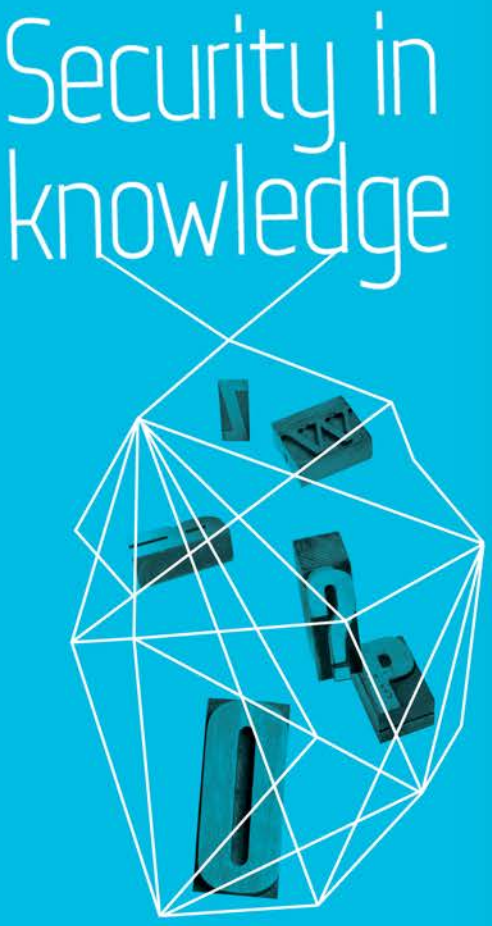
Hacking Exposed: Embedded
Securing the Unsecurable



Stuart McClure
CEO, Cylance Inc.

Billy Rios
Terry McCorkle

Justin W. Clarke
Chris Abad

Session ID: EXP-W21

Session Classification: Advanced

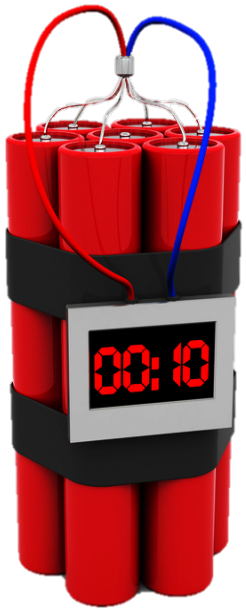
Disclaimer

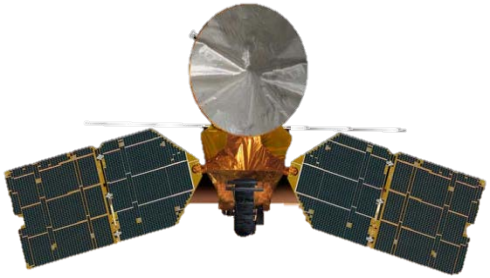
Warning:

- Loud noises during demo
- Do not sit close to the demo if you are sensitive to loud noises

World of Embedded

Estimated 10Billion WorldWide
Designed without Security
Endless Connectivity options
Few protective solutions





Embedded and RealTime Operating Systems

Access Linux Platform
AirOS by Ubiquiti Networks
AlliedWare by Allied Telesis
Android
bada
BlackBerry OS
Boot to Gecko
brickOS
CatOS by Cisco Systems
Cisco IOS by Cisco Systems
Contiki
DD-WRT by NewMedia-NET
DSPnano RTOS
eCos
Embedded Linux
Embedded Linux by Wind River
FreeBSD
freeRTOS, openRTOS and safeRTOS
FTOS by Force10 Networks
Green Hills Software
Inferno (Bell Labs)
iOS (a subset of Mac OS X)
IOS-XR by Cisco Systems
IronWare by Foundry Networks
JunOS by Juniper Networks
leJOS
LiMo Platform
MeeGo (Maemo & Moblin)
MINIX
Mobilinux
MotoMagx
NCOS
Openmoko Linux
OPhone
Palm OS
PEN/GEOS, GEOS-SC, GEOS-SE
polyBSD (embedded NetBSD)
Qt Extended
REX OS (microkernel OS)
ROM-DOS
RouterOS by Mikrotik
RTOS by Force10 Networks
RuggedCom OS by RuggedCom
ScreenOS by Juniper Networks
Symbian OS platform
ThreadX
Timos by Alcatel-Lucent
TinyOS
uClinux
Unison Operating System by RoweBots
VxWorks by Wind River Systems
webOS
Windows CE
Windows Embedded
Windows Embedded Enterprise
Windows Embedded POSReady
Windows Embedded Standard
Windows Mobile
Wombat OS (microkernel OS)
µTasker

ThreadX by ExpressLogic (rtos.com)

ARM
Atmel ARM
Atmel AVR32
BlackFin
CEVA-TeakLite-III
ColdFire/68K
Energy Micro EFM32
Freescale ARM
Fujitsu FM3
G-Series
Hitachi H8/300H
Infineon XMC-4000
Leon3
M-CORE
MicroBlaze
Microchip PIC24/dsPIC
Microchip PIC32
MIPS
Nios II
NXP
Power Architecture
Renesas RX
Renesas SH
Renesas V8xx
SHARC
ST Microelectronics STM32
StarCore
StrongARM
Synopsys ARC
TI ARM
TI MSP430
TMS320C54x
TMS320C6x
Univers A2P
Win32
x86/x386
Xilinx ARM
Xscale
Xtensa/Diamond

“Security” in Embedded today

Weatherproof

Resilient

Highly Available

Tamperproof

"Real" Security Flaws

Shared Secrets

Private certificates

Hardcoded passwords and backdoors

Open source bugs

Weak cryptography

Weak authentication

Exploitation of server software (HMI, Management, Web)

I/O communications

Distributed/Denial of Service

Exploitation of ladder logic

The first step in the 7 Stages of Death is…

DENIAL

"NONE of that stuff is on the Internet…"

41.45.169.172
TE Data
Added on 16.08.2012
ADSL Router, VxWorks SNMPv1/v2c Agent, Conexant System, Inc.

62.224.133.144
Deutsche Telekom AG
Added on 16.08.2012
Neuenstein
ADSL Router, VxWorks SNMPv1/v2c Agent, Conexant System, Inc.

208.104.181.58
Comporium Communications
Added on 16.08.2012
Fort Mill
208-104-181-58.fttp.sta.comporium.net

HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 126
EXT:
LOCATION: http://208.104.181.58:2869/IGatewayDeviceDescDoc
SERVER: VxWorks/5.4.2 UPnP/1.0 iGateway/1.1
ST: upnp:rootdevice
USN: uuid:13814000-4ff1-11f2-9be3-c67e816b4bfb::upnp:rootdevice

31.222.236.214
The Blue Zone East / Jordan
Added on 16.08.2012
VxWorks SNMPv1/v2c Agent

119.234.154.174
SingTel Mobile
Added on 01.02.2013
Singapore

HTTP/1.0 401 Unauthorized
Date: Fri, 01 Feb 2013 23:46:32 GMT
Server: HyperX/1.0 (ThreadX)
Content-Length: 0
WWW-Authenticate: Basic realm="EGX"
Keep-Alive: timeout=6, max=100
Connection: Keep-Alive
Cache-Control: public, max-age=3600

193.146.47.94
Universidad de Vigo
Added on 01.02.2013
Vigo
depx04.uvigo.es

HTTP/1.0 401 Unauthorized
Date: Sat, 02 Feb 2013 00:32:08 GMT
Server: HyperX/1.0 (ThreadX)
Content-Length: 0
WWW-Authenticate: Basic realm="EGX"
Keep-Alive: timeout=6, max=100
Connection: Keep-Alive
Cache-Control: public, max-age=3600

187.10.67.65
TELEF⊕NICA BRASIL S.A
Added on 08.02.2013
Avaré
ucd-snmp-4.1.2/eCos
187-10-67-65.dsl.telesp.net.br

200.217.48.210
Telemar Norte Leste S.A.
Added on 02.02.2013
ucd-snmp-4.1.2/eCos

177.97.177.223
Global Village Telecom
Added on 02.02.2013
Belo Horizonte
ucd-snmp-4.1.2/eCos

124.194.205.49
Dacom
Added on 01.02.2013
Seoul
Juniper Networks, Inc. ex2200-24t-4g internet router, kernel JUNOS 12.1R4.7 #0: 2012-10-24 21:59:21 UTC builder@briath.juniper.net:/volume/build/junos/12.1/release/12.1R4.7/obj-arm/junos/bsd/kernels/JUNIPER-EX-2200/kernel Build date: 2012-10-24 22:40

195.39.144.206
Qnet WAN
Added on 01.02.2013
Juniper Networks, Inc. srx650 internet router, kernel JUNOS 10.4R4.5 #0: 2011-05-06 06:14:23 UTC builder@warth.juniper.net:/volume/build/junos/10.4/release/10.4R4.5/obj-octeon/bsd/sys/compile/JSRXNLE Build date: 2011-05-06 05:56:53 UTC Copyright (c)

"THAT stuff's not on MY network…"

UDP Port 17185 - Debug port running on some 250M devices worldwide

Redline RedCONNEX AN80
HP StorageWorks MSA2012i
Toshiba e-Studio Network Printer
IBM TotalStorage SAN Switch
Canon ImageRunner Printer/Copier
Cisco MGX Chassis OS
Sonicwall Appliances
Xerox Phaser 5400
Cisco Wireless IP phones

20%

So we worry about the WRONG things…

True 0-days (public and vendor don't know)

¼-days (vendor knows, public doesn't, no fix)

½-days (vendor and public knows, no fix)

¾-days (patch available, not installed)

∞-days (it's a feature!)

Vendor knows about it,
has chosen not to fix it

RSA CONFERENCE 2013

EMBEDDED HACKING
DeathStar Style

Jan. 2008 – Lodz, Poland

"He treated it like any other schoolboy might a giant train set, but it was lucky nobody was killed."

- Miroslaw Micor, Lodz Police

"Features" can Kill…

Infusion Pumps
Insulin Pumps
Implantable Cardiac Defibrillators (ICDs)
Implantable Deep Brain Neurostimulators

You can't make this stuff up…

- **Season 2 – "Broken Hearts" episode: Pacemaker**

"Features" can Eavesdrop and Control

GSM Authentication Spoofing (2012)

Read and Write SMS
Make and Receive Calls
Approve 2nd factor requests
Spoof all activity
Use the device Fradulently

“Features” can Eavesdrop and Control

iJacking – iDevice MITM (2011)
Android Zero Shell (2012)
ATT 5ESS hacking (2012)
Rogue USB mouse (2012)
NFC and Bluetooth hacking (2012)
Garretcom (2012)
Ruggedcom (2012)


```
-----BEGIN RSA PRIVATE KEY-----
MIICWAIBAAKBgEBdBnFfd2mu9V7Sk9dUyuGZgXklqzQfNwcflQmjvp/EHm+Y/50m
iudCIUFfrqlt/yAS5QSGsiEks6kjsmKxNGBhcFHiNuvXWOqGDIT5ihgH+HQpImVn
J1tC2ZYl5qb/hoIVKHx4DVjVtd1EaAXCoftbh+SlTRquMvcPdbdyCVMFAgMBAAEC
gYAt0kxg8EcyLQWwsRfhiBM70y4y0ld1LvfdEWXoS/PNCDFm37Sy65qeEx1bzkOp
iY7FBc6Xj1FHeTqSosA/tMqFUHP+ysoBcHDGoovN/eFqT008PBqlmGxXYxYq42am
CUpLJ50VyDbzOPd3j7xYwpC5SMB8WDsW0Wcm5DT0XnnyDQJAgHgJHdxrU3vNY6o3
O1ZIZ5kUUiPTEVJunWAGGp8R6iW1ZsIcBkgTW5gZSX6yIAE3HmCsbjJyiH0xMpw3
UpU8PwJAgEHGFn4ngURreUsV+1niHPs/VA/2Cr0x3yN8Lxx94USHYgFSv2IxY95p
VhNyUA8oRyxndWZChzNZTapkiFlvuwJAYDkIIwyYesQs12yDx/bdbnMS7F8W1U+X
uFpW2BOy+FzcHSZglTfg/+bRceHqitw+K4ufOz6f2KlkcxLcwQc0QwJAeGFD04jE
+4eEeGwJTcmneRw47GWuwZWiYZWk0XMkk3MGvu4PBKLdSKdQpwHJoWsYmvUKhh5d
AxknEMaFZZTMUQJAE7t5oIJXL/FSf01kQKMpOoooHhwyT/oVWTtIji0tcfd8DfD9
N2t//6LChzOdCEtdszLXjeaODIMCZiuuEscc9w==
-----END RSA PRIVATE KEY-----
```

LIVE HACKS

Hack Scenario

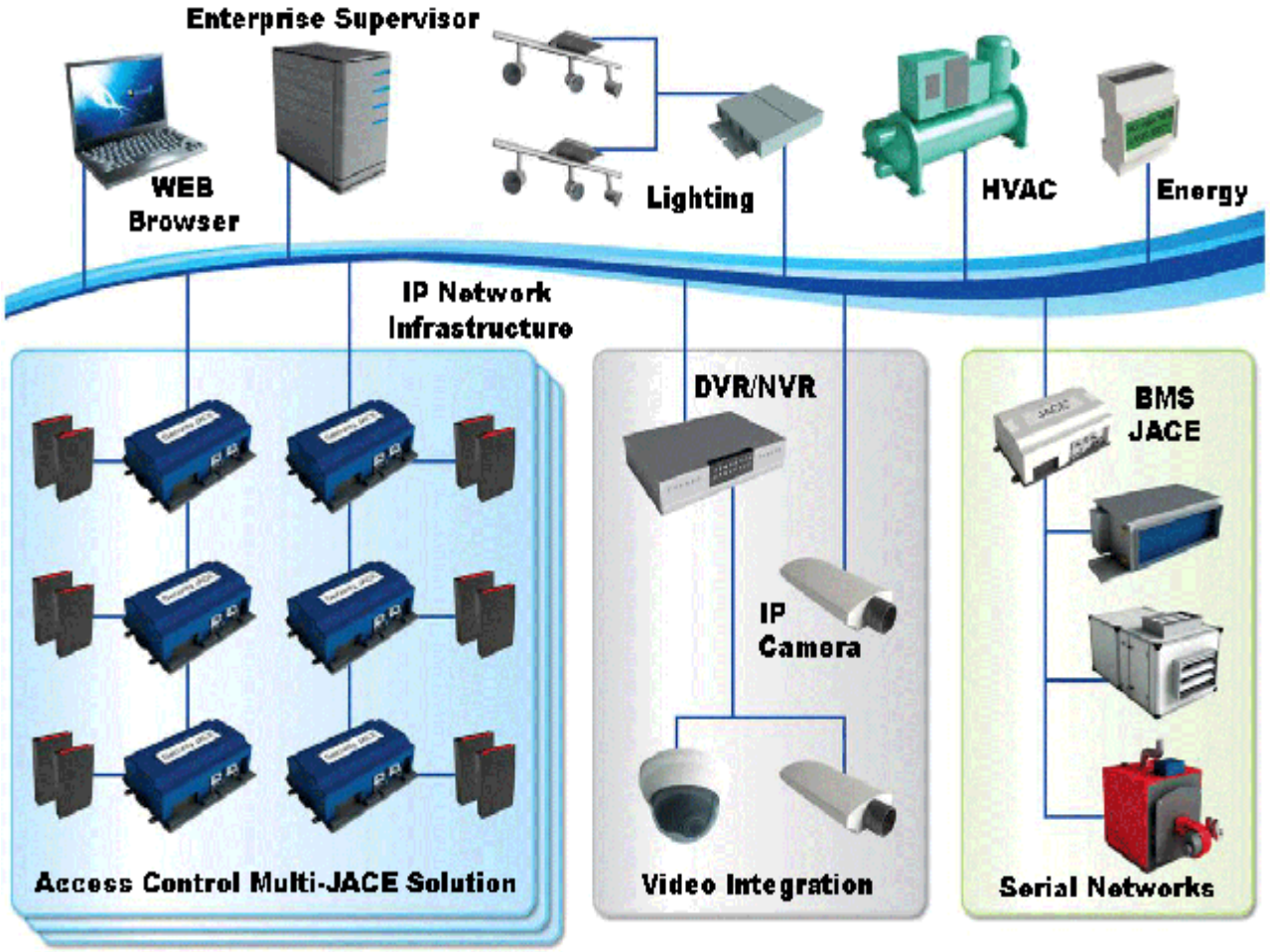
- Sit in car outside office parking lot
- Samsung TVs in the lobby
- Gain access to internal network
- Find and attack the Building Management Server
- Control door access
- When all else fails, just use “the key”…

Samsung "Smart" TV Vulnerability

- Unauthenticated IR
- Universal Remote, replaced IR LED with IR Laser
- Long distance (200 feet) possible
- Full reconfiguration of TV including TV as Access Point
- Access to full network resources
- Pose as the user on the system for FB, Twitter, mail, etc.

LIVE DEMO

Tridium Niagara AX Framework



Niagara Vulnerability

Remote

Pre-authentication

Privilege escalation

ROOT on embedded and SYSTEM on Win32 (SoftJace)

LIVE DEMO

Lockbox Vulnerability

Hardened, weatherproof, industrial key storage

Fire/Police/Emergency access

Keyed by district/county/state

Available on eBay

Rekeying possible

Instant access to buildings

Shared secret problem

LIVE DEMO

IT'S HOPELESS!!

COUNTERMEASURES

Samsung Countermeasures

- Disable IR port w/black electrical
  - Use your Bluetooth remote until…
- IDS to detect suspect network attempts
- Patched and Hardened Endpoint with Firewalls
- Hardwire network onto DMZ network
- Make sure all patches have been applied as soon as they are made available
- Double pane or tinted window glass

Tridium Countermeasures

- Tridium
  - Restrict physical access to the box
  - Remove systems from the Internet
  - ACLs approved remote management IPs
    - Web (80)
    - Fox TCP 1911 and Platform TCP 3011 (restrict at firewall and alert)
  - Enforce VPN in front of any systems
  - Sign the Java modules (vendor should do this)
  - Inline Serial PLC monitoring IN/OUT
  - Hardware safety controls

Lockbox Countermeasures

- Connect tamper switches from a Knox Box to fire and/or security alarm system(s)
- Track and audit all keys and other materials within your Knox Box
- Have a plan to revoke access to any compromised keys within your Knox Box
- Install and manage CCTV
- Ensure Knox Boxes are within your CCTV's field of view
- Use this as a lesson to think about other inherent low-hanging risks to your facilities that may be overlooked
- Install and manage Door Entry Alarm systems (and don't let them get hacked)

Where to Hunt?

RECON

Footprinting

Scanning

Enumeration

Assessment

ACCESS

Exploitation

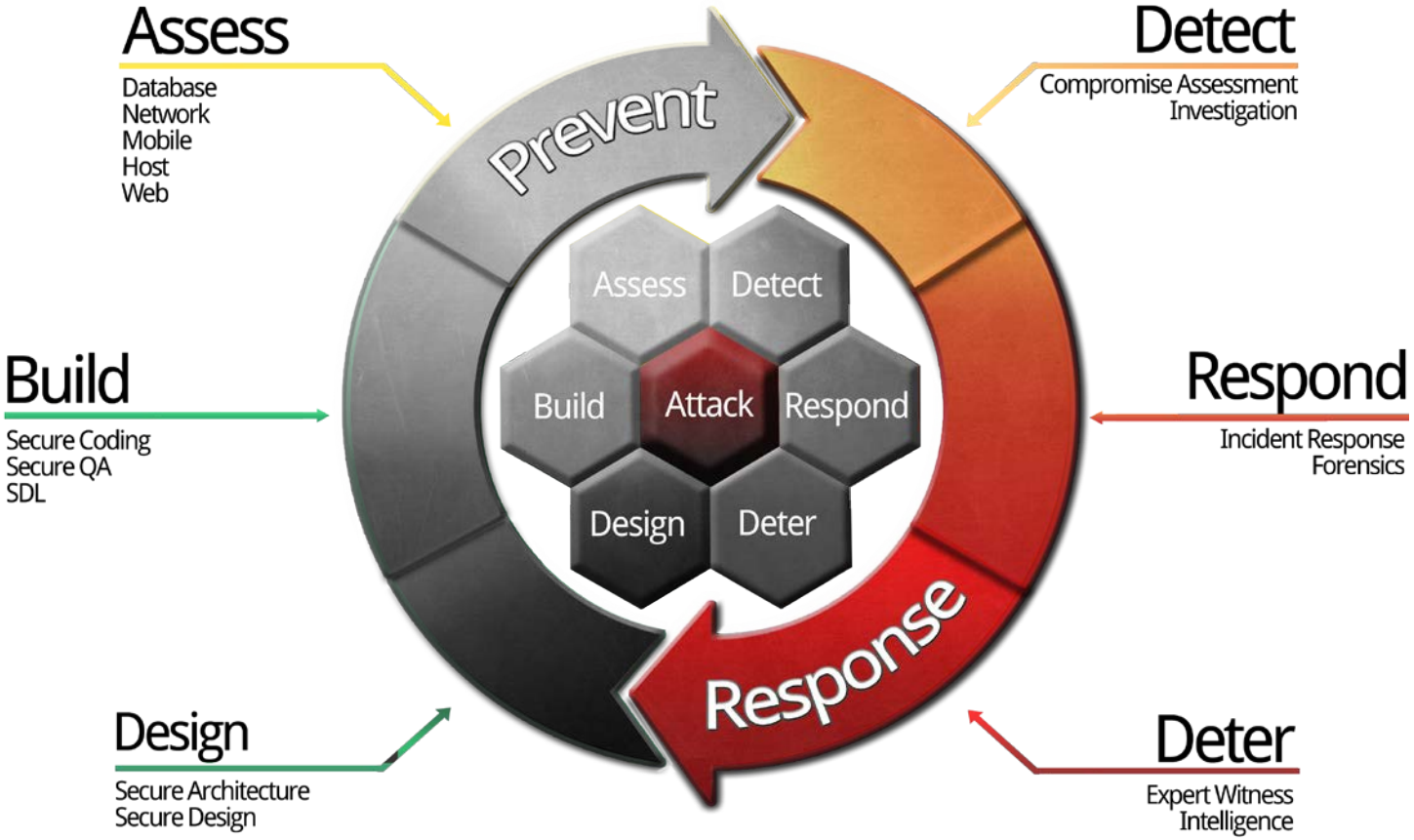
Priv. Esc

C2/RATs

Pivot/Spread

DAMAGE

Address the CORE of the problem



True Solutions to the Security Problem

Inputs (90%)

Wifi/RJ45, RJ-11, DB-9, RF, GPS, Bluetooth, IR,
RS-232, RS-485, HDMI, DVI, SATA, USB

Processing (8%)

Memory management, encryption,
boot loaders logic, ROMs

Outputs (2%)

Exports, alerting, printing,
disk writes (/tmp), extended memory

Resources

www.hackingexposed.com

www.twitter.com/hackingexposed

www.twitter.com/cylanceinc

www.linkedin.com/company/cylanceinc

www.facebook.com/CylanceInc

www.youtube.com/stuartmcclureYT

www.youtube.com/user/HackingExposedLIVE

Book Signings

- Wed. Feb. 27 @ 11am to noon
  HBGary/Mantech booth #2650
- Wed. Feb. 27 @ 3pm to 4pm
  Cigital booth #132
- Thu. Feb. 28 @ 11am to noon
  CounterTack booth, #2533

Thank you!