limitations

As with all applications, there are advantages and limitations that must be considered when using RTOS and UEFI BIOS'.

VxWorks:

- ✓ The use of RTOS allows maximum consumption of the system – The user can keep all devices active, with a large resource output
- ✓ RTOS are mostly, if not always error free – This means the user can have confidence of fewer system crashes or other foreseeable issues that could affect their application
- ✓ Finally, the use of an RTOS allows the user to focus on the application. This is because no 'unknown' background tasks are executed and so complete focus falls to the current task. Less action or management is required and exact results can be given on the current work execution
- X Ease of application – RTOS are known for their ease of access when it comes to installation. Due to the desire for proficiency in programming there is an often-difficult process involved during set up
- X Following in a similar path to the previous disadvantage is the complex algorithms and codes required for use. A desired outcome is a result of complexity in designing algorithms and precise codes. This is an obvious disadvantage for a user with less experience or technical knowledge
- X Finally, the systems, due to their expert application are more expensive. Expense in resources required to run, and even more expensive with regards to the knowledge required to set up and use them.[iii]

UEFI Secure Boot:

- ✓ One obvious advantage is the use of Secure Boot itself. This ensures no tampering or external corruption of the operating system due to the advance security the system holds
- ✓ A simplified boot process allows shorter OS load times. An increased load time is often crucial in many situations and an obvious advantage of Secure Boot
- ✓ Finally, a secondary partition is stored in another location. Meaning in the event of an unforeseeable crash, you are ensured that your partition table can be retrieved and recovered without any secondary corruption
- X One key disadvantage is there is an overhead to a system that doesn't really need it. One example would be 32-bit pointer-sectors for partitions that only need to load an operating system
- X Finally UEFI still doesn't fix one of the problems of our old BIOS/MBR setups. We still have to re-probe for devices once the operating system loads[iv]

The Application Note

The application note, entitled: Step by Step Instructions for creating signed Secure Bootable VxWorks 7 UEFI Boot Loader and signed final images, provides the reader with an overview of how a user can create a signed Secure Bootable VxWorks 7 UEFI Boot Loader and signed VxWorks final images. It is important to note, that the application note has been written under the pretenses that the user is familiar with configuring, building and creating VxWorks images and they are doing so on a device that already has the Concurrent Technologies supplied Board Support Package. The application note does however touch upon how a user can include the Security package, if they have not already installed it. A final thing to remember is that the signature created in this example are those created by the WindRiver Workstation Software. It is possible to use one's own signature list, however this is beyond the scope of the application note.

---

[i] *The definition of VxWorks can be found here: https://searchnetworking.techtarget.com/definition/VxWorks*
[ii] *The definition of Secure boot can be found here: https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot*
[iii] *Advantages and Disadvantages of using RTOS as explained by ITRelease (2014): http://www.itrelease.com/2014/07/advantages-disadvantages-real-time-operating-systems/*
[iv] *Advantages and Disadvantages of Secure Boot as explained by Phoenix TS (2016): https://phoenixts.com/blog/booting-uefi-mode/*