

# EMBEDDED HACKING

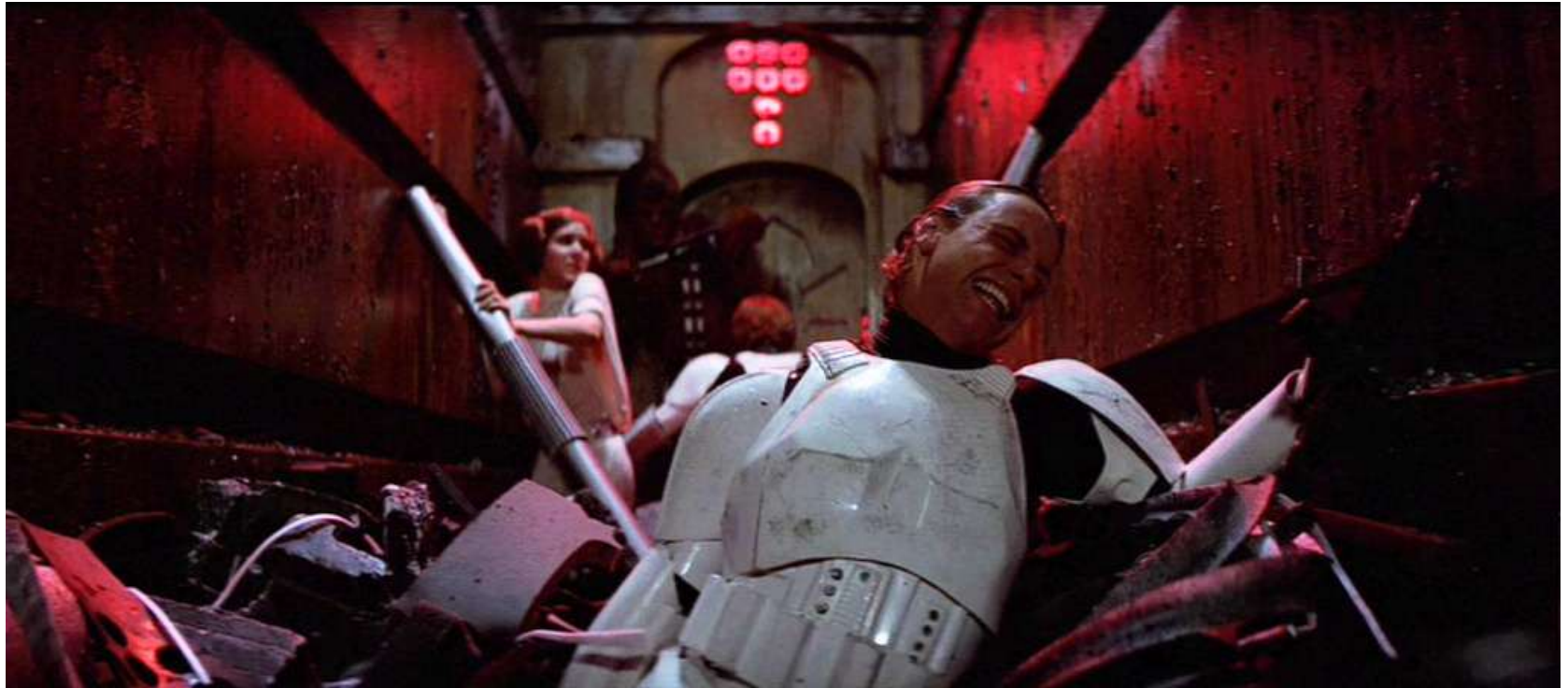
**STUART MCCLURE**  
CYLANCE, INC.



Session ID: HTA-201

Session Classification: Advanced

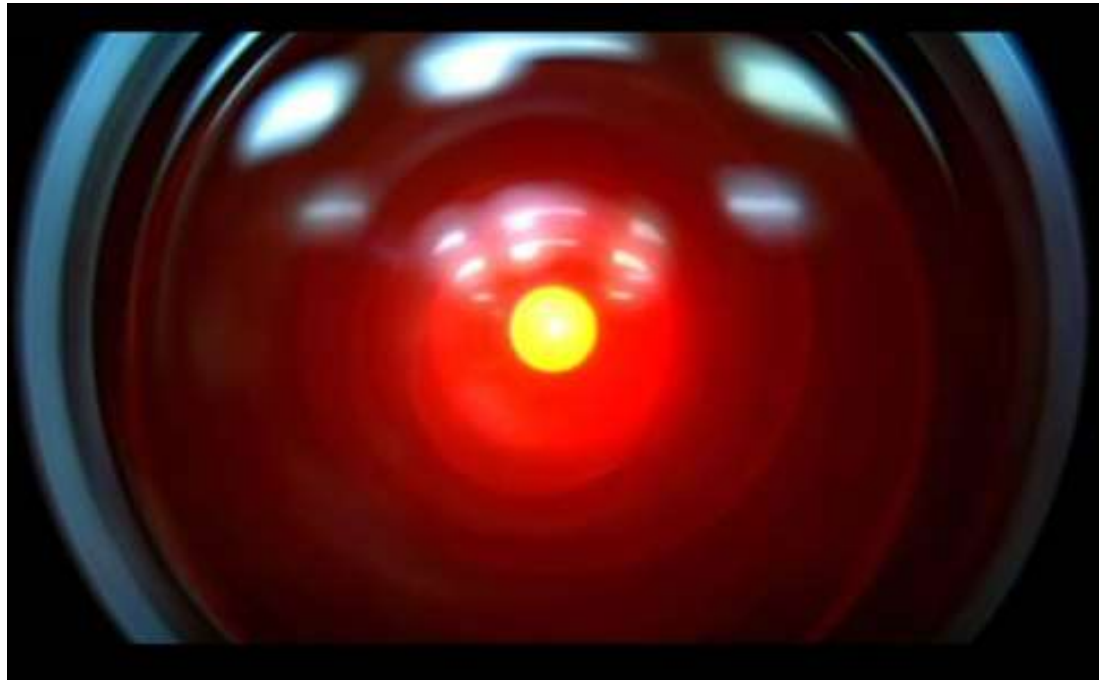
**RSACONFERENCE**  
EUROPE 2012





**Star Wars (1977)**





**2001: A Space Odyssey (1968)**



# We be talkin...

## Focus 2011



**FOCUS<sup>11</sup>**  
SECURITY CONFERENCE

Hacking Exposed LIVE: Embedded

WE HAVE EVOLVED FROM WINDOWS

- ENERGY
- SMART CARS
- EMBEDDED
- MAIL FACTORIES
- RSA
- INDUSTRIAL DEVICES
- COMPOSER
- DATA BASES
- SCADA
- MOBILE
- SLICOR
- EVANET
- ALPINA
- BEIS
- MOBILE MEDIA

**BLUETAPPING**

- Discover and coverable Bluetooth devices and pair with them
- Listen to the traffic without pairing

INTERCEPTED

McAfee

FOCUS<sup>11</sup>

## RSA 2012 Keynote



## RSA Hacking Exposed



# World of Embedded

- ~10 Billion devices WW
- Little to NO security by design
- Radio, GPS, Wifi, Bluetooth and hardwire connectivity
- No protective solutions



# Embedded/RTOSes

BlackBerry OS  
Embedded Linux  
Access Linux Platform  
Android  
bada  
Boot to Gecko  
Openmoko Linux  
OPhone  
MeeGo (from merger of Maemo & Moblin)  
Mobilinux  
MotoMagx  
Qt Extended  
LiMo Platform  
webOS  
PEN/GEOS, GEOS-SC, GEOS-SE  
**iOS** (a subset of Mac OS X)  
Palm OS  
Symbian platform (successor to Symbian OS)  
Windows Mobile (superseded by Windows Phone)

AlliedWare by Allied Telesis  
AirOS by Ubiquiti Networks  
CatOS by Cisco Systems  
Cisco IOS by Cisco Systems  
DD-WRT by NewMedia-NET  
Inferno (distributed OS originally from Bell Labs)  
IOS-XR by Cisco Systems  
IronWare by Foundry Networks  
JunOS by Juniper Networks  
**RuggedCom OS by RuggedCom**  
RouterOS by Mikrotik  
ScreenOS by Juniper Networks  
Timos by Alcatel-Lucent  
Unison Operating System by RoweBots  
FTOS by Force10 Networks  
RTOS by Force10 Networks  
**VxWorks by Wind River Systems**  
**Embedded Linux by Wind River Systems**  
**Green Hills Software**

Contiki  
eCos  
FreeBSD  
uClinux  
MINIX  
NCOS  
freeRTOS, openRTOS and safeRTOS  
polyBSD (embedded NetBSD)  
REX OS (microkernel OS)  
ROM-DOS  
TinyOS  
 $\mu$ Tasker  
**ThreadX**  
DSPnano RTOS  
**Windows Embedded**  
Windows CE  
Windows Embedded Standard  
Windows Embedded Enterprise  
Windows Embedded POSReady  
Wombat OS (microkernel OS))  
brickOS  
leJOS



# ThreadX by ExpressLogic

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

THREADX UNITS HARD AT WORK

1,289,333,044





# VxWorks and Embedded Linux

*By Wind River Systems*

- ~2B devices today



# Infrastructure

August, 2010

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

## Enterprise Customer Survey

- 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 MGX or IOS 12.X devices
- Cisco Wireless IP phones



# Shodan

**41.45.169.172**

TE Data

Added on 16.08.2012



**62.224.133.144**

Deutsche Telekom AG

Added on 16.08.2012



Neuenstein

**208.104.181.58**

Comporium Communications

Added on 16.08.2012



Fort Mill

208-104-181-58.ftp.sta.comporium.net

ADSL Router, **VxWorks** SNMPv1/v2c Agent, Conexant System, Inc.

ADSL Router, **VxWorks** SNMPv1/v2c Agent, Conexant System, Inc.

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-c67e816b4fbf::upnp:rootdevice

**114.129.177.17**

SkyMesh Satellite Network

Added on 16.08.2012



**vxWorks-6.6 Target**

**64.105.18.30**

Covad Communications

Added on 16.08.2012

Chicago

h-64-105-18-

30.chcgigm.static.covad.net

HTTP/1.1 200 OK

CACHE-CONTROL: max-age = 126

EXT:

LOCATION: http://64.105.18.30:2869/IGatewayWEADeviceDescDoc

SERVER: **VxWorks** 5.4.2 UPnP/1.0 iGateway/1.1

ST: upnp:rootdevice

USN: uuid:33814000-1dd1-11b2-9ff-c67e816b4fbf::upnp:rootdevice

**218.48.175.18**

Hanaro Telecom Co.

Added on 16.08.2012



**VxWorks** SNMPv1/v2c Agent

**31.222.236.214**

The Blue Zone East / Jordan

Added on 16.08.2012

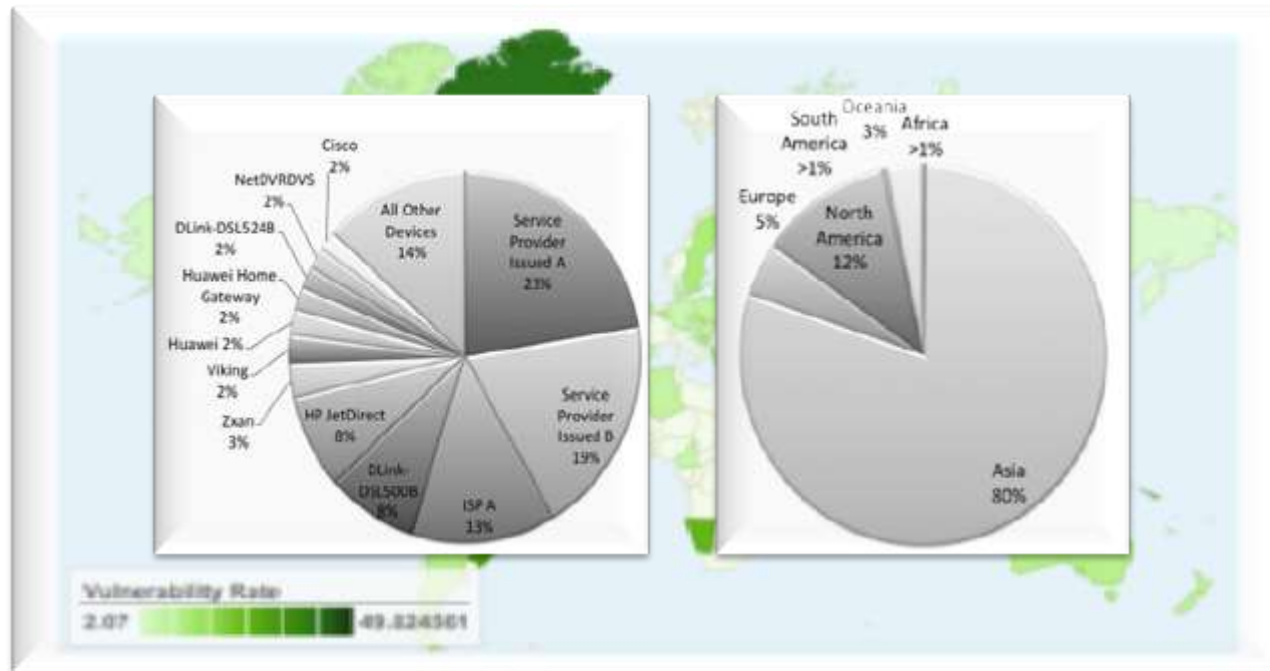


**VxWorks** SNMPv1/v2c Agent



# Columbia University Finding

- 3.9M discovered
- 540K vulnerable default “root” passwords (13% of discovered)



# New One: The Web Server Uses SSL!

## 1.3. The ROS® Web Server Interface

### 1.3.1. Using a Web Browser to Access the Web Interface

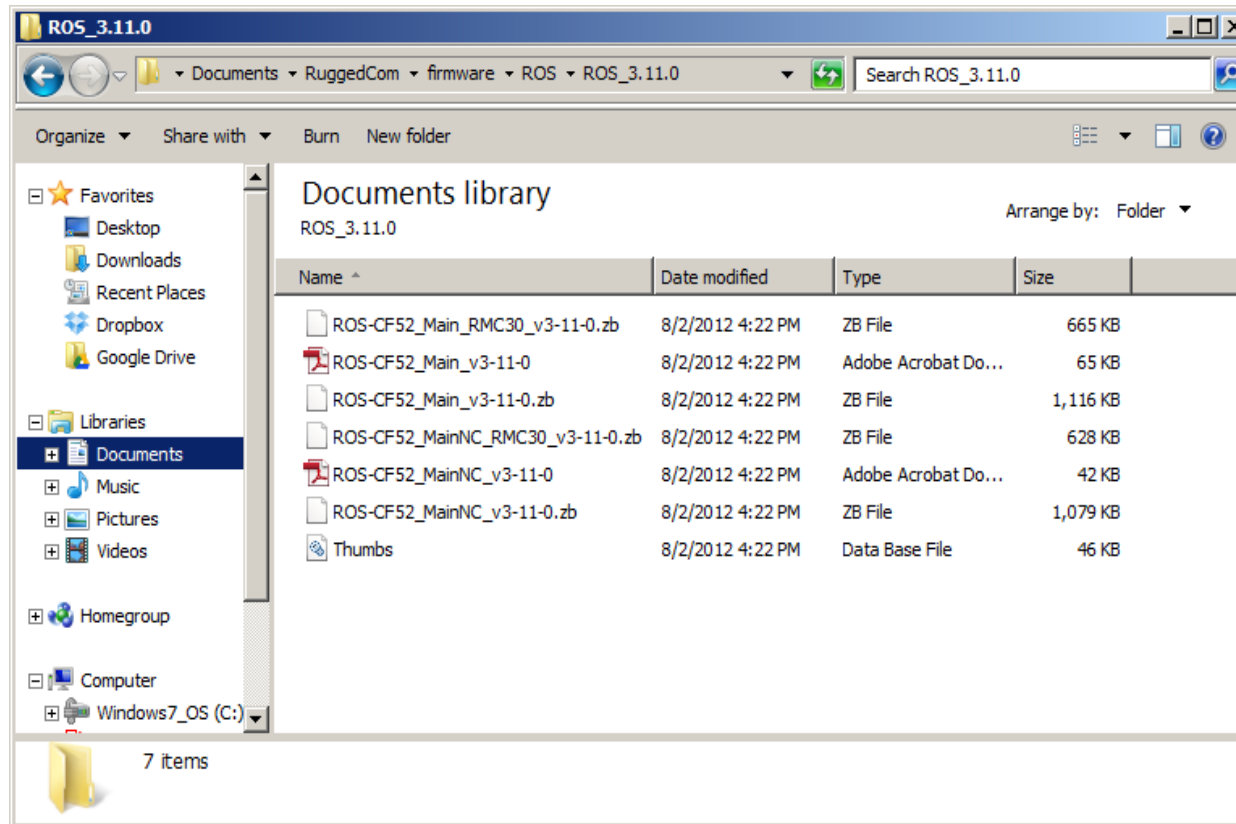
A web browser uses a secure communications method called SSL (Secure Socket Layer) to encrypt traffic exchanged with its clients. The web server guarantees that communications with the client are kept private. If the client requests access via an insecure HTTP port, it will be rerouted to the secure port. Access to the web server via SSL will be granted to a client that provides a valid user name / password pair.



*It can happen that upon connecting to the ROS® web server, a web browser may report that it cannot verify the authenticity of the server's certificate against any of its known certificate authorities. This is expected, and it is safe to instruct the browser to accept the certificate. Once the browser accepts the certificate, all communications with the web server will be secure.*



# Step 1: Acquire Firmware



# Step 2: Unpack

```
jc@grids:~/ROS_3.11.0
[jc@grids ROS_3.11.0]$ deezee ./ROS-CF52_Main_v3-11-0.zb
Scanning file ./ROS-CF52_Main_v3-11-0.zb for compressed components
Compressed size: 1142052 bytes
Compressed segment found at 0x51d1. Expanded to 635584 bytes
Compressed segment found at 0x346b5. Expanded to 2436768 bytes
[jc@grids ROS_3.11.0]$ md5sum *
07d22863c37cce8afee73ffdcdd592b8 ROS-CF52_MainNC_RMC30_v3-11-0.zb
d42b30fabbd53ab9395a99123fb82a5 ROS-CF52_MainNC_v3-11-0.pdf
85a296186b2bd25762e8f4012ae312c4 ROS-CF52_MainNC_v3-11-0.zb
320026d7dcl1a2a8de5d2727c26c3c743 ROS-CF52_Main_RMC30_v3-11-0.zb
5e4c783f4833b20cb00915e55dd467dc ROS-CF52_Main_v3-11-0.pdf
8aaa2eed09973d6a9d039e1bcbf942c9 ROS-CF52_Main_v3-11-0.zb
e1e5cb625cc57198e2ef5e6b4f0f7403 ROS-CF52_Main_v3-11-0.zb.0
a0977d1e39d2fae577c80d28b80cfe7c ROS-CF52_Main_v3-11-0.zb.1
d41d8cd98f00b204e9800998ecf8427e ROS-CF52_Main_v3-11-0.zb.2
5dc291a5a2e262eca1b756aa9283af4a Thumbs.db
[jc@grids ROS_3.11.0]$
```







# Step 3: Locate Crypto Goldmine

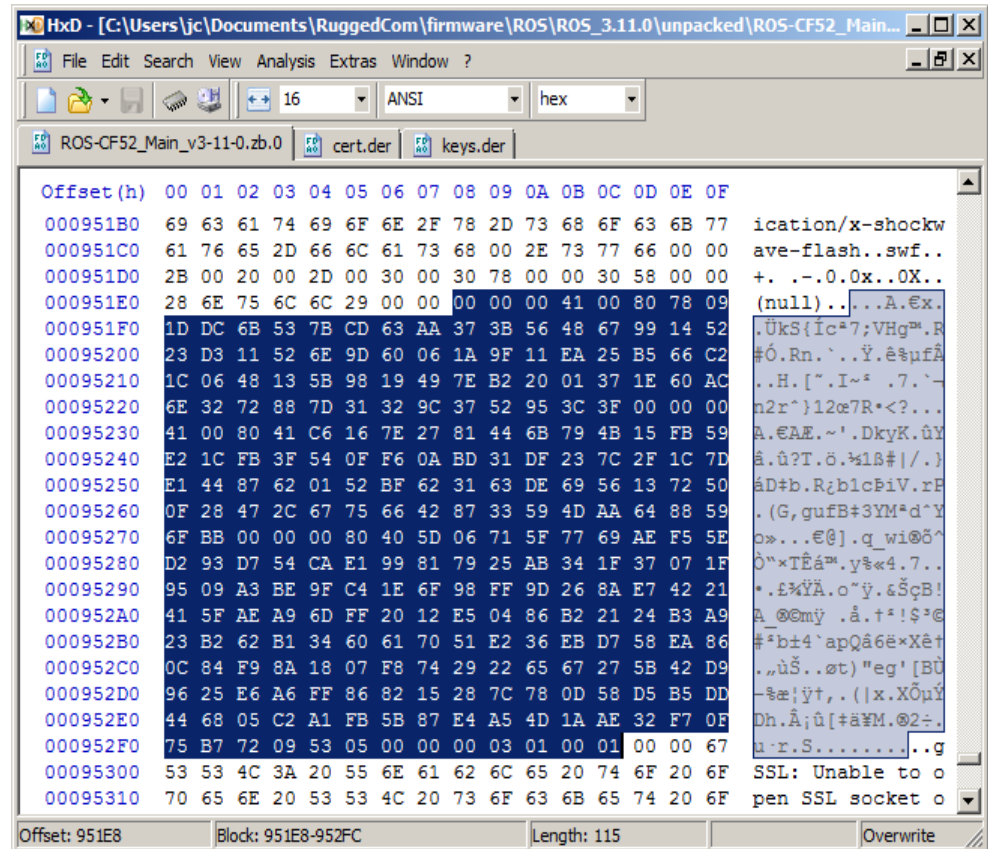
1. Find Public Cert
2. Validate Cert With OpenSSL

```
/cygdrive/c/users/jc/Documents
jc@GRIDS /cygdrive/c/users/jc/Documents
$ openssl x509 -inform DER -in cert.der -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4a:a4:c0:d7:02:a2:ea:39:39:ea:0c:ef:2c:20:f6:1f:f2:a0:a3:95
    Signature Algorithm: md5withRSAEncryption
    Issuer: C=Canada, ST=Ontario, L=Concord, O=Ruggedcom Inc., OU=En
    ggedcom.com
    Validity
      Not Before: Aug 18 00:01:26 2005 GMT
      Not After : Aug 18 00:01:26 2025 GMT
    Subject: C=Canada, ST=Ontario, L=Concord, O=Ruggedcom Inc., OU=
    uggedcom.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1023 bit)
      Modulus:
        40:5d:06:71:5f:77:69:ae:f5:5e:d2:93:d7:54:ca:
        e1:99:81:79:25:ab:34:1f:37:07:1f:95:09:a3:be:
        9f:c4:1e:6f:98:ff:9d:26:8a:e7:42:21:41:5f:ae:
        a9:6d:ff:20:12:e5:04:86:b2:21:24:b3:a9:23:b2:
        62:b1:34:60:61:70:51:e2:36:eb:d7:58:ea:86:0c:
        84:f9:8a:18:07:f8:74:29:22:65:67:27:5b:42:d9:
        96:25:e6:a6:ff:86:82:15:28:7c:78:0d:58:d5:b5:
        dd:44:68:05:c2:a1:fb:5b:87:e4:a5:4d:1a:ae:32:
        f7:0f:75:b7:72:09:53:05
      Exponent: 65537 (0x10001)
    Signature Algorithm: md5withRSAEncryption
      3d:49:87:20:d2:ce:e4:5b:87:43:61:fc:5b:46:f8:2c:a2:34:
      ff:66:51:c1:15:7f:46:4e:e4:c5:6b:bf:b7:b5:f1:bd:38:07:
      67:91:47:8d:94:f7:2e:61:3d:65:d2:1c:ee:52:4e:b1:03:6a:
      cb:e9:d5:71:a2:6c:ff:1f:c5:d1:1c:df:c1:43:56:8e:b5:81:
      0c:35:72:18:f4:b8:cf:7c:3d:ac:ca:62:b0:7c:6c:20:e1:d1:
      2c:f2:df:fd:41:51:36:0d:74:87:b8:ca:e3:3e:28:ab:c0:
      1b:c2:fc:78:67:64:21:8a:b9:24:bf:37:cc:26:3f:03:13:57:
      a3:be
-----BEGIN CERTIFICATE-----
MIICeJCCAeOgAwIBAgIUSqTA1wki6jk56gzvLCD2H/Kgo5UwCwYJKoZIhvcNAQEE
MHwxDzANBgNVBAYTBkNhbmcKfYEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBmMx
Q29uY29yZDEuXzEwLjYyYy4xZDAsBgNVBA8TODVud211u
ZWVyaW50YXJpbzEQMA4GA1UEBmMxQ29uY29yZDEuXzEwLjYyYy4xZDAsBgNVBA8T
ODVud211u
ZTI1MDgwODAwMDEyLjYyYy4xZDAsBgNVBA8TODVud211u
cm1vMRAwDgYDVQQHEwdB25jb3JkMRcwFQYDVQQKEw5SdWdnZWRjb20gSW5JLjEJ
MBIGA1UECMLRw5naW5lZXJpbmNlcjEjZ2ZlZGZlZGZlZGZlZGZlZGZlZGZlZGZl
CwYJKoZIhvcNAQEBAAQGMADCBiAKBgEBdBnFfd2mu9V7Sk9duyugZgXk1qzQFNwcf
lQmjvp/EHm+Y/50miudCIUffrqlt/yAS5QSGSiEks6kjsmKxNGBhCFHINuvXW0qG
DIT5ihgH+HQpImVnJ1tC2ZY15qb/hoIVKHx4DvjVtD1EaAXCoFtbh+S1TrqumVcP
dbdyCVMFAGmBAAEwDQYJKoZIhvcNAQEEBQADgYEAPUmHINL0SFuHQ2H8W0b4LKOZ
/2ZRwRV/Rk7kxwu/t7XxvTGHZ5FHjZT3LmE9ZdIc7lJ0s0Nqy+hVcaJ5/x/FORf
wUNWjrwBDDVvGPS4z3w9rMpiSHxsIOHRLPLf/UFRRNg10h7jJk4z40gkvAG8L8eGdk
IYq5JL83zCY/AxNXo74=
-----END CERTIFICATE-----
```



# Step 3: Locate Crypto Goldmine

1. Find Public Cert
2. Validate Cert With OpenSSL
3. Find Private Key



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000951B0 69 63 61 74 69 6F 6E 2F 78 2D 73 68 6F 63 6B 77  ication/x-shockw
000951C0 61 76 65 2D 66 6C 61 73 68 00 2E 73 77 66 00 00  ave-flash..swf..
000951D0 2B 00 20 00 2D 00 30 00 30 78 00 00 30 58 00 00  +. -.0.0x..0X..
000951E0 28 6E 75 6C 6C 29 00 00 00 00 00 41 00 80 78 09  (null)...A.€x.
000951F0 1D DC 6B 53 7B CD 63 AA 37 3B 56 48 67 99 14 52  .ÜkS{Ïc^7;VHg™.R
00095200 23 D3 11 52 6E 9D 60 06 1A 9F 11 EA 25 B5 66 C2  #Ó.Rn.´.ÿ.è&µfÅ
00095210 1C 06 48 13 5B 98 19 49 7E B2 20 01 37 1E 60 AC  ..H.[^I~^ .7.`-
00095220 6E 32 72 88 7D 31 32 9C 37 52 95 3C 3F 00 00 00  n2r^}12œ7R*?<...
00095230 41 00 80 41 C6 16 7E 27 81 44 6B 79 4B 15 FB 59  A.€AE.~'.DkyK.ûY
00095240 E2 1C FB 3F 54 0F F6 0A BD 31 DF 23 7C 2F 1C 7D  ä.û?T.ö.*1B#|/.)
00095250 E1 44 87 62 01 52 BF 62 31 63 DE 69 56 13 72 50  áD+b.R¿b1cPiV.rF
00095260 0F 28 47 2C 67 75 66 42 87 33 59 4D AA 64 88 59  .(G,gufB+3YM*d^Y
00095270 6F BB 00 00 00 80 40 5D 06 71 5F 77 69 AE F5 5E  o>...€@].q wi@ð^
00095280 D2 93 D7 54 CA E1 99 81 79 25 AB 34 1F 37 07 1F  ò^*TÈá™.y&«4.7..
00095290 95 09 A3 BE 9F C4 1E 6F 98 FF 9D 26 8A E7 42 21  *.f%YÄ.o^ÿ.€ŠçB!
000952A0 41 5F AE A9 6D FF 20 12 E5 04 86 B2 21 24 B3 A9  A_@œmÿ .á.+*!$*€
000952B0 23 B2 62 B1 34 60 61 70 51 E2 36 EB D7 58 EA 86  #*b±4`apQâ6è×Xê†
000952C0 0C 84 F9 8A 18 07 F8 74 29 22 65 67 27 5B 42 D9  ..,üŠ..øt)"eg'[BÜ
000952D0 96 25 E6 A6 FF 86 82 15 28 7C 78 0D 58 D5 B5 DD  -&æ!ÿ†.(|x.XÖµÿ
000952E0 44 68 05 C2 A1 FB 5B 87 E4 A5 4D 1A AE 32 F7 0F  Dh.Ä;û[+ã¥M.ø2÷.
000952F0 75 B7 72 09 53 05 00 00 00 03 01 00 01 00 00 67  u.r.S.....].g
00095300 53 53 4C 3A 20 55 6E 61 62 6C 65 20 74 6F 20 6F  SSL: Unable to o
00095310 70 65 6E 20 53 53 4C 20 73 6F 63 6B 65 74 20 6F  pen SSL socket o
Offset: 951E8 Block: 951E8-952FC Length: 115 Overwrite
```

# Step 3: Locate Crypto Goldmine

1. Find Public Cert
2. Validate Cert With OpenSSL
3. Find Private Key
4. Ask Vendor How To Decode

## 4.15 How are Keyblobs formatted?

NanoSSL uses callback functions during authentication to verify public keys, string representations of Mocana version 1 keyblobs, formatted as follows:

- For RSA keys, the data following the header is:
  - 4 bytes length of e string
  - n bytes length of e byte string
  - 4 bytes length of n string
  - n bytes length of n byte string
  - 4 bytes length of p string
  - n bytes length of p byte string
  - 4 bytes length of q string
  - n bytes length of q byte string



# Step 4: Turn Numbers Into Certs

1. Using RSA values P, Q, N, E from firmware, calculate other values: d, dP, dQ, qInv  
[http://mobilefish.com/services/rsa\\_key\\_generation/rsa\\_key\\_generation.php](http://mobilefish.com/services/rsa_key_generation/rsa_key_generation.php)
2. Create PEM-encoded RSA private key:  
Use an ASN.1 editor  
<http://lipingshare.com/Asn1Editor>



# Step 4: Turn Numbers Into Certs

Yes, this really is the RuggedCom private key

```
-----BEGIN RSA PRIVATE KEY-----
MIICWAIBAABgEBdBnFfd2mu9V7Sk9dUyuGZgXklqzQfNwcf1Qmjvp/EHm+Y/50m
iudCIUffrqlt/yAS5QSGsiEks6kjsmKxNGBhcfHiNuvXWOqGDIT5ihgH+HQpImVn
J1tC2ZYl5qb/hoIVKHx4DVjVtd1EaAXCofTbh+S1TRquMvcPdbdyCVMFAgMBAAEC
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-----
```



# Step 5: Does it Decrypt?

The image shows a Wireshark capture of network traffic. The top part shows a list of packets, with packet 246 selected. The packet details pane shows the following layers:

- Frame 246: 736 bytes on wire (5888 bits), 736 bytes captured (5888 bits)
- Ethernet II, Src: IntelCor\_79:57:70 (24:77:03:79:57:70), Dst: Ruggedco\_06:22:1c (00:0a:dc:06:22:1c)
- Internet Protocol Version 4, Src: 10.0.1.9, Dst: 10.0.1.187 (10.0.1.187)
- Transmission Control Protocol, Src Port: 47692 (47692), Dst Port: https (443), Seq: 227, Ack: 111, Len: 736
- Secure Sockets Layer
  - TLSv1 Record Layer: Application Data Protocol: ssl
    - Content Type: Application Data (23)
    - Version: TLS 1.0 (0x0301)
    - Length: 32
    - Encrypted Application Data: 913a81c1983fa31f79721ff82bb93f5cf026ab768d00fa3e...
  - TLSv1 Record Layer: Application Data Protocol: ssl
    - Content Type: Application Data (23)
    - Version: TLS 1.0 (0x0301)
    - Length: 640

The packet bytes pane shows the raw data for the selected packet, with the following hex and ASCII values:

Offset	Hex	ASCII
0190	0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 73	..Referer: https
01a0	3a 2f 2f 31 30 2e 30 2e 31 2e 31 38 37 2f 49 6e	://10.0.1.187/in
01b0	69 74 69 61 6c 50 61 67 65 2e 61 73 70 0d 0a 41	itialPage.asp..A
01c0	63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	cept-Encoding:
01d0	67 7a 69 70 2c 64 65 66 6c 61 74 65 2c 73 64 63	gzip,deflate,sdc
01e0	68 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61	h..Accept-Langua
01f0	67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30	ge: en-US,en;q=0
0200	2e 38 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73	.8..Accept-Chars
0210	65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75	et: ISO-8859-1,u
0220	74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30	tf-8;q=0.7,*;q=0
0230	2e 33 0d 0a 0d 0a 55 73 65 72 3d 61 64 6d 69 6e	.3...User=admin
0240	26 50 61 73 73 77 6f 72 64 3d 61 64 6d 69 6e 26	&Password=admin&
0250	63 68 6f 69 63 65 3d 4c 6f 67 49 6e	choice=Login

The bottom of the packet bytes pane shows the decryption status:

Frame (736 bytes) | Decrypted SSL data (1 bytes) | Decrypted SSL data (604 bytes)



# Stuxnet



# Infusion Pumps





# Insulin Pumps

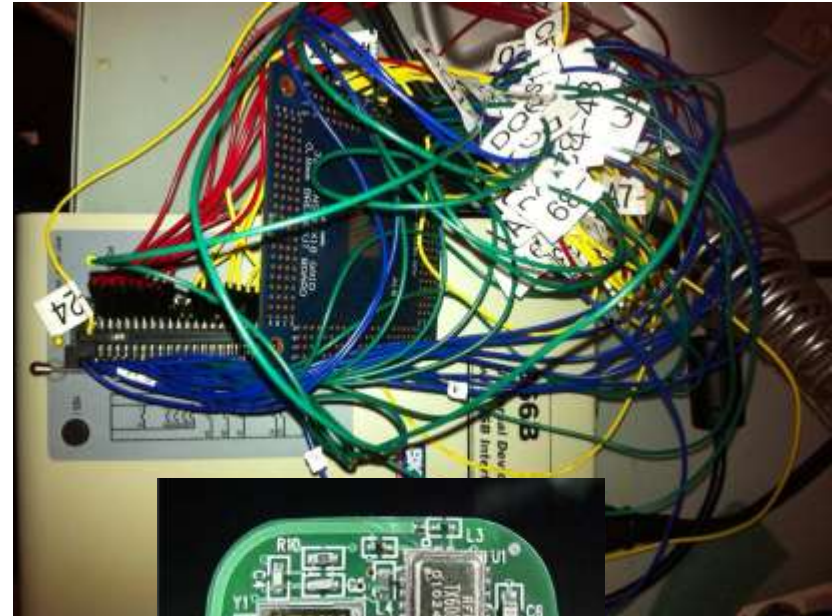


# Insulin Pumps



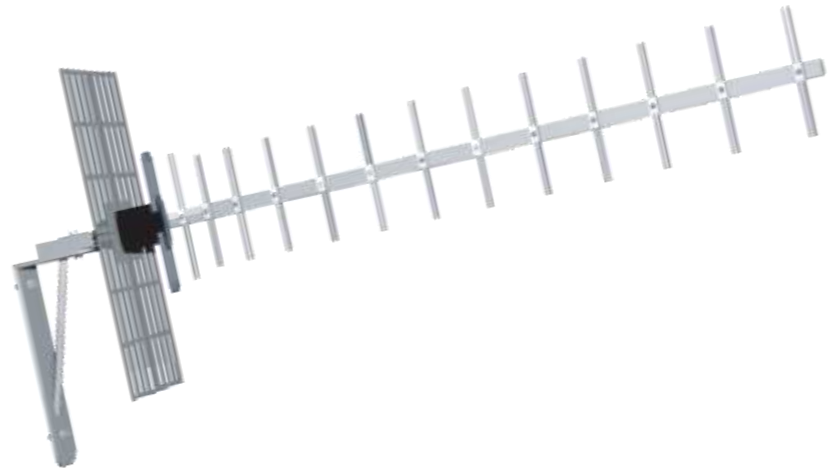
# Locating Vulnerabilities

- Disassembled insulin pump and removed all chips
- Reversed engineered all ROMs
- Documented all core functionality
- Focused on RF packet handling code
- Found backdoor in authentication routine



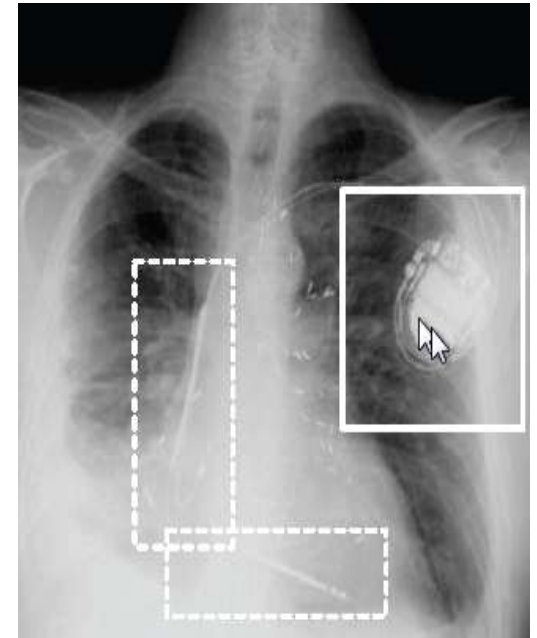
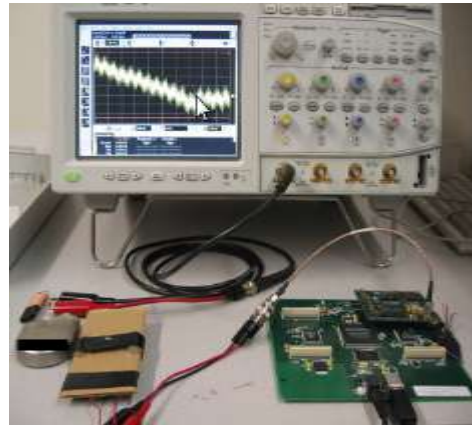
# Insulin Pump Vulnerability

- Backdoor allows communication with any pump
- No prior knowledge of serial required
- Can communicate up to 300 feet away
- All models that support wireless are vulnerable
- Currently no method of updating firmware

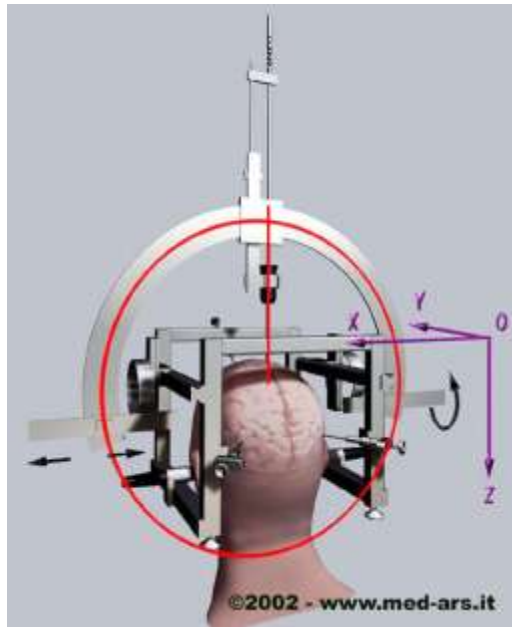


# Implantable Cardiac Defibrillators

- In 2008, three Universities came together to RE 2003 IMD's – they were able to:
  - Extract private data
  - Reprogram the therapy settings
  - Keep the device “awake” to run out the battery quicker
  - Disable the “shocking” mechanism to regulate beat
  - Introduce additional “shock” to produce fibrillation



# Deep Brain Stimulator



# RFID



# Unmanned Aerial Vehicles

- Domestic vs. International
- Univ. Texas at Austin
  - Unencrypted comms
  - Spoof GPS signals to guide and land



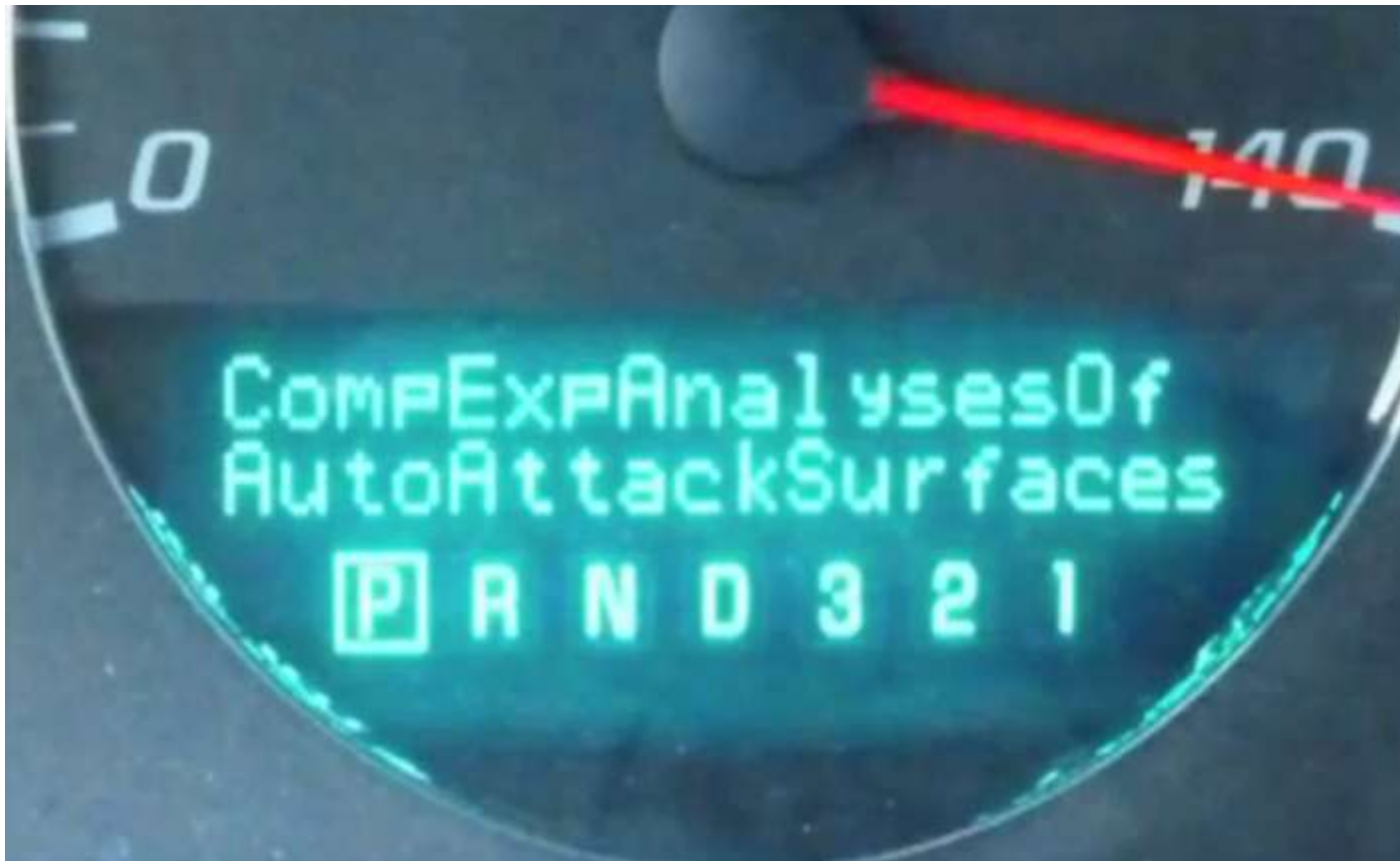


# Transportation

- Trains, Metro, Autos



# Automobiles



# ATMs

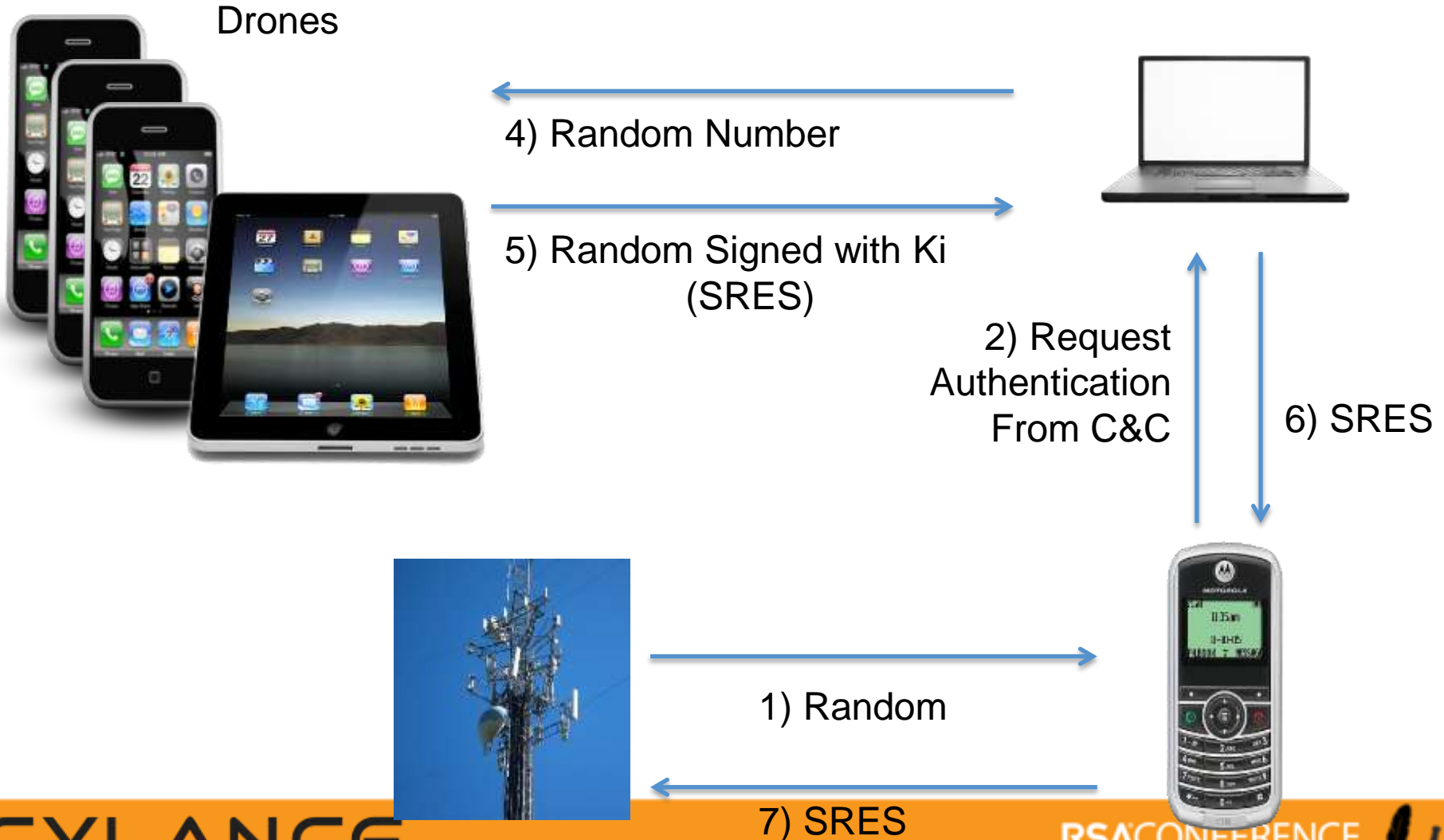


# Man-in-the-Phone (MiTP)

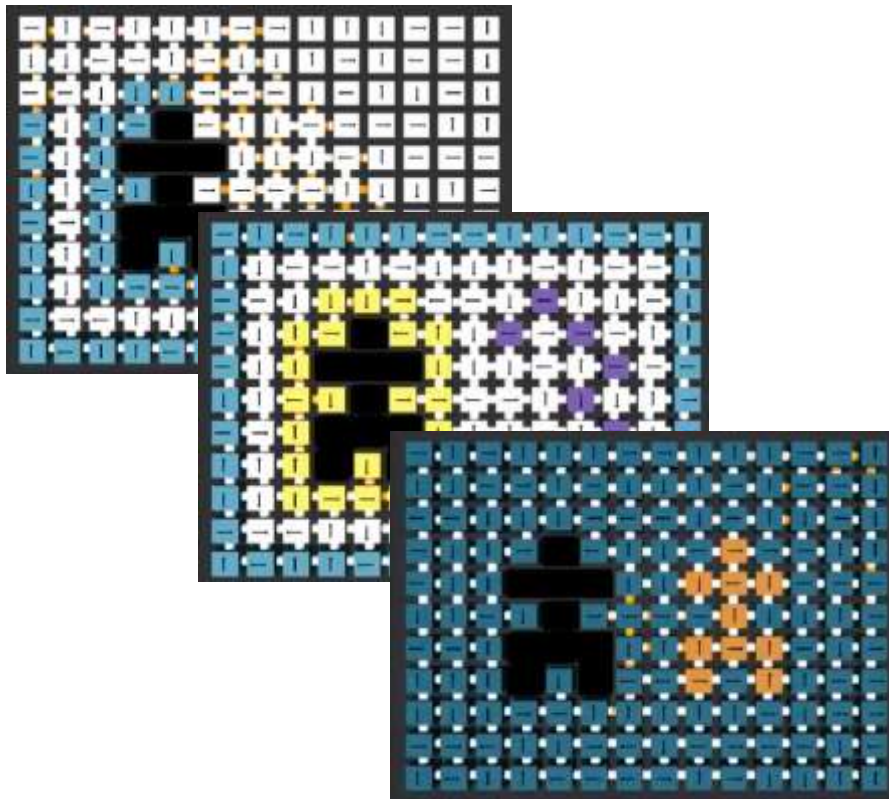
- 1) iPhone is rooted (baseband modem access exists at /dev/dlci.spi-baseband.\*)
- 2) Motorola C118 or other Calypso Digital Base Band Firmware is patched using modified OsmocomBB layer1.bin with SIMCARD proxy modifications
- 3) Connection chain is : Motorola <-> UART Serial <-> Linux PC <-> SSH Tunnel <-> iPhone <-> /dev/dlci.spi-basband <-> SIMCARD
- 4) Motorola performs GSM login and authentication process and sends the iPhone IMSI
- 5) Cell tower sends over RAND challenge, and looks up secret Ki in database for IMSI
- 6) Motorola asks iPhone to perform signing of RAND
- 7) Motorola sends back Kc, SRES response to tower
- 8) Tower authenticates Motorola as iPhone



# GSM Authentication Spoofing



# Nanobots - MIT's Smart Sand



# “Digital Pearl Harbor”





**Silliman Science Laboratory Building**  
Mt. Hermon, MA  
*Sat. Nov. 20, 1965*





# Legoland anyone?



# THANK YOU

