BlackBerry | QNX

How Your Choice of Software Impacts the Security of Medical Devices

Scott L. Linke

June 25, 2019

Cybersecurity Vulnerabilities

When medical devices get hacked, hospitals often don't know it

The threat to medical d
and it's a patient safet
compliance.

By Jessica Davis | May 11, 2018

The past three months have see
126 percent in the first quarter o
Recall Index. The biggest culprit
increase in high-tech devices th

Emergent Tech ▸ Internet of Things

Medical device vuln allows hackers to falsify patients' vitals

McAfee: Patient monitoring systems open to hack attacks

By John Leyden 14 Aug 2018 at 08:05 14 SHARE ▼

Hackers may be able t
hospital networks.

healthcare informatics Health IT Summits Innovators

Healthcare Data Breach Costs Remain H
Per Record

July 13, 2018 by Heather Landi

The global average cost of a data breach is up 6.4 percent over the previous year to $3.

Click To View Gallery

The cost of a data breach for healthcare organizations continues t
$408 per record this year, as the healthcare industry also continue
breaches compared to any other industry, according to a new stud
Institute.

The global average cost of a data breach is up 6.4 percent over the previous year to $3.86 mill
to the 2018 Cost of a Data Breach study. The average cost for each lost or stolen record conta
sensitive and confidential information, globally and across all industries, also increased by 4.8
over year to $148. And, the 2018 cost of a data breach compares to $3.50 million in 2014, repr
nearly a 10 percent net increase over the past five years of the study.

For the eighth year in a row, healthcare organizations had the highest costs associated with data breaches – costing them $408 per los
record – nearly three times higher than the cross-industry average ($148). The next highest industry was financial services with an average of $206
per lost or stolen record. You can read about last year's study here.

6.1M healthcare data breach victims in 2018: 5 of the biggest breaches so far

Written by Julie Spitzer | August 22, 2018 | Print | Email

Share Tweet 8 Share G+

There have been 229 data breaches affecting 6.1 million individuals submitted to HHS' Office for Civil Rights' breach portal since the start of 2018, according to *HealthcareInfoSecurity.*

HIPAA-
incident
been c

Of the breache
individuals), 91
as theft or loss
disposal (affect
individuals).

Here are the fiv

1. West Des M
2. California De
3. Bartlett, Tenn
4. Baltimore-ba
5. SSM Health

Hacking

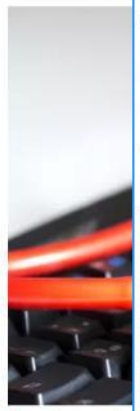
Hackable implanted medical devices could cause deaths, researchers say

Alex Hern in Las Vegas
@alexhern
Thu 9 Aug 2018 18.36 EDT

201

This article is over 3 months old

Medtronic, a manufacturer of pacemakers and implantable insulin pumps



Security researcher
can be hacked. Photo

A range of imp
vulnerabilities
that, if abused

ort the
has

million

3.15M Records Exposed by 142 Healthcare Data Breaches in Q2 2018

In the second quarter of 2018, 3.15 million patient records were compromised in 142 healthcare data breaches, according to the Protenus Breach Barometer.

By Fred Donovan

August 09, 2018 - In the second quarter of 2018, 3.15 million patient records were compromised in 142 healthcare data breaches, according to the **Protenus Breach Barometer**.

Why Medical Devices?

High value data with low barriers to intrusion…

- Medical devices are the key pivotal points of attack in a hospital network
- Network-Visible points of vulnerability
- Hardest endpoints to remediate, even when malware is detected

A Healthcare network:

- Replete with internet-connected systems and medical devices
- A highly connected device community that brings the most vulnerable devices together with some of the highest value data
- All devices are inter-connected with access to enterprise systems like Electronic Medical Records (EMR) and others.

Challenges for Healthcare Organizations

Healthcare IT teams typically cannot address malware on medical devices

- Don't have the product knowledge to access memory dumps on specific medical devices
- Detection and remediation tools don't exist
- Majority of the IT cyber-defense software products do not run on medical devices
  - Anti-Virus products run on open Windows, Linux IT servers
- Any software beyond a patch provided by the manufacturer might negatively impact FDA approval

Medical devices being treated as 'black boxes'

Healthcare organizations reverting to stronger language in Support Agreements from the device vendors

- Support Agreements typically pertain only to product functionality, not cyber-security
- Support technicians typically not trained or skilled sufficiently to handle complex security issues within an installed unit and prefer to replace the unit

Resources for Medical Device Developers

FDA

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
  - First issued Oct. 2, 2014 / NEW DRAFT Available for Review
- Cybersecurity for Networked Medical Devices Containing Offthe-Shelf (OTS) Software
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

IEEE

- Building Code for Medical Device Software Security

Industrial Internet Consortium (IIC)

- Industrial Internet Security Framework

FDA Guidance for Securing Medical Devices

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- First issued Oct. 2, 2014 / NEW DRAFT Available for Review
- Guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management

General Principles:

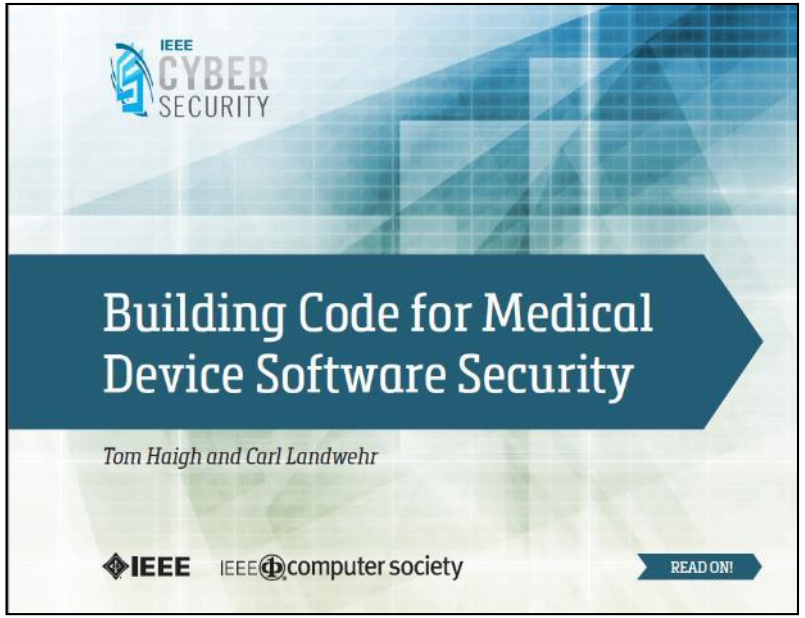
Manufacturers should:

- Develop a set of cybersecurity controls
- Address cybersecurity during the design and development of the medical device.
- Establish design inputs related to cybersecurity
- Provide justification for the security chosen functions

IEEE Cyber Security:

Building Code for Medical Device Software Security

- Issued May 2015
- A set of guidelines are meant to help companies "establish a secure baseline for software development and production practices of medical devices."
- The code applies to software which runs in a wide range of medical devices
- Similar to a 'building code' for houses and structures, this provides guidance on building safe and secure software for medical devices



QOS	Topic
✓	MEMORY-SAFE programming languages
✓	Deploy SECURE coding STANDARDS
✓	"SECURELY" generating random numbers
✓	WHITELISTING applications
✓	LOGGING security-RELATED events
✓	DISABLE execution of DATA
✓	Deploy LEAST PRIVILEGE Principles

Understanding Security Needs

Who are we protecting ourselves against?

- "Script Kiddy"?

  Someone competent enough to affect attacks discovered by others leveraging unpatched vulnerabilities.

- Independent black-hat hacker?

  Skilled engineer working alone or in ad-hoc groups for personal gain or simply peer credit.

- Organized crime/hacktivists?

  Often the origin of ransom-ware or other attacks often motivated by financial gain or the desire to make a political statement.

- Corporate espionage?

  May or may not be better funded or more skilled than organized crime, but most often interested in theft of information.

- Nation State?

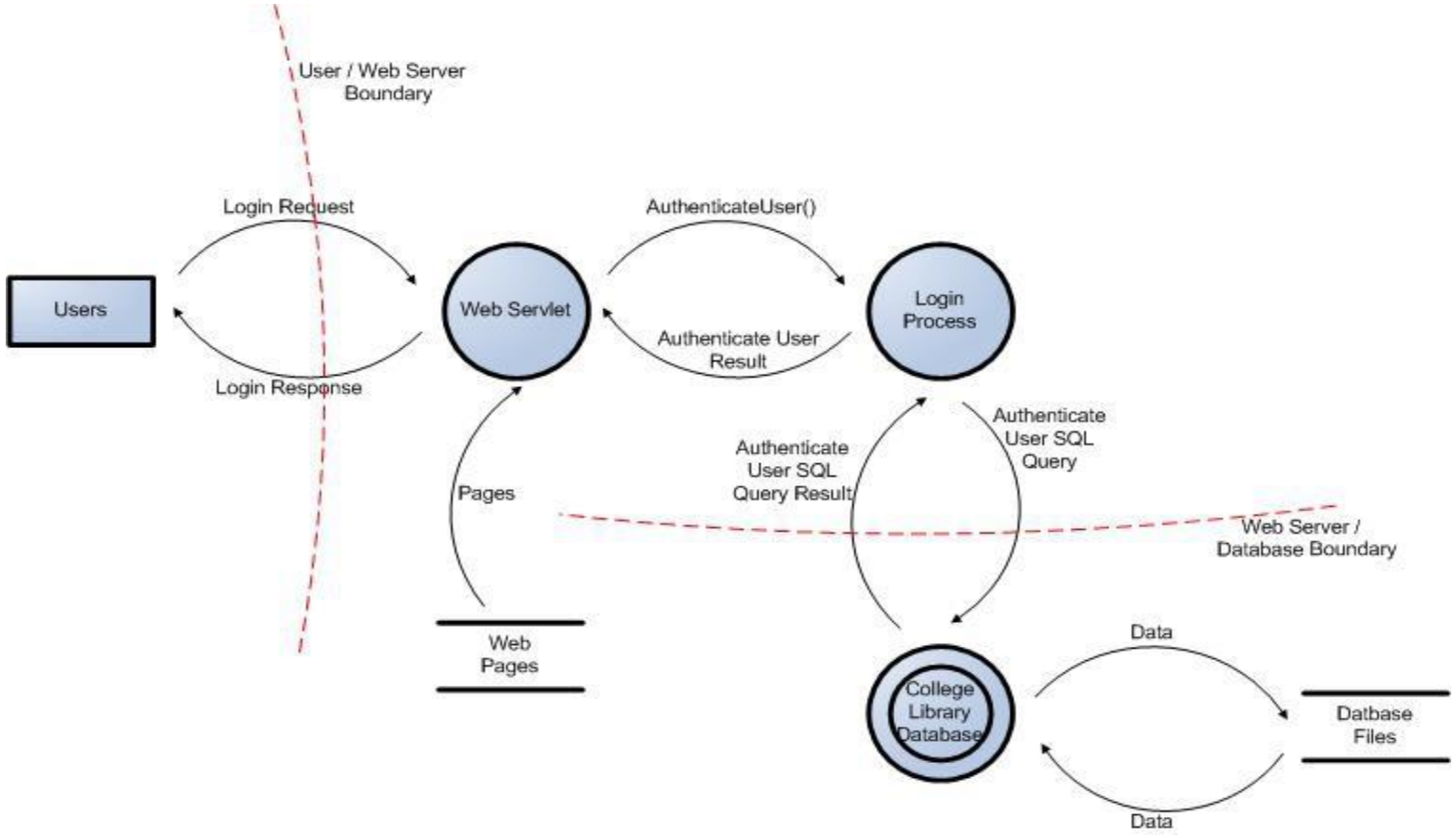
  Good for you for doing something important enough to warrant this level of attention. I'm sorry, though. I can't help you.

Security is a cost-benefit game. The goal isn't "hack proof"… should you spend $1B ??

The goal is "beyond the means of the threat source" or not "worth the investment".

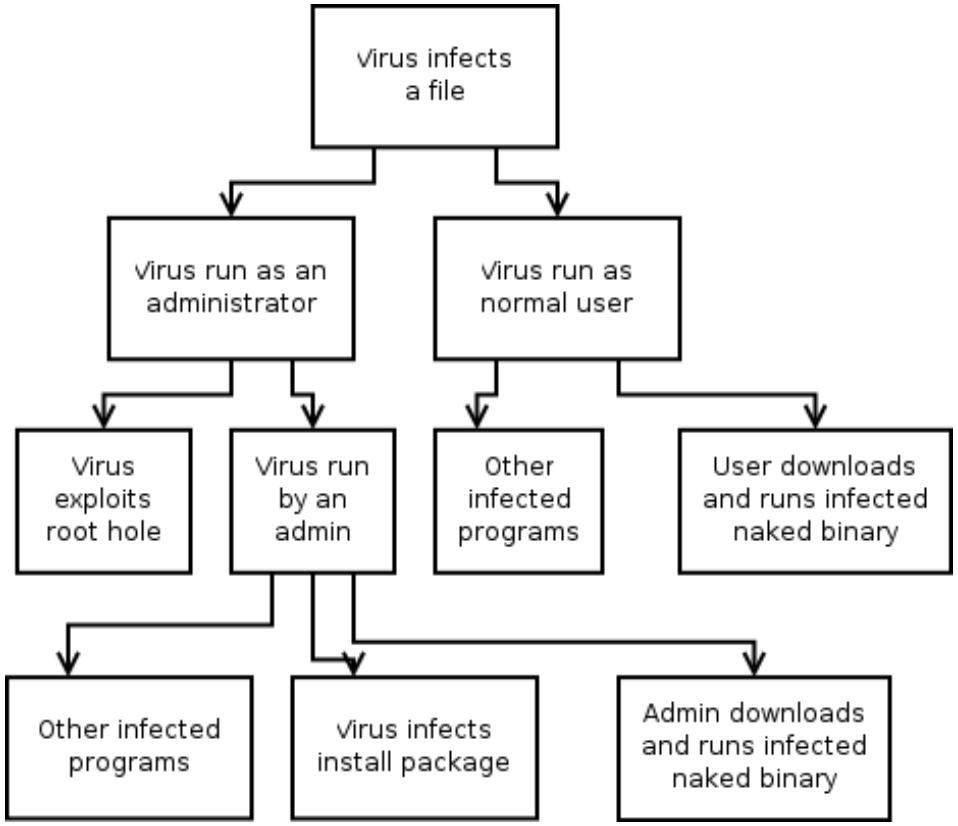
Security Analysis – Threat Modelling

Construct a data-flow diagram (DFD), including 'threat boundaries' and protections put in place at to protect data as it crosses.



Security Analysis – Attack Tree

Following the flow of an attack through the system to ensure all avenues are closed.



Security Analysis – More Models

STRIDE

- **S**poofing
  Falsifying identity, or origin or destination of data.
- **T**ampering
  Altering data.
- **R**epudiation
  Disputing the legitimacy of some interaction.
- **I**nformation Disclosure
  Unauthorized release of data.
- **D**enial-of-service
  Forced loss of availability.
- **E**levation of Privilege
  Bypass of authorization system.

DREAD

- **D**amage
  How bad could an attack be?
- **R**eproducibility
  How easy is it to reproduce the attack?
- **E**xploitability
  How much work is it to launch the attack?
- **A**ffected Users
  What is the scope of the impact?
- **D**iscoverability
  How likely is the threat to be discovered?

Think like a “hacker”…

- Exhaustive approach to threat analysis is not the most effective means
- Identify the most valuable assets
- Identify the least secure links
- An attack will most likely target one or more of these four goals:

Arbitrary Code Execution

Data Modification

Theft of Data

Denial of Service

How to start…

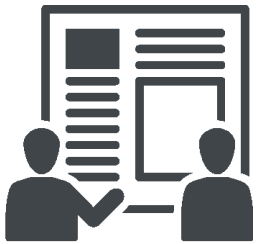
BlackBerry 7-Pillar Cybersecurity

01	02	03	04	05	06	07
SECURE THE SUPPLY CHAIN	USE TRUSTED COMPONENTS	ISOLATION	IN FIELD MONITORING	RAPID INCIDENT RESPONSE	LIFE CYCLE MANAGEMENT	SAFETY / SECURITY CULTURE

Available | In progress

01	02	03	04	05	06	07
Certicom AMS	FIPS 140-2 Toolkits	Hypervisor & Gateways	Remote Analytics / Diagnostics	Crisis Connect	Secure OTA SW updates	Safety Training
Binary Code Scanning	QNX OS	Secure Messaging	Integrity Checks	Emergency Alerts	Selective Manifest Install	Security Training
Pen & Vulnerability Testing	Application Management	Guarding Buses	Credential Management	Advisories	UEM	

Security Principles and Best Practices from Standards



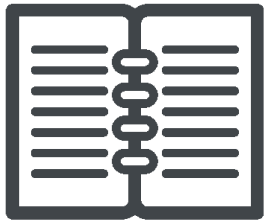
ISO 27000

NIST

SAE J3061

IISF

FIPS



Availability

Ensuring the system is available for use only by those allowed

Integrity

Ensuring data/information has not been tampered with

Authentication

Ensuring users are who they say they are

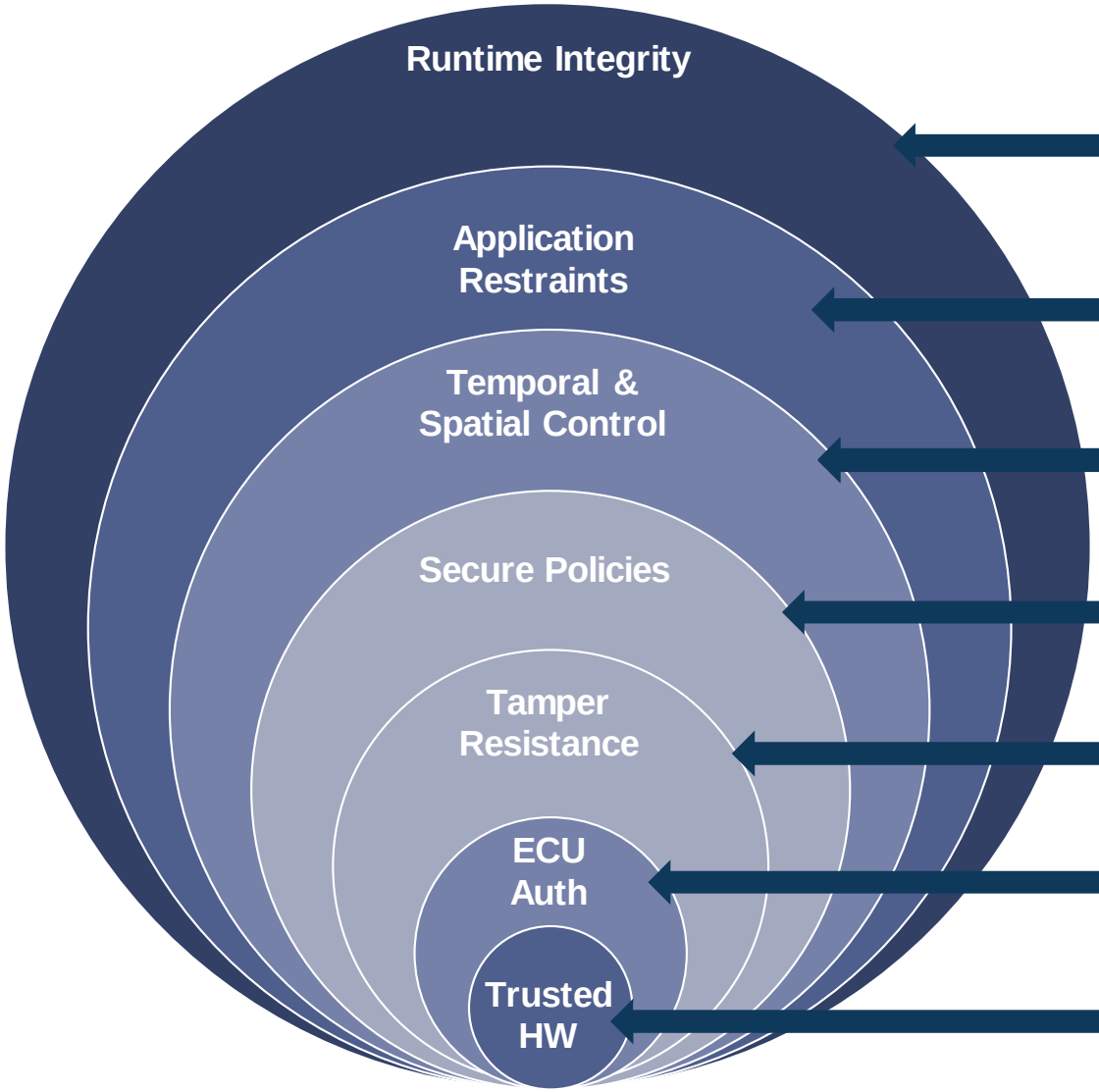
Confidentiality

Data is protected and only those authorized are allowed to access it

Least privilege

Only give privileges needed to perform a given task(s) and nothing more

OS Runtime Security - Defense in Depth



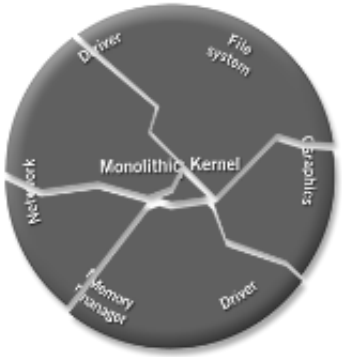
- Monitor system behavior, Intrusion detection logging & reporting
- Whitelisting, Pathspace control, Resource Access
- Control & Restrict CPU usage,
  Protect against defects and rogue execution
- Mandatory Access Control (MAC), Abilities, ACLs
- Secure boot, Image Verification, Integrity Measurement model
- Unique Certificate through Certicom Secure Manufacturing
- Immutable Hardware Root of Trust

Availability

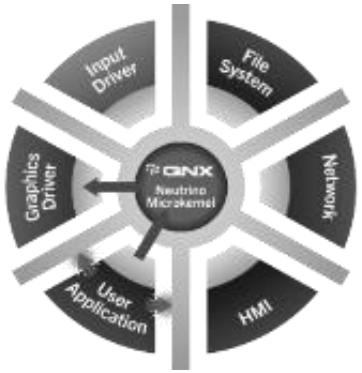
Microkernel Architecture

QNX's microkernel architecture separates critical OS components into their own protected memory partitions, unlike a monolithic OS that places them all together. Reduces attack surface.

Monolithic (Linux)



Microkernel (QNX)



OS Architecture Foundation

Temporal Separation

QNX's Adaptive Partitioning System (APS) supports CPU time partitions to limit CPU usage from misbehaved or rogue applications and/or services. The *adaptive* capability ensures maximum system efficiency.

Time Protection

Process Protection

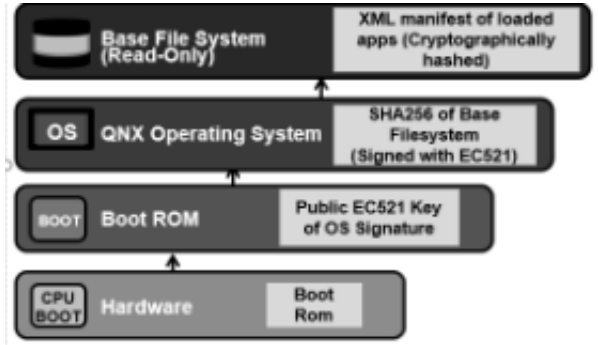
The QNX OS provides process-level features that help protect from attacks: Address Space Layout Randomization (ASLR), heap cookies, stack guard pages, non-executable stack.

Fine-grained Process Protection

Integrity

Secure Boot

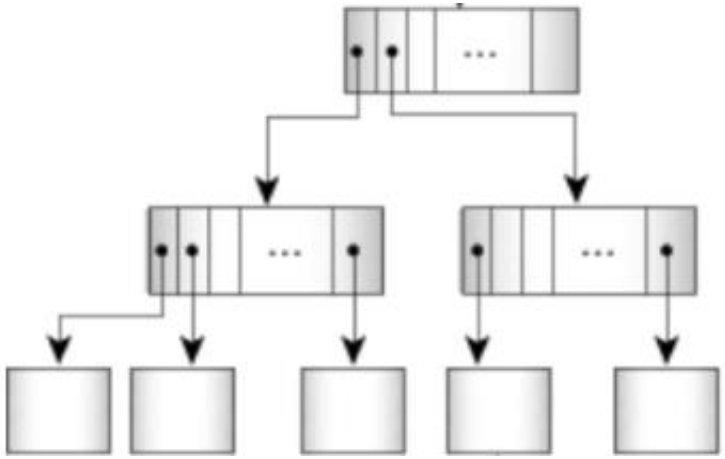
Maintain complete chain of trust through signed code execution and image verification with support for Trustzone and TPM. Modification detection through rules based measurement at runtime. Complete policy enforcement and logging of any violations.



Chain of Trust

Self-Verifying File System

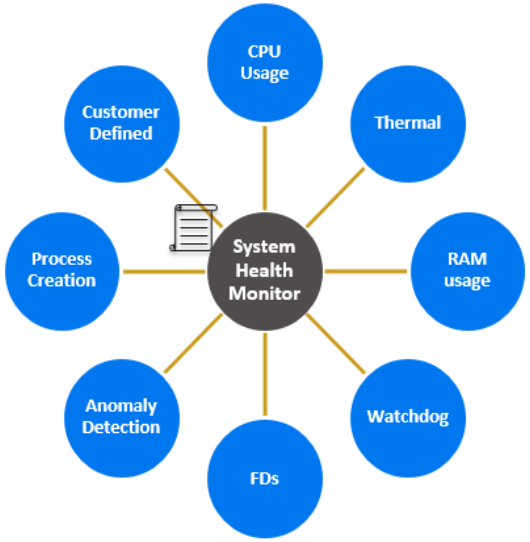
The integrity of the local file system is verified on each access and done at a block level.



Block-Level Verification

Integrity Measurement

Tamper-proof mechanism to record boot process integrity. Logs can be analyzed at runtime or offline.



System Monitoring

Authentication

Pluggable Authentication

PAM is an industry standard way of providing authentication related services within the QNX framework.

Pluggable Authentication

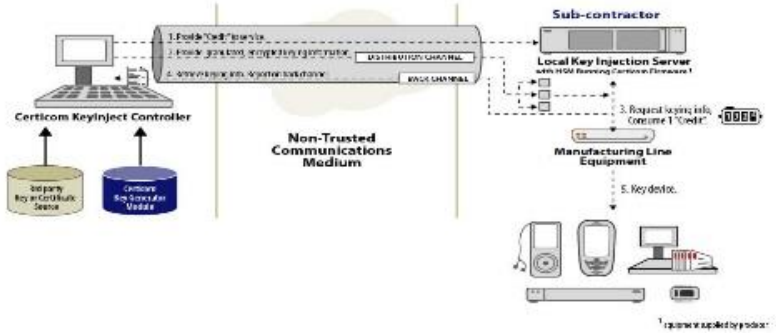
M-PKI

Managed PKI service, digital certificate management service, creating & managing “certified device identities”.

Key Infrastructure

AMS

Managed PKI service, digital certificate management service, creating & managing “certified device identities”.

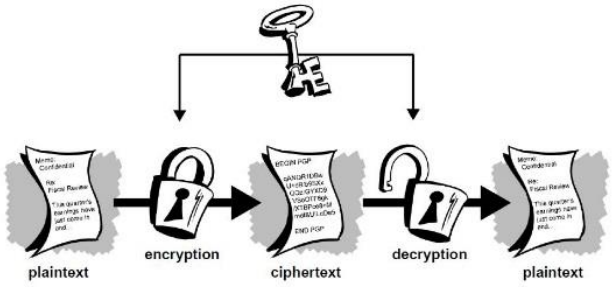


Provisioning

Confidentiality

Crypto Support

Security Builder software for Public and symmetric crypto with integration of hardware



Payload Protection

Secure File System

The file system supports multiple encryption partitions to secure data.

Storage Protection

Network Security

The QNX network stack supports industry standard security protocols including TLS, SSL, IPSEC including hardware crypto offload.

Connectivity Protection

Least Privilege

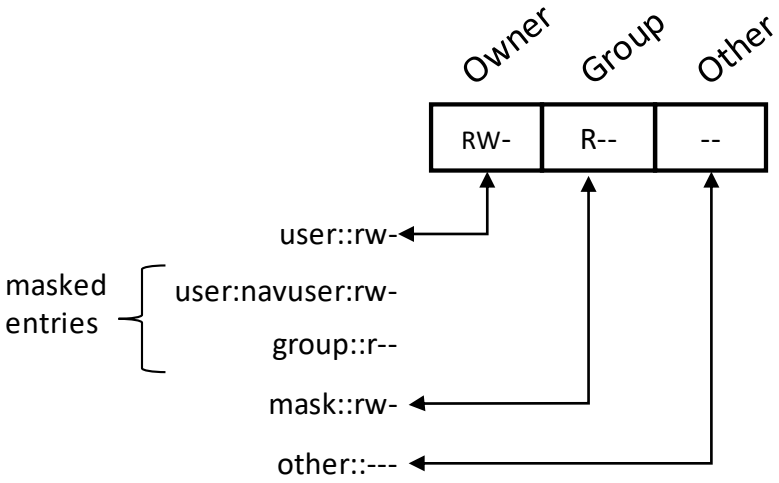
Rootless Operation

Root access is divided into >50 root level capabilities via QNX Abilities. Processes can be limited to the QNX Abilities they need. Allows for root-less operation.

Root Access Protection

File, Pathspace and Control List

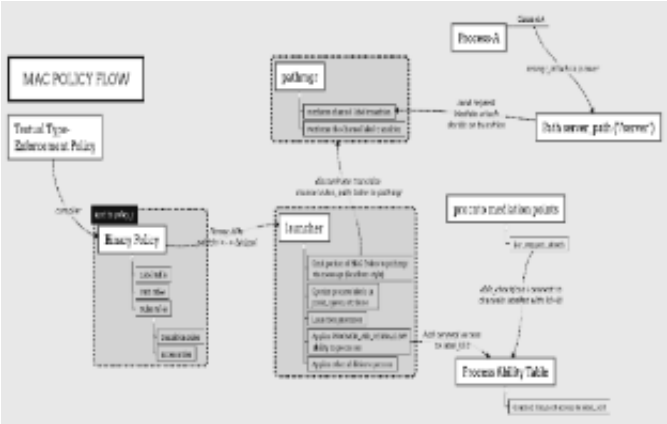
POSIX file mode permission enforcement. Limited access of a process to a defined path space. Fine-grained control over file and device access.



File Permissions and Protection

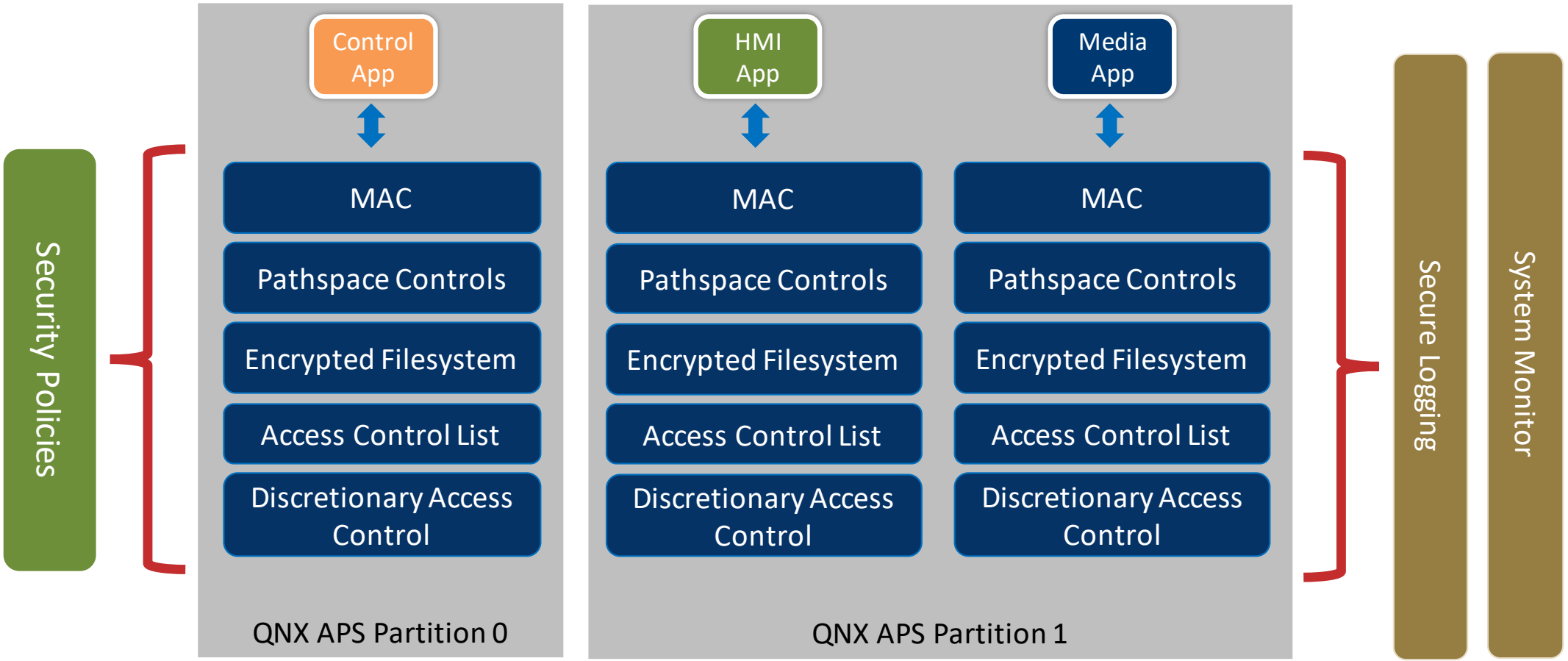
Mandatory Access Control

Controls which paths can be accessed or created. The QNX runtime Launcher loads and configures all processes at launch time.



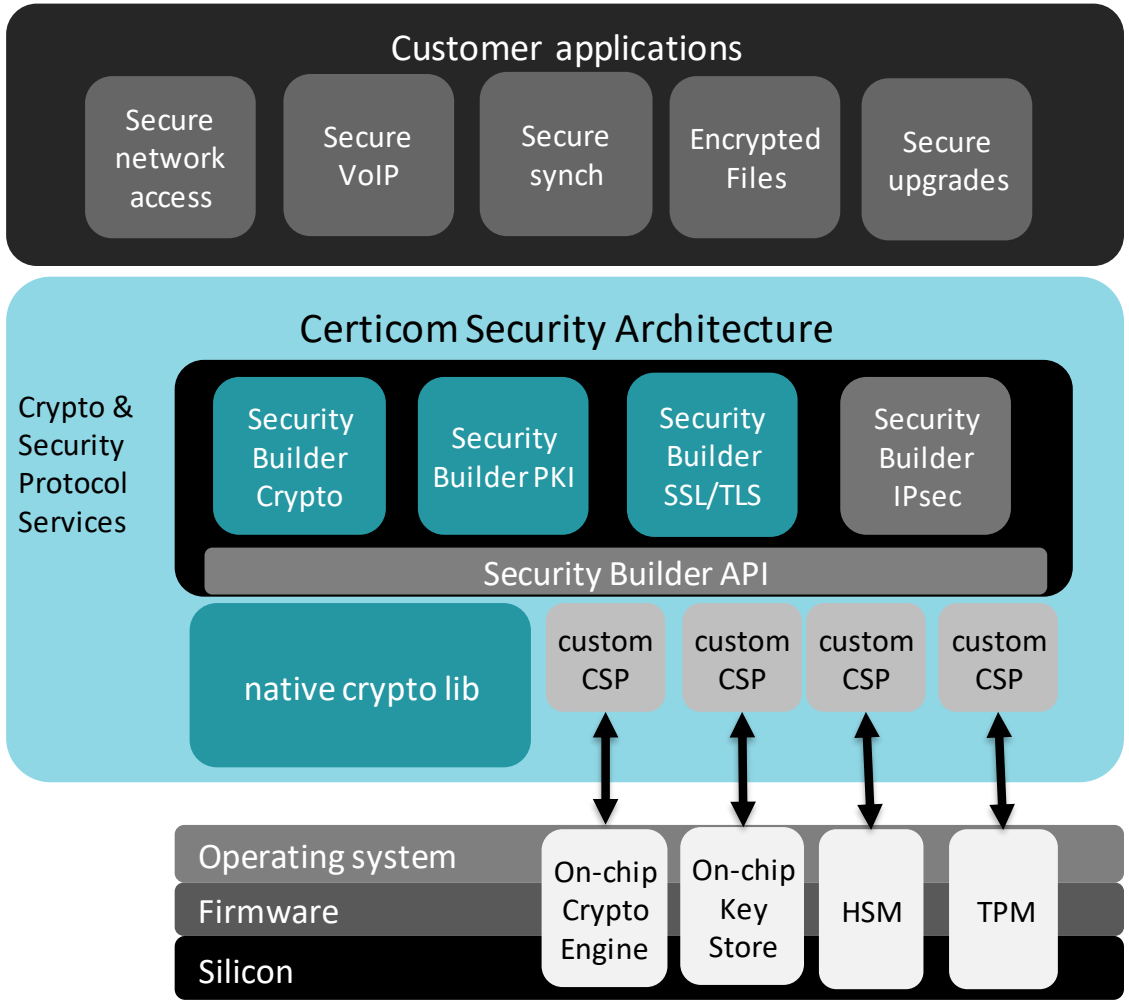
Process Permissions

QNX Runtime Security Multi-layered, Policy-driven



Certicom Security Builder

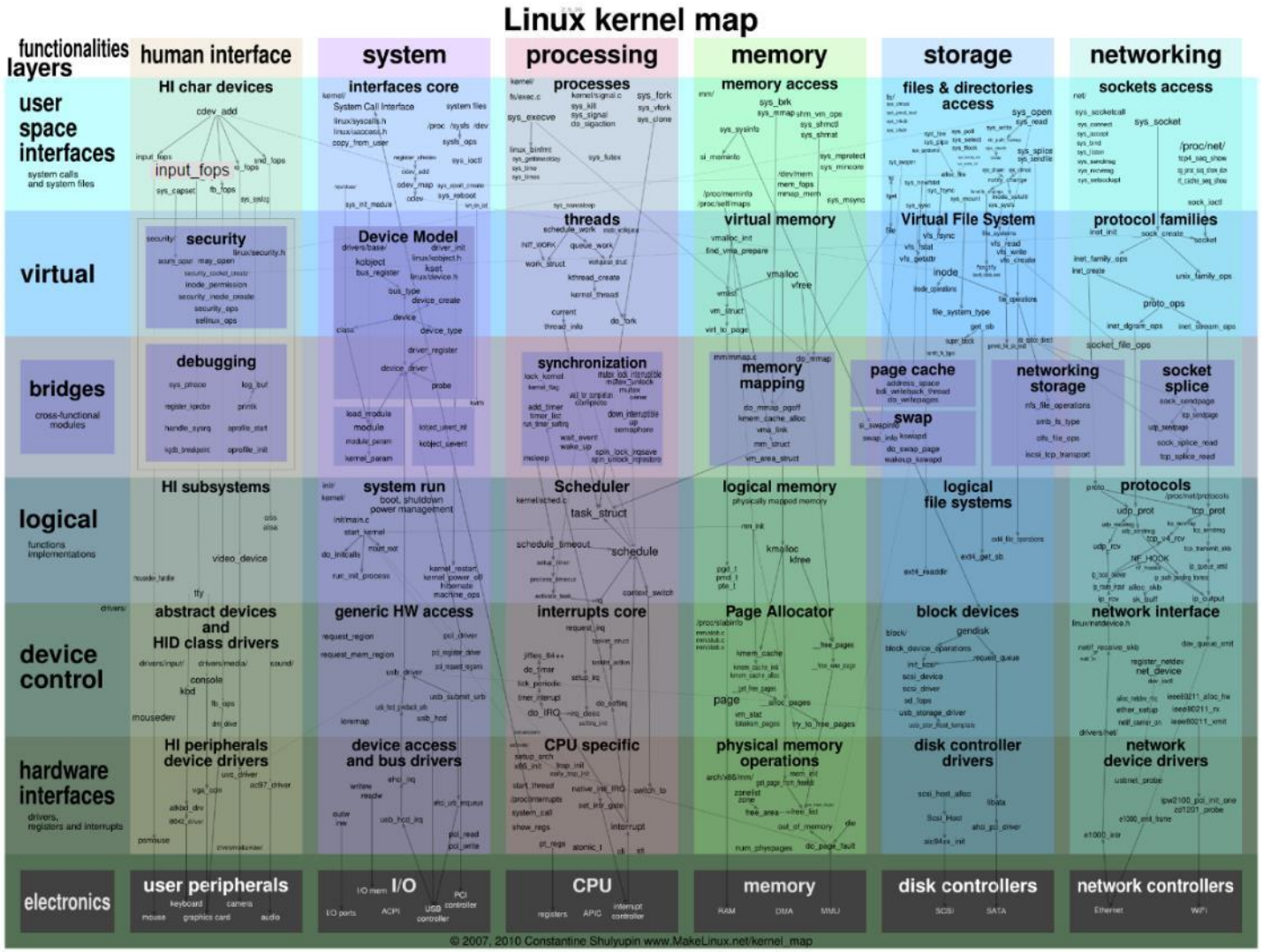
- **Cryptographic libraries**
  - Wide range of public key, symmetric ciphers and hash algorithms
  - Architecture supports custom hardware/crypto service provider (CSP) integration options
- **PKI libraries**
  - Comprehensive certificate management protocols and encoding support
- **Available in ANSI-C and Java**
- **FIPS validated "GSE-C" option**



Safety Compounds Your Choices…

- **IEC 62304 has code management criteria**
  - "known your code"
  - Code that is not required/related to your product's function must be removed
  - Controlled/known software development process
- **Security is not so different…**
- **Choices can precipitate an unexpected (unconfessed) commitment to become an OS supplier**

Linux Kernel Map



Source: www.makelinux.net/kernel_map

Linux by the Numbers…

- **8,000-12,000 – The number of patches going into each recent kernel release.**
- **8-12 – The desired release period (in weeks) for a major kernel release.**

Patches per hour:

- **3,616 –** The number of patches for kernel version 2.6.11, the fewest of any release.
- **12,243 –** The number of patches for kernel version 2.6.25, the largest of any release.

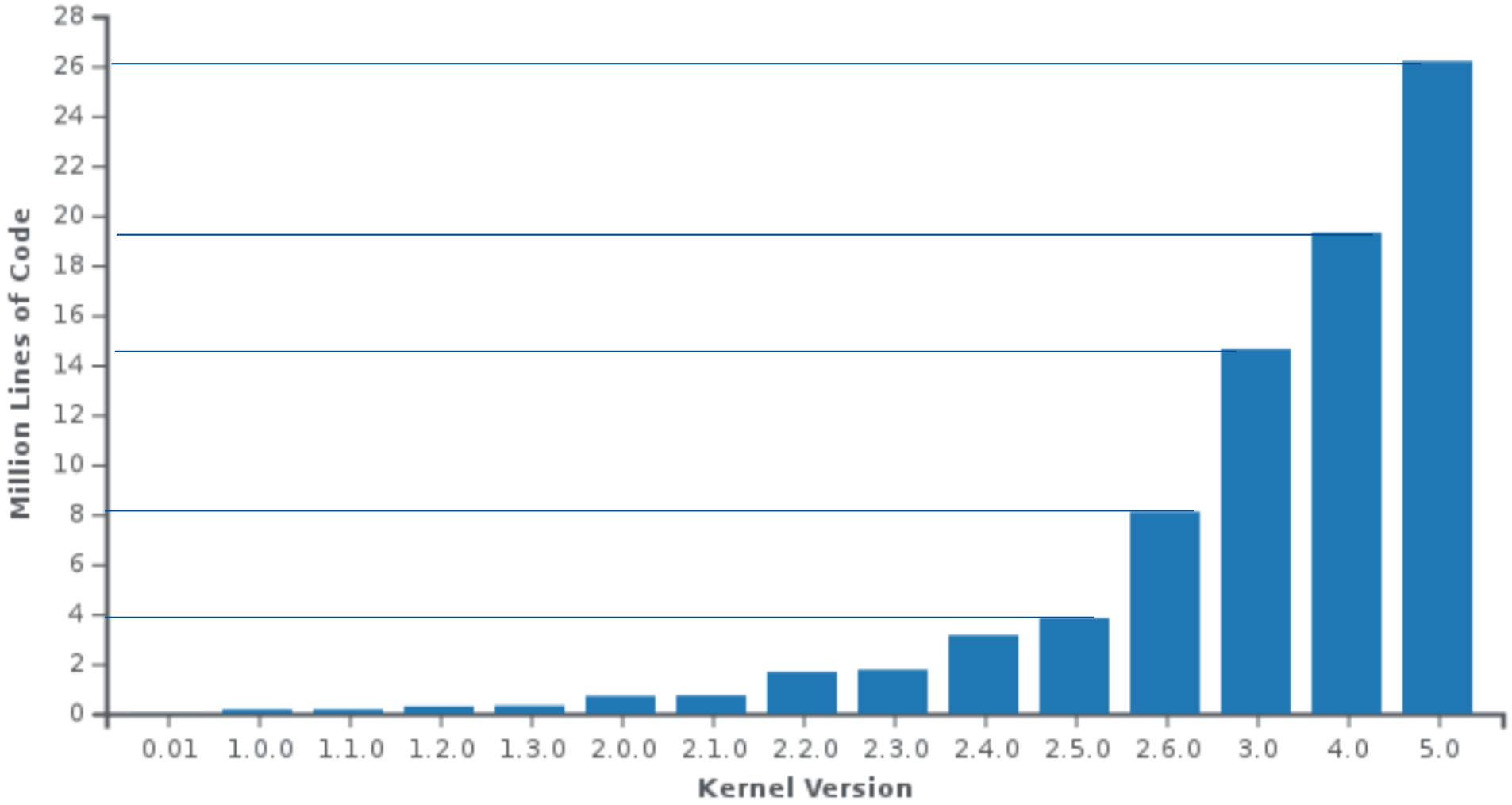
Changes per hour:

- **1.95 –** The number of changes per hour for kernel version 2.6.12, the lowest of any release.
- **6.88 –** The number of patches per hour for kernel version 3.2, the highest of any release.
- **3,315 – The number of fixes in 2.6.32, the highest of any release.**
- **Files, LOC:**
  - **17,090 –** The number of files in the 2.6.11 kernel version
  - **37,626 –** The number of files in the 3.2 kernel version
  - **15,004,006 –** The number of lines of code in the 3.2 kernel version

- **4.3 – Estimated that Linux kernel 4.3 would be the first version using more than 20 million lines of code.**

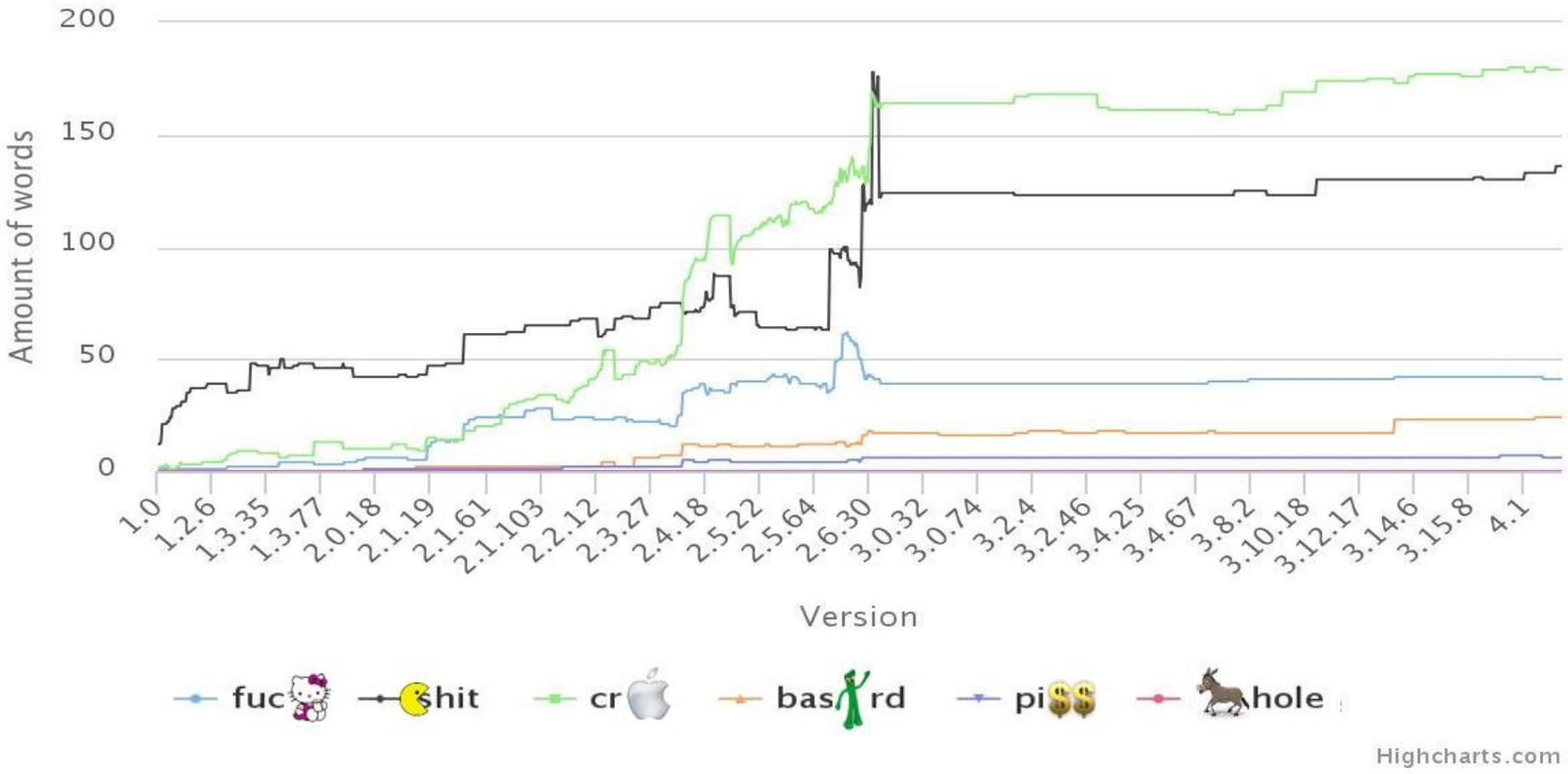
Circa 2015

Lines of code per Kernel Version



https://www.linuxcounter.net/statistics/kernel

Bad Words Within the Code of the Linux Kernel



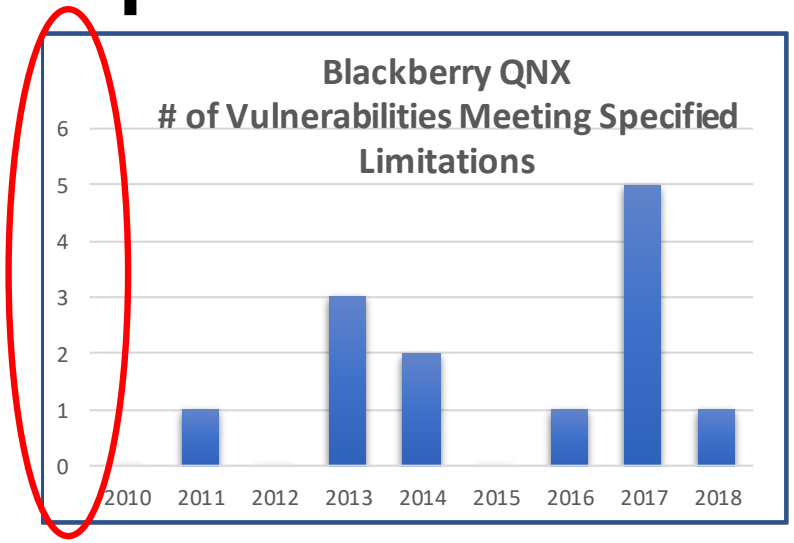
Software Vulnerabilities & Fallacy Of Open Source

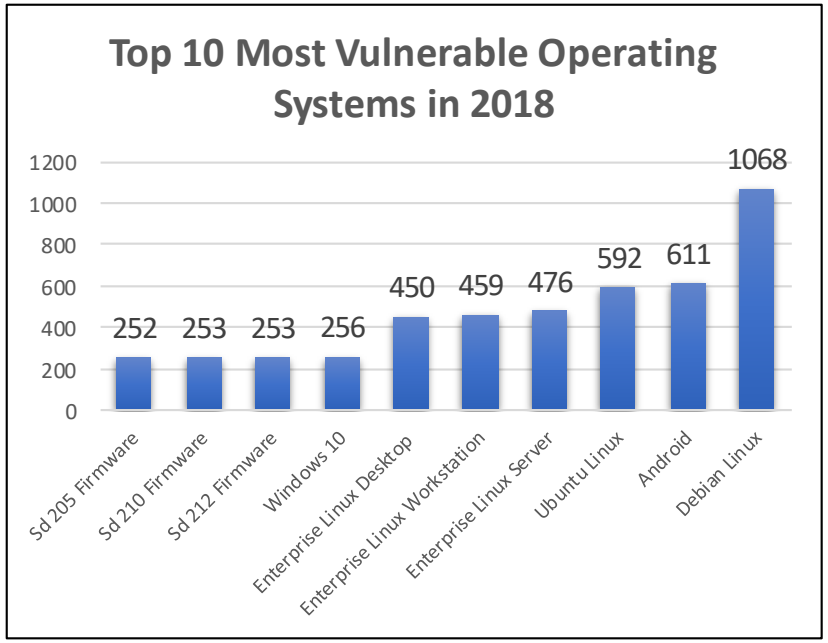
Carnegie Mellon University, Software Engineering Institute (SEI)

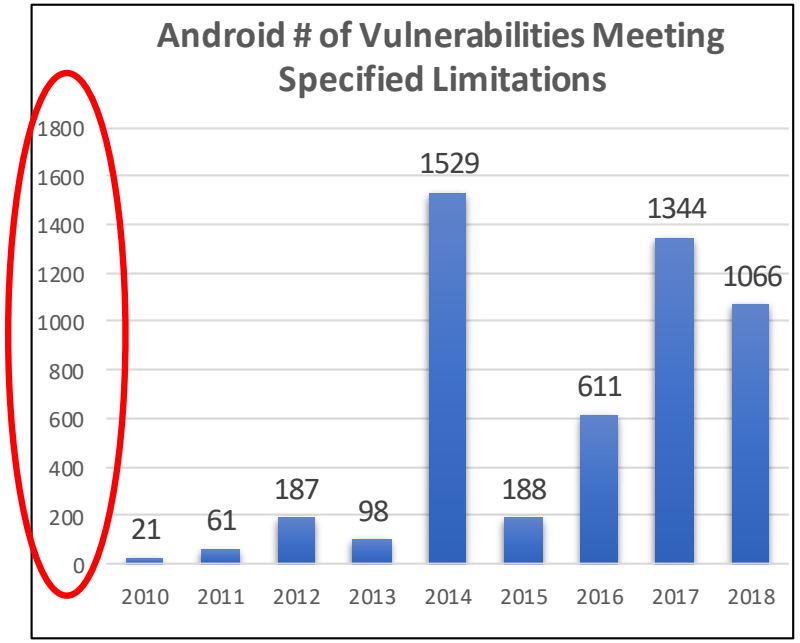
- **"Average"** code developed in the US has 0.75 defects per function point, or, **6,000 defects per Million Lines Of Code (MLOC).**
- "**Very good**" levels would be **600 to 1,000 defects per MLOC**
- "**Exceptional**" levels would be < **600 defects per MLOC**.
- **1% - 5%** of defects should be considered vulnerabilities.

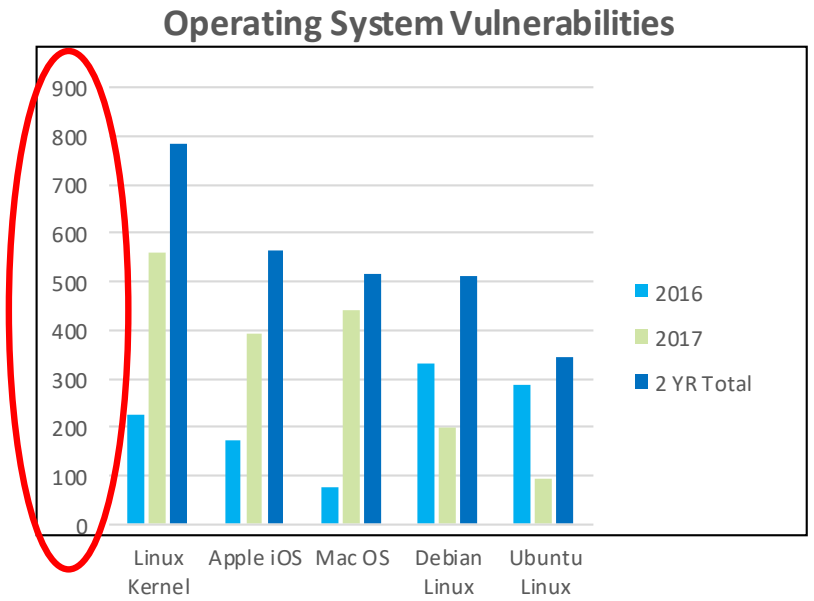
Assuming ALL code is "Very good"

- Modern Car has 100 MLOC, 100K Defects, & **1,000-5,000** vulnerabilities









* There are now confirmed cases of "backdoor" vulnerabilities in the opensource software.

Source: CVE details, https://nvd.nist.gov/ 2017

Blackberry and Established Partners

Enterprise Software

- End Point Management

BlackBerry IoT

- OTA and Edge Analytics

BlackBerry | QNX

- Mission-critical operating system

BlackBerry | certicom

- Crypto and PKI experts

BlackBerry

- Code Scanning and Hardening

Portfolio

Partners

Acquisition

rti Your systems. Working as one.

- Data-centric messaging bus

WITTENSTEIN

- SAFERTOS for microcontroller platforms

CYLANCE

- Intrusion Detection and Prevention
- Cloud-Based Machine Learning

BlackBerry and partners to develop a real time protection solution.

IEC 62304 Class C Compliant

- Pre-assessed to be compliant with the requirements of the EN 62304 and can be used in applications up to class C.
- Assessment performed by reputable auditing firm: TÜV Rheinland
- Scope of assessment includes the core of the operating system
- Supported on 32 and 64-bit ARM and x86 platforms
- 100% API compatible with QNX standard RTOS
- Share the same pedigree as QNX OS for safety (development artefacts and process flow)

Product Purpose

- **QNX OS for Medical is designed to be used in systems that:**
  - Must be compliant with IEC 62304
  - Have real-time performance goals
  - Require the usage of a full-featured RTOS
- **Using QNX OS for Medical helps you:**
  - Build functional safety on a reliable foundation
  - Reduce certification risk and control certification scope
  - Leverage QNX's domain knowledge and expertise

Assessment Scope

- **Target software**
  - QNX Neutrino microkernel and process manager, including multicore support and adaptive partitioning scheduler
  - Libc
  - Image filesystem and security policy utility
- **Compatibility**
  - Compatible with QNX SDP 7.0
  - Supported on 32 and 64-bit ARM and x86 hardware platforms

Product Package

- **QNX OS for Medical must be installed on top of an existing SDP 7.0 dev seat (dev seat is not included as part of the QNX OS for Medical product)**
- **Product package includes:**
  - Binaries and header files for microkernel, process manager and libc
  - Safety manual
  - Installation and usage guide
  - Hazard and risk analysis
  - Safety case