What’s New in QNX Neutrino OS 7.0

BlackBerry | QNX

The leading mission-critical OS gets a major update with a focus on security

QNX Neutrino is a fundamentally safe microkernel architecture OS which has evolved since its creation in 1982 to further increase its reliability in mission-critical applications. In the connected world, safety can only be assured by tackling the security threats which represent a growing challenge to operating integrity. Thus in QNX 7.0, while introducing improved safety features and supporting new processors, the key focus – leveraging Blackberry’s unrivalled pedigree in this area – was to create the world’s most secure embedded OS.

The main improvements in QNX 7.0 can be summarized:

- Security features
- 64-bit support
- New/updated safety certification and manuals
- Tools, libraries and API

Where safety and security converge

Most of the many new features in QNX 7.0 improve safety by addressing security threats. Sometimes, the boundary between safety and security driven features is not distinct - for example, the High Availability Manager fundamentally improves safety because it will act as a safety-net to detect and recover failure of system processes or services; however by ensuring resilience it is also a valuable security feature in a system under attack.

The overarching advantage of QNX, leveraged by many of the new features, is the microkernel (vs. monolithic kernel) architecture which means that the sustained operation of the OS kernel is not contingent on the integrity of drivers, which can be stopped and started independently. This is explored in a recent (entirely independent) paper: “The Jury Is In: Monolithic OS Design Is Flawed:Microkernel-based Designs Improve Security”

Security features and enhancements

Most security-oriented features have been improved or are new in QNX 7.0.

Pluggable Authentication Module

OpenPAM is a standard which supports authentication and identification and is newly integrated with QNX Neutrino 7.0. Via standardized methodologies, the PAM allows the developer to create authentication dialogues and manage users.

Relevant QNX modules such as login, ftpd, passwd, su are therefore now PAM-aware.

This important feature allows users to implement a systematic approach to user authentication which is less likely to be vulnerable to attack.

What is QNX?

Over the past 35 years, QNX software has become a big part of everyday life. People encounter QNX-controlled systems whenever they drive, shop, watch TV, use the Internet, or even turn on a light. Its ultra-reliable nature means QNX software is the preferred choice for life-critical systems such as air traffic control systems, surgical equipment, and nuclear power plants. And its cool multimedia features have QNX software turning up in everything from in-dash radios and infotainment systems to the latest casino gaming terminals.

Direct Insight is QNX’s UK partner. As well as supporting all development with QNX, we offer hardware solutions with QNX 7.0 compatibility guaranteed – including our TRITON-TX6 range of ARM modules with i.MX6 processor, providing a flexible range of system-level options.

© Direct Insight Limited 2018. This document may be distributed unmodified - see page 5 for terms

Rootless Operation

While all developers know that it is good practice to ensure that only the most essential tasks are running as root, in a monolithic OS it is nevertheless understood that that many processes, including drivers and services, must run at this privilege level. This is not so in a microkernel OS architecture, and as of 7.0, QNX offers a policy-driven approach which allows non-root processes to be dynamically granted “abilities” which permit selective access to privileged operations.

This makes it possible to architect a system with no processes running as, or objects owned by, root, which by means of good programming should make it effectively impossible to achieve root privilege escalation – a well known and difficult to defend attack strategy whereby an attacker might look for an object that already has root privileges and then co-opt it for malicious purposes.

Mandatory Access Controls

Access controls, first introduced in QNX 6.6, are a mechanism used to secure a system by limiting the actions available to a process. 7.0 sees the introduction of “Mandatory Access Controls” which are defined by a formal security policy, which is developed and expressed as a text source file with the aid of utilities. These controls are then enforced by the process manager rather than at the discretion of individual processes.

Access controls constrain the ability of a process to connect to channels of other processes – and all channels of communication must have a corresponding declaration.

Because security policy can be developed and formalised independently of application development (ideally by a person outside the coding team), safety is enhanced by the associated diversity and redundancy, while security is inherently improved by the explicit control of process interaction.

Access Control Lists

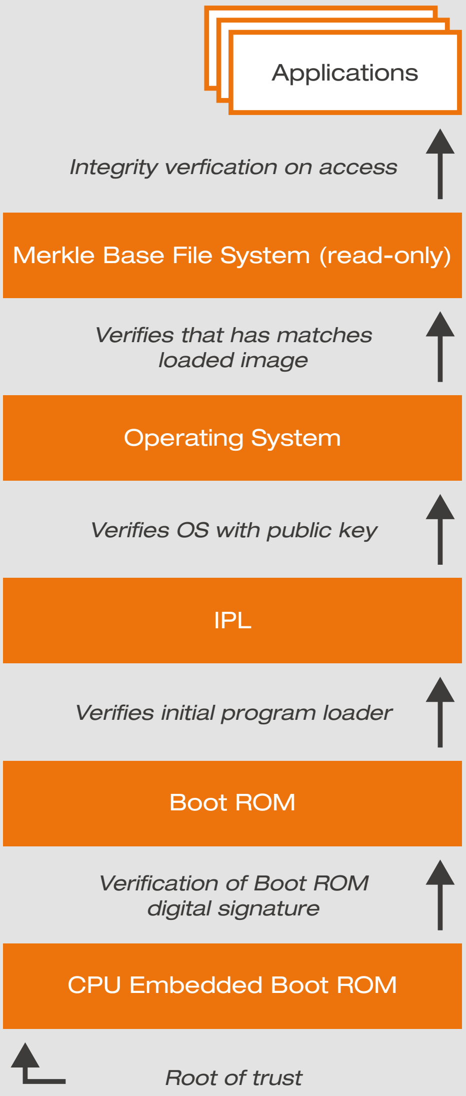
ACLs extend the traditional permissions as set with chmod, giving the user finer control over access to files and directories. In QNX 7.0 ACLs are fully implemented for the first time

Secure Boot

The secure boot mechanism is based on the concept of a chain of trust. This kind of chain relies on a key hash hardware-programmed into a compatible processor or SoC, which is inherently trusted. A secure state machine within the processor hardware allows only a correctly signed image to boot. This chain of trust is then extended via a public key known to the firmware, where the private key is used to sign files such as the IFS image. A Merkle filesystem provides integrity protection via a hash tree of all filesystem blocks which are verified on demand. The root hash of the tree is signed with a key pair providing assurance that the filesystem has not been tampered with. Accessing a part of the filesystem which fails the integrity check returns an error.

The result is a system which is virtually impervious to attack at start-up as it will only run a trusted image and file-system. In practice secure-boot implementation is moderately challenging, and so QNX 7.0 provides a framework which facilitates setup.

The Secure Boot Chain of Trust


Applications
Integrity verfication on access
Merkle Base File System (read-only)
Verifies that has matches loaded image
Operating System
Verifies OS with public key
IPL
Verifies initial program loader
Boot ROM
Verification of Boot ROM digital signature
CPU Embedded Boot ROM
Root of trust

© Direct Insight Limited 2018. This document may be distributed unmodified - see page 5 for terms

Secure Logging

With QNX 7.0, system activities are automatically logged in order to detect security violations (realized or attempted) or anomalous behaviour in the system. Events such as file and device accesses are recorded in a hashed and therefore tamper-proof log file.

Networking Security

The network stack provided enhanced security starting with QNX 6.6, with minor updates and improvements in 7.0. The network stack supports industry standard security protocols including TLS, SSL, IPSEC & HW crypto-offload Access to the stack, services and ports are restricted via security policy using pathspace control, process manager abilities and mandatory access controls newly introduced in QNX 7.0. OpenVPN has been validated with QNX 7.0.

Pathspace Control

Pathspace control restricts the access of a process to a system's path space by trapping connect messages and matching the given path against a list of allowed and forbidden patterns. In QNX 7.0 Pathspace Control is implemented as a feature of Security Policy

Process Protection

In QNX 7.0, guard pages – a reserved area immediately after the assigned memory area that the thread can't write to - for heaps and stacks are implemented by default to provide resilience against overflow. Address Space Layout Randomization (ASLR) randomizes the stack start-address and code locations in executables and libraries, and heap cookies. This makes buffer overflow and code or data-injection attack far more difficult to achieve.

Anomaly Detection

New in QNX 7.0, the anomaly detection utility monitors the system to detect anomalies in runtime behaviour, after learning the expected behaviour and determining a system signature. Unexpected behavioural changes could indicate that someone unauthorized is accessing the system, perhaps with the intention of exploiting it. In the absence of a clear attack pattern, the anomaly detector may notice something important that could be otherwise overlooked. Where an anomaly is detected a user-defined response, such as a warning message or shutdown is initiated.

Adaptive Partitioning

First introduced in QNX 6.6, and improved and refined in QNX 7.0, adaptive partitioning greatly increases resilience against outside attack (and safety with respect to other unexpected conditions) by providing effective temporal partitioning. This means that each process can be assigned a maximum share of available processor time, so that should it malfunction is such a way as to make extreme demands on processor resources – as might be expected to happen during a Denial of Service (DOS) attack – the scheduler will automatically implement a limit, so that the rest of the system does not experience starvation. The system is configurable at run-time, and automatically releases resources required to maintain minimum processor share for any partition group of threads, processors or applications, which are therefore only reserved according to dynamic demand.

Direct Insight now offers a QNX 7.0 BSP for the pin-compatible TRITON-TX range of system-on-modules.

With processors ranging from the quad-core i.MX6 QuadPlus with enhanced, HD-ready graphics, to the low-power low-cost single-core i.MX6 UltraLite, TRITON-TX6 offers a tried-and-tested path for ARM-based QNX users as well as a cost and power-reduction migration opportunity for x86 users, with even higher performance pin-compatible 64-bit i.MX8 solutions in the works.

As well as our in-house QNX 7.0 BSP, Direct Insight offers consultancy and production programming facilities to allow Secure Boot implementation via NXP's "High Assurance Boot" features.

Direct Insight also provides complete board and box level solutions based on TRITON-TX modules with i.MX6 processors.

© Direct Insight Limited 2018. This document may be distributed unmodified - see page 5 for terms

High Availability Manager

Available from QNX 6.6, the High Availability Manager (HAM) is not a new feature of QNX 7.0, but is worth including in any list of security features given its critical role in ensuring system resilience. The HAM is a "smart watchdog" which transparently monitors key processes and system services and can perform a multistage recovery when they fail, do not respond, or provide an unacceptable level of service. A mirror process called the Guardian monitors the HAM in turn.

64-bit support

x86 processors have offered 64-bit operation for a while, and the latest generation of ARM processors featuring the ARMv8 instruction set offer a 64-bit architecture and are optimized for 64-bit operation. Use of 64-bit execution allows the maximum performance to be achieved for a given processor and in many cases permits the use of a less expensive processor than would be required by the same application running in 32-bit mode. Additionally 64-bits means expansion of the address space beyond 4GB. QNX 7.0 introduces 64-bit support, and includes support for x86 family processors in 64-bit mode as well as many new processor families including NXPs i.MX8, Xilinx Ultrascale, and Qualcomm 820A. Many new ARM v7 BSP have also been added in QNX 7.0, as well as support for the latest GPU architectures, and big-little cluster support.

Safety Certifications

QNX OS 7.0 for Safety has been newly certified according to ISO 26262 ASIL D and IEC 61508 safety standards, with medical certification of QNX OS 7.0 for Medical to IEC62304 pending completion in 2018.

Other improvements

There are many other enhancements which debut in QNX 7.0. Since the focus of this report is the security features, these improvements are simply listed below for completeness:

- New USB Stack, including USB 3.0 SuperSpeed
- Audio Enhancements – Audioman, LoLAA
- Command line tools including LLVM, hardfloat support
- Valgrind integration within IDE
- Momentics updates: Neon IDE, C++14/C11 awareness, usability enhancements
- Qt support
- Unit test framework (supports Google Test)
- QNX Software Centre for licence management / updates
- POSIX Compliance to PSE52
- DBUS implementation
- New PCI Server
- UEFI startup support. Intel Speedstep

Rugged industrial PCs qualified with QNX 7.0

ECD700 tiny industrial PC

Low-power and lightweight, the ECD700 is a tiny industrial PC with surprisingly good performance and dual display support, thanks to a quad-core E3845 Bay Trial processor. The ECD700 offers a number of features suited to mission-critical environments, such as ECC RAM and optional SLC industrial class mSATA storage.

Direct Insight is a worldwide supplier of hardware solutions for QNX 7.0, as well as Blackberry QNX's official UK and Ireland distribution.

If you have a QNX question please don't hesitate to get in touch:

Direct Insight Ltd.
The Hayloft, Greatworth Hall,
Greatworth, Banbury, Oxfordshire,
OX17 2DH, UK

Phone: +44 1295 768800
Fax: +44 1295 762499
Web: www.directinsight.co.uk

© Direct Insight Limited 2018. This document may be distributed unmodified - see page 5 for terms

DIRECTinsight
directinsight.co.uk

Direct Insight Ltd.
The Hayloft, Greatworth Hall,
Greatworth, Banbury, Oxfordshire,
OX17 2DH, United Kingdom

Phone: +44 1295 768800
Fax: +44 1295 762499
Web: www.directinsight.co.uk

© Direct Insight Limited 2018. You may freely distribute this white paper in unmodified form.
This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.