The Realities of Maintaining a Secure Software Supply Chain

Adam Boulton
CISSP, CSSLP, CCSP, OCJA, CSTM, ISO 27001 LA
SVP, Security Technology

Christine Gadsby
Director, BlackBerry Security Response and Cybersecurity Services

Security Engineering and patching, patching, patching

QNX | BlackBerry Subsidiary

Good | Powered By BlackBerry

movirtu | By BlackBerry

secusmart | BlackBerry Subsidiary

WatchDox | By BlackBerry

AtHoc | Division of BlackBerry

certicom | BlackBerry Subsidiary

BlackBerry
Secure Smartphone
Powered by Android™

WELL ESTABLISHED GLOBAL RELATIONSHIPS – GENERAL EMBEDDED

General Embedded

AECL | CAT | fortna | BAE SYSTEMS | HARRIS | TOSHIBA Leading Innovation >>> | GE | infinera | JDSU | Nokia Siemens Networks

ALSTOM | EMERSON. Process Management | INTUITIVE SURGICAL | THALES | IGT | NASA | DragonWave | ADTRAN | CISCO

Abbott A Promise for Life | Johnson & Johnson MEDICAL | UNITED STATES POSTAL SERVICE | LOCKHEED MARTIN | SIEMENS medical | ROBODOC Curexo Technology Corporation | Bally TECHNOLOGIES | OLYMPUS

OMRON | Rockwell Collins | ABB | Alcon | AREVA | BOSCH | MURPHY reliable innovation | Auto Meter COMPETITION INSTRUMENTS | GENERAL DYNAMICS

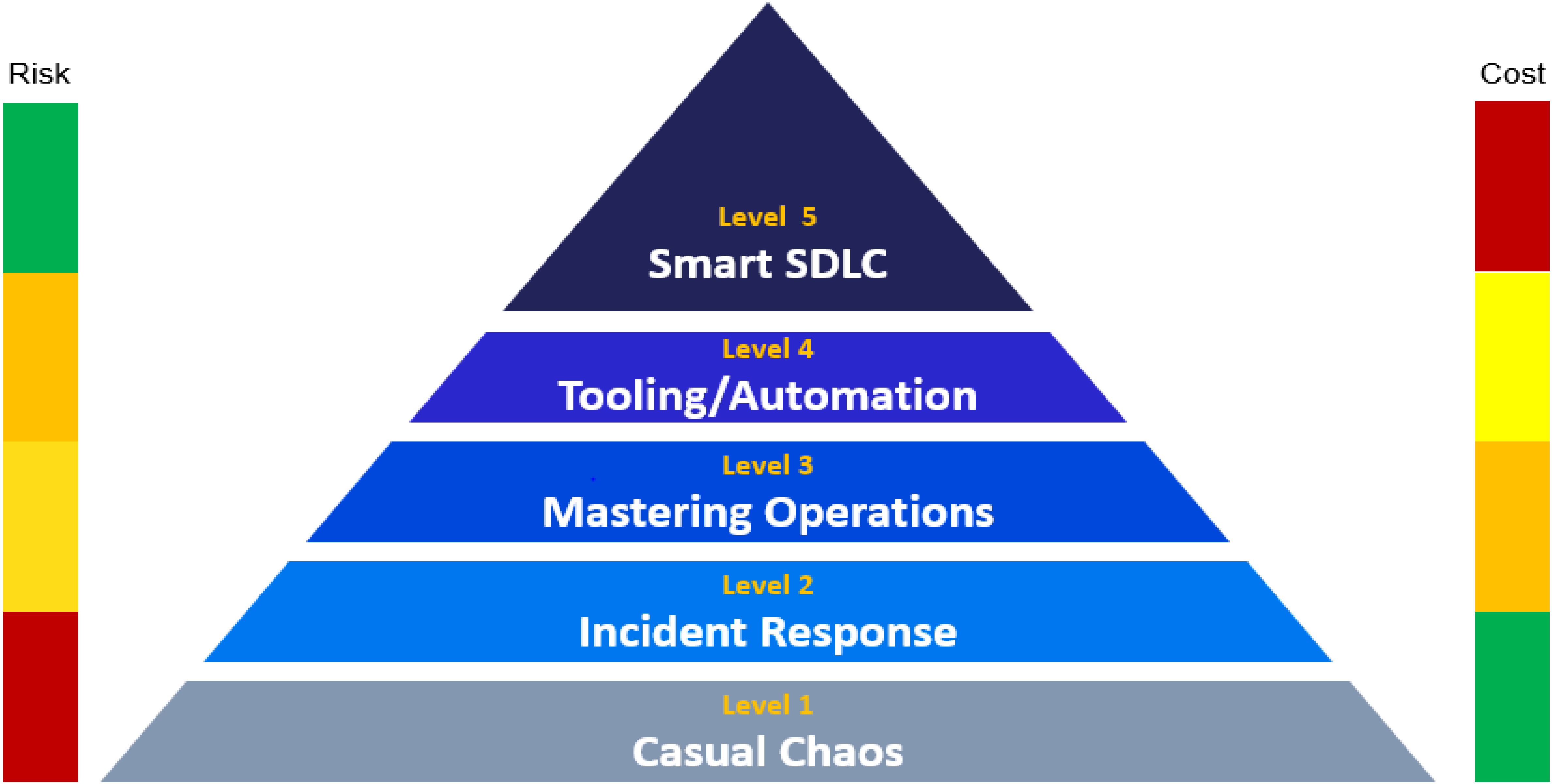
Honeywell | Schneider Electric | ZEBRA TECHNOLOGIES | SCHEIDT&BACHMANN SB | FUJITSU | H [illegible] | Canon | STOKE | intune networks

QNX software deployed and trusted by 1000s of companies large and small to ensure the very best combination of performance and reliability in the worlds most mission critical systems

Fun BlackBerry OSS facts

- 563 unique libs tracked across 86 product variants
- One single product could have 195 unique OSS libs
- A product could contain 47 copies of the same library
- Up to 16 different versions of a unique library in a single product

BlackBerry's OSS Maturity Model



Practical advice for OSS OPS

- Know and understand what is in your products
  - Build a cataloged BOM

    Across all products, integrated

    Track OSS vulns DAILY

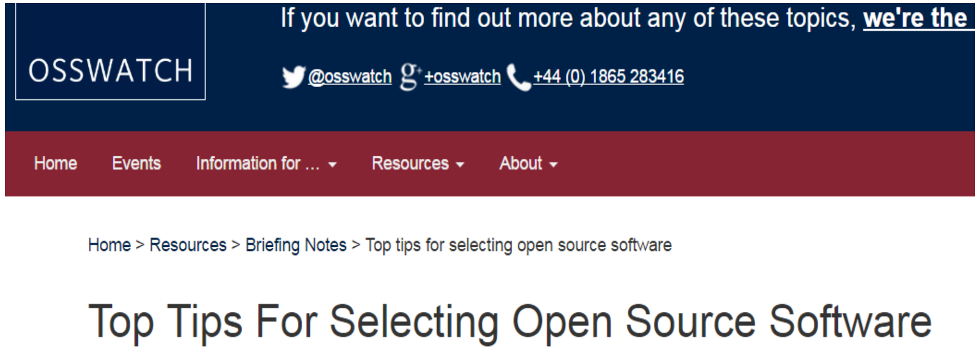
- Evaluate the OSS you are using, limit the additions, maintain what you have

  Blacklist unhealthy OSS projects

  You need a SIRT function and an SRR

  Don’t let dev police themselves

  it will always come to features vs. fixes



If you want to find out more about any of these topics, we're the

@osswatch +osswatch +44 (0) 1865 283416

Home > Resources > Briefing Notes > Top tips for selecting open source software

Top Tips For Selecting Open Source Software

How to evaluate the sustainability of an open source project

- https://opensource.com/life/14/1/evaluate-sustainability-open-source-project
- http://oss-watch.ac.uk/resources/tips

Practical advice for OSS Security Engineering

- Secure Design Principles
  - Understand the scope of the OSS that is required and how best maintain security
    - Is the entire library really required?
    - Design using: Least Privilege, sandboxing, know what your alternative OSS libs are
    - Reduce risk with compiler defenses by reducing chances of exploitability
    - Plan for OSS maintenance: MR, version updates, patch accordingly

- Hold your supply chain accountable
  - Supplier contracts that limit OSS use
  - Liability deference for those that don't comply
  - Periodic checks for compliance

Bottom Line : Be prepared. Understand TCO of the libraries you use. Free software is great, but it still requires investment.

Cost to manage free OSS during 2015

cURL

$200,345

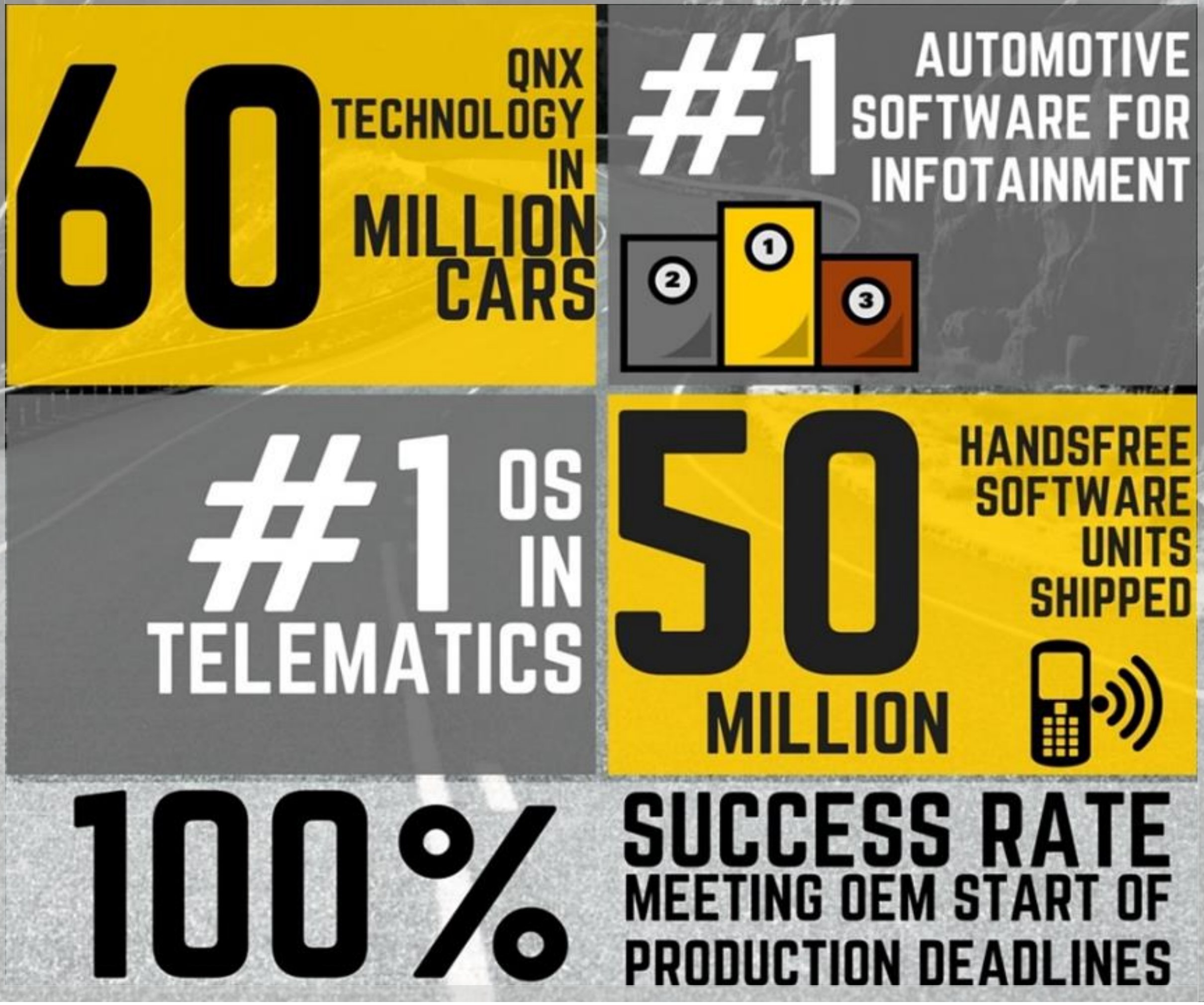
libpng

$203,678

OpenSSL

$370,690

QNX: AUTOMOTIVE MARKET LEADER



60 MILLION CARS
QNX TECHNOLOGY IN

#1 AUTOMOTIVE SOFTWARE FOR INFOTAINMENT

#1 OS IN TELEMATICS

50 MILLION HANDSFREE SOFTWARE UNITS SHIPPED

100% SUCCESS RATE MEETING OEM START OF PRODUCTION DEADLINES

“QNX, a tech company that is to connected cars what Microsoft is to PCs.”
TIME Magazine - 2016

WELL ESTABLISHED GLOBAL RELATIONSHIPS - AUTOMOTIVE

Automakers

GM · OnStar · BUICK · HOLDEN · TOYOTA · LEXUS · Audi · PORSCHE · SKODA AUTO · BUGATTI · LAMBORGHINI · B

CHRYSLER · FIAT · Jeep · JAGUAR · LAND ROVER · BMW · MINI · HONDA · ACURA · NISSAN · SUBARU · HYUNDAI

Ford · DAEWOO · SAAB · FISKER · mazda · FLEETWOOD · SSANGYONG · CHERY · KIA · Peterbilt · MOTOR HARLEY-DAVIDSON CYCLES

Tier 1

HARMAN · Johnson Controls · DELPHI · Visteon · Lectronix · BOSCH · Continental · TechniSat · Valeo · MAGNETI MARELLI · MTA Advanced Automotive Solutions

JVC · LG Electronics · DAEWOO DAEWOO PRECISION INDUSTRIES CO., LTD. · ALPINE · SUMITOMO · DENSO · AISIN · Panasonic · SAMSUNG · HYUNDAI AUTONET

QNX software deployed by over 40 OEMs in hundreds of vehicle platforms and over 60 million vehicles throughout North America, Europe, and Asia.

Consumer confidence in automotive security

57%

DOUBT THAT AUTOMOTIVE software development teams have the skills to combat software security threats

90%

THINK IT IS DIFFICULT to secure automotive applications

55%

LACK THE TRAINING of necessary security–enabling technologies

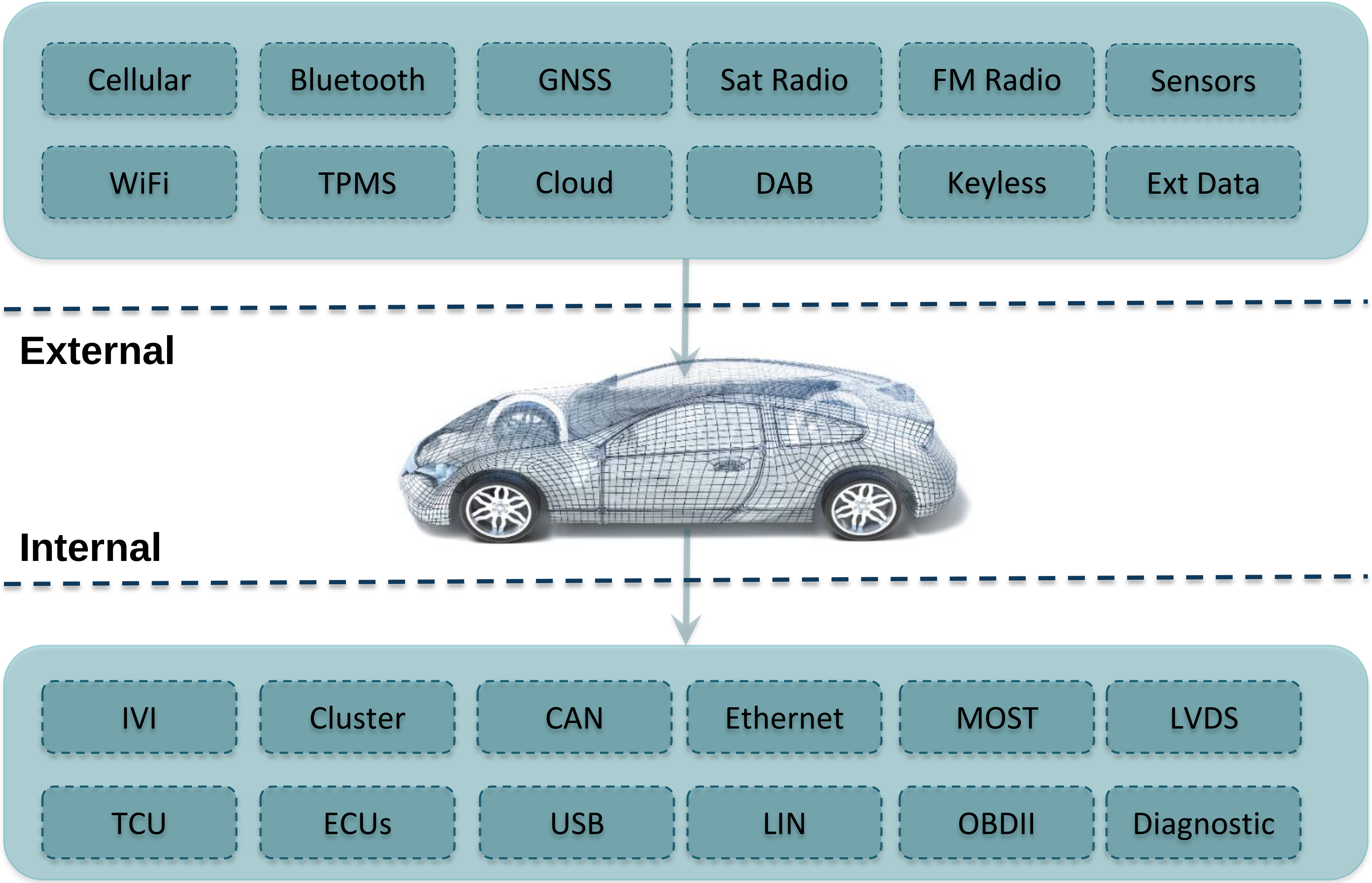
51%

CONSIDER SECURITY AN ADD-ON FEATURE rather than integrating it into the software development cycle

Response: Automakers seeking security expertise, solutions, & partnerships

Source: Poneman institute 2015

Automotive Attack Vectors



Cellular
Bluetooth
GNSS
Sat Radio
FM Radio
Sensors
WiFi
TPMS
Cloud
DAB
Keyless
Ext Data

External

Internal

IVI
Cluster
CAN
Ethernet
MOST
LVDS
TCU
ECUs
USB
LIN
OBDII
Diagnostic

Entrenched challenges

- Pervasively computerised

- The automotive supply chain is a large, complex operation that requires sophisticated management techniques, substantial information technology expertise

- Very large attack surface
  - Complexity is the enemy in safety and security critical systems
  - V2X - data points on the V2X standards
  - Very complex supply chain - hundreds of companies making thousands of parts and components

- Standards and legislation are dispersed
  - It takes a lot of familiarity to know the best path forward

- Legacy technology
  - CAN, message based protocol from early 1980s
  - Was never designed with security in mind (which we should also be grateful for)

Entrenched challenges

- Security critical systems vs usability, safety critical vs performance

- Security and safety critical systems aren’t orthogonal concerns, they have alot in common, HOWEVER, there is conflict

- Security & Safety - It all starts with design, economy of mechanism, isolation, redundancy, reliability
  - **A layered approach that incorporates chain of trust, integrity management and mandatory access control**

- How do you rate vulnerabilities and risk?
  - **CVSS isn’t fitting for safety critical systems**

- Building safety and security critical systems in an art in engineering

QNX Runtime Security Features

Secure File Systems

The file system supports multiple encryption partitions to secure data. Complete integration of Certicom 256bit AES FIPS compliant encryption.

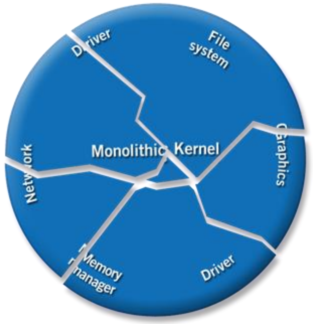
File Protection

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.

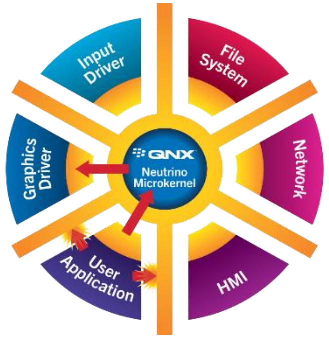
Monolithic

(LinuxX, LinuxY…)



Microkernel

(QNX)



Memory Protection

Temporal Seperation

QNX’s Adaptive Partitioning System (APS) supports CPU time partitions to limit CPU usage from potential misbehaved or rogue applications and/or services.

Time Protection

QNX Runtime Security Features (CONT'D)

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

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

Heap and Stack Protection

Network Security

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

Connectivity Protection

Process Approach

Break your security and safety program down

- Understand what you really need to achieve
- AND the expectations from your supply chain, check, check, check!

Standards

- Due diligence in your supply chain, including OSS
- System Readiness Review
    - What is your residual risk?

Education

- Security awareness & training across the organisation
    - Are procurement thinking about this?
- Relationships with the security community

Assessment

- Pro-active and re-active
- Within your code repos and continuous build environments
- Testing in depth - really at the heart of safety & security critical systems

Practical approaches

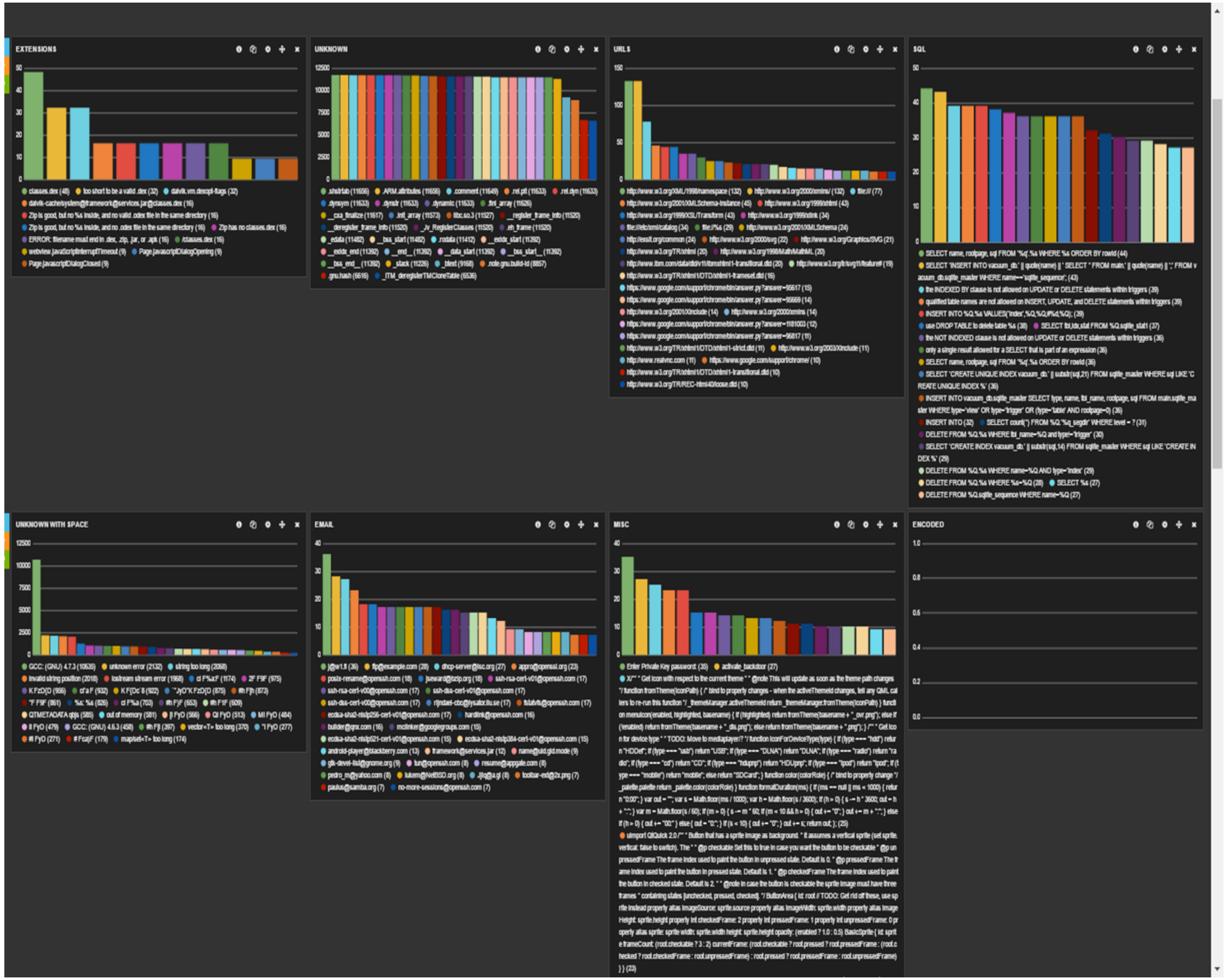
- In security engineering, it is very wise to look at the safety engineering
  - We're all talking about improving quality, reducing risk
  - Design out single points of failure
  - Justify real time scheduling with analysis
  - Watchdog timers that have real "bite"
  - You can never truly have a safe system without security

- DO-178B
- SAE J3061
- ISO 26262
- IEC 61508
- ISO 27K group
- MISRA C
- CERT C
- SPY CAR Act - Edward Markey

- JARVIS - Secure Agile Software Craftsmanship

BlackBerry Binary Security Analytics

- Measure secure agile software craftsmanship
- Understand platform security posture
- Assurance within complex supply chains
- Continuous assessment
- Platform hardening
- Determining deltas in your builds
  - More secure today than yesterday?
- Measure SROI - Security isn't a leap of faith


EXTENSIONS
50
40
30
20
10
0
classes.dex (48)
too short to be a valid .dex (32)
dalvik.vm.dexopt-flags (32)
dalvik-cache/system@framework@services.jar@classes.dex (16)
Zip is good, but no %s inside, and no valid .odex file in the same directory (16)
Zip is good, but no %s inside, and no .odex file in the same directory (16)
Zip has no classes.dex (16)
ERROR: filename must end in .dex, .zip, .jar, or .apk (16)
/classes.dex (16)
webview.javaScriptInterruptTimeout (9)
Page.javascriptDialogOpening (9)
Page.javascriptDialogClosed (9)
UNKNOWN
12500
10000
7500
5000
2500
0
.shstrtab (11656)
.ARM.attributes (11656)
.comment (11649)
.rel.plt (11633)
.rel.dyn (11633)
.dynsym (11633)
.dynstr (11633)
.dynamic (11633)
.fini_array (11626)
__cxa_finalize (11617)
.init_array (11573)
libc.so.3 (11527)
__register_frame_info (11520)
__deregister_frame_info (11520)
_Jv_RegisterClasses (11520)
.eh_frame (11520)
_edata (11482)
__bss_start (11482)
.rodata (11412)
__exidx_start (11392)
__exidx_end (11392)
__end__ (11392)
__data_start (11392)
__bss_start__ (11392)
__bss_end__ (11392)
_stack (11226)
_btext (9168)
.note.gnu.build-id (8857)
.gnu.hash (6616)
_ITM_deregisterTMCloneTable (6536)
URLS
150
100
50
0
http://www.w3.org/XML/1998/namespace (132)
http://www.w3.org/2000/xmlns/ (132)
file:/// (77)
http://www.w3.org/2001/XMLSchema-instance (45)
http://www.w3.org/1999/xhtml (43)
http://www.w3.org/1999/XSL/Transform (43)
http://www.w3.org/1999/xlink (34)
file:///etc/xml/catalog (34)
file://%s (29)
http://www.w3.org/2001/XMLSchema (24)
http://exslt.org/common (24)
http://www.w3.org/2000/svg (22)
http://www.w3.org/Graphics/SVG (21)
http://www.w3.org/TR/xhtml (20)
http://www.w3.org/1998/Math/MathML (20)
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd (20)
http://www.w3.org/tr/svg11/feature# (19)
http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd (16)
https://www.google.com/support/chrome/bin/answer.py?answer=95617 (15)
https://www.google.com/support/chrome/bin/answer.py?answer=95669 (14)
http://www.w3.org/2001/XInclude (14)
http://www.w3.org/2000/xmlns (14)
https://www.google.com/support/chrome/bin/answer.py?answer=1181003 (12)
https://www.google.com/support/chrome/bin/answer.py?answer=96817 (11)
http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd (11)
http://www.w3.org/2003/XInclude (11)
http://www.realvnc.com (11)
https://www.google.com/support/chrome/ (10)
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd (10)
http://www.w3.org/TR/REC-html40/loose.dtd (10)
SQL
50
40
30
20
10
0
SELECT name, rootpage, sql FROM '%q'.%s WHERE %s ORDER BY rowid (44)
SELECT 'INSERT INTO vacuum_db.' || quote(name) || ' SELECT * FROM main.' || quote(name) || ';' FROM vacuum_db.sqlite_master WHERE name=='sqlite_sequence'; (43)
the INDEXED BY clause is not allowed on UPDATE or DELETE statements within triggers (39)
qualified table names are not allowed on INSERT, UPDATE, and DELETE statements within triggers (39)
INSERT INTO %Q.%s VALUES('index',%Q,%Q,#%d,%Q); (39)
use DROP TABLE to delete table %s (38)
SELECT tbl,idx,stat FROM %Q.sqlite_stat1 (37)
the NOT INDEXED clause is not allowed on UPDATE or DELETE statements within triggers (36)
only a single result allowed for a SELECT that is part of an expression (36)
SELECT name, rootpage, sql FROM '%q'.%s ORDER BY rowid (36)
SELECT 'CREATE UNIQUE INDEX vacuum_db.' || substr(sql,21) FROM sqlite_master WHERE sql LIKE 'CREATE UNIQUE INDEX %' (36)
INSERT INTO vacuum_db.sqlite_master SELECT type, name, tbl_name, rootpage, sql FROM main.sqlite_master WHERE type='view' OR type='trigger' OR (type='table' AND rootpage=0) (36)
INSERT INTO (32)
SELECT count(*) FROM %Q.'%q_segdir' WHERE level = ? (31)
DELETE FROM %Q.%s WHERE tbl_name=%Q and type!='trigger' (30)
SELECT 'CREATE INDEX vacuum_db.' || substr(sql,14) FROM sqlite_master WHERE sql LIKE 'CREATE INDEX %' (29)
DELETE FROM %Q.%s WHERE name=%Q AND type='index' (29)
DELETE FROM %Q.%s WHERE %s=%Q (28)
SELECT %s (27)
DELETE FROM %Q.sqlite_sequence WHERE name=%Q (27)
UNKNOWN WITH SPACE
12500
10000
7500
5000
2500
0
GCC: (GNU) 4.7.3 (10635)
unknown error (2132)
string too long (2068)
invalid string position (2018)
iostream stream error (1968)
cl F%a:F (1174)
2F F9F (975)
K FzD(D (956)
cl'a F (932)
K F(Dc`8 (922)
`"JyD"K FzD(D (875)
#h F|h (873)
"F F9F (861)
%s: %s (826)
cl F%a (703)
#h F)F (653)
#h F1F (609)
QTMETADATA qbjs (585)
out of memory (581)
[l FyD (566)
Ql FyD (513)
Ml FyD (484)
Il FyD (479)
GCC: (GNU) 4.6.3 (458)
#h F|l (397)
vector<T> too long (370)
"l FyD (277)
#l FyD (271)
# Fca)F (179)
map/set<T> too long (174)
EMAIL
40
30
20
10
0
j@w1.fi (36)
ftp@example.com (28)
dhcp-server@isc.org (27)
appro@openssl.org (23)
posix-rename@openssh.com (18)
jseward@bzip.org (18)
ssh-rsa-cert-v01@openssh.com (17)
ssh-rsa-cert-v00@openssh.com (17)
ssh-dss-cert-v01@openssh.com (17)
ssh-dss-cert-v00@openssh.com (17)
rijndael-cbc@lysator.liu.se (17)
fstatvfs@openssh.com (17)
ecdsa-sha2-nistp256-cert-v01@openssh.com (17)
hardlink@openssh.com (16)
builder@qnx.com (16)
mclinker@googlegroups.com (15)
ecdsa-sha2-nistp521-cert-v01@openssh.com (15)
ecdsa-sha2-nistp384-cert-v01@openssh.com (15)
android-player@blackberry.com (13)
framework@services.jar (12)
name@uid.gid.mode (9)
gtk-devel-list@gnome.org (9)
fun@openssh.com (8)
resume@appgate.com (8)
pedro_m@yahoo.com (8)
lukem@NetBSD.org (8)
Jjlq@a.gl (8)
toolbar-ext@2x.png (7)
paulus@samba.org (7)
no-more-sessions@openssh.com (7)
MISC
40
30
20
10
0
Enter Private Key password: (35)
activate_backdoor (27)
X/** * Get icon with respect to the current theme * * @note This will update as soon as the theme path changes */ function fromTheme(iconPath) { /* bind to property changes - when the activeThemeId changes, tell any QML callers to re-run this function */ _themeManager.activeThemeId return _themeManager.fromTheme(iconPath) } function menuIcon(enabled, highlighted, basename) { if (highlighted) return fromTheme(basename + "_ovr.png"); else if (!enabled) return fromTheme(basename + "_dis.png"); else return fromTheme(basename + ".png"); } /** * Get icon for device type * * TODO: Move to mediaplayer/? */ function iconForDeviceType(type) { if (type === "hdd") return "HDDef"; if (type === "usb") return "USB"; if (type === "DLNA") return "DLNA"; if (type === "radio") return "radio"; if (type === "cd") return "CD"; if (type === "hdupnp") return "HDUpnp"; if (type === "ipod") return "ipod"; if (type === "mobile") return "mobile"; else return "SDCard"; } function color(colorRole) { /* bind to property change */ _palette.palette return _palette.color(colorRole) } function formatDuration(ms) { if (ms == null || ms < 1000) { return "0:00"; } var out = ""; var s = Math.floor(ms / 1000); var h = Math.floor(s / 3600); if (h > 0) { s -= h * 3600; out = h + ":"; } var m = Math.floor(s / 60); if (m > 0) { s -= m * 60; if (m < 10 && h > 0) { out += "0"; } out += m + ":"; } else if (h > 0) { out += "00:" } else { out = "0:"; } if (s < 10) { out += "0"; } out += s; return out; }; (25)
uImport QtQuick 2.0 /** * Button that has a sprite image as background. * It assumes a vertical sprite (set sprite.vertical: false to switch). The * * @p checkable Set this to true in case you want the button to be checkable * @p unpressedFrame The frame index used to paint the button in unpressed state. Default is 0. * @p pressedFrame The frame index used to paint the button in pressed state. Default is 1. * @p checkedFrame The frame index used to paint the button in checked state. Default is 2. * * @note In case the button is checkable the sprite image must have three frames * containing states [unchecked, pressed, checked]. */ ButtonArea { id: root // TODO: Get rid of these, use sprite instead property alias imageSource: sprite.source property alias imageWidth: sprite.width property alias imageHeight: sprite.height property int checkedFrame: 2 property int pressedFrame: 1 property int unpressedFrame: 0 property alias sprite: sprite width: sprite.width height: sprite.height opacity: (enabled ? 1.0 : 0.5) BasicSprite { id: sprite frameCount: (root.checkable ? 3 : 2) currentFrame: (root.checkable ? root.pressed ? root.pressedFrame : (root.checked ? root.checkedFrame : root.unpressedFrame) : root.pressed ? root.pressedFrame : root.unpressedFrame) } } (23)
ENCODED
1.0
0.8
0.6
0.4
0.2
0.0

QUESTIONS?