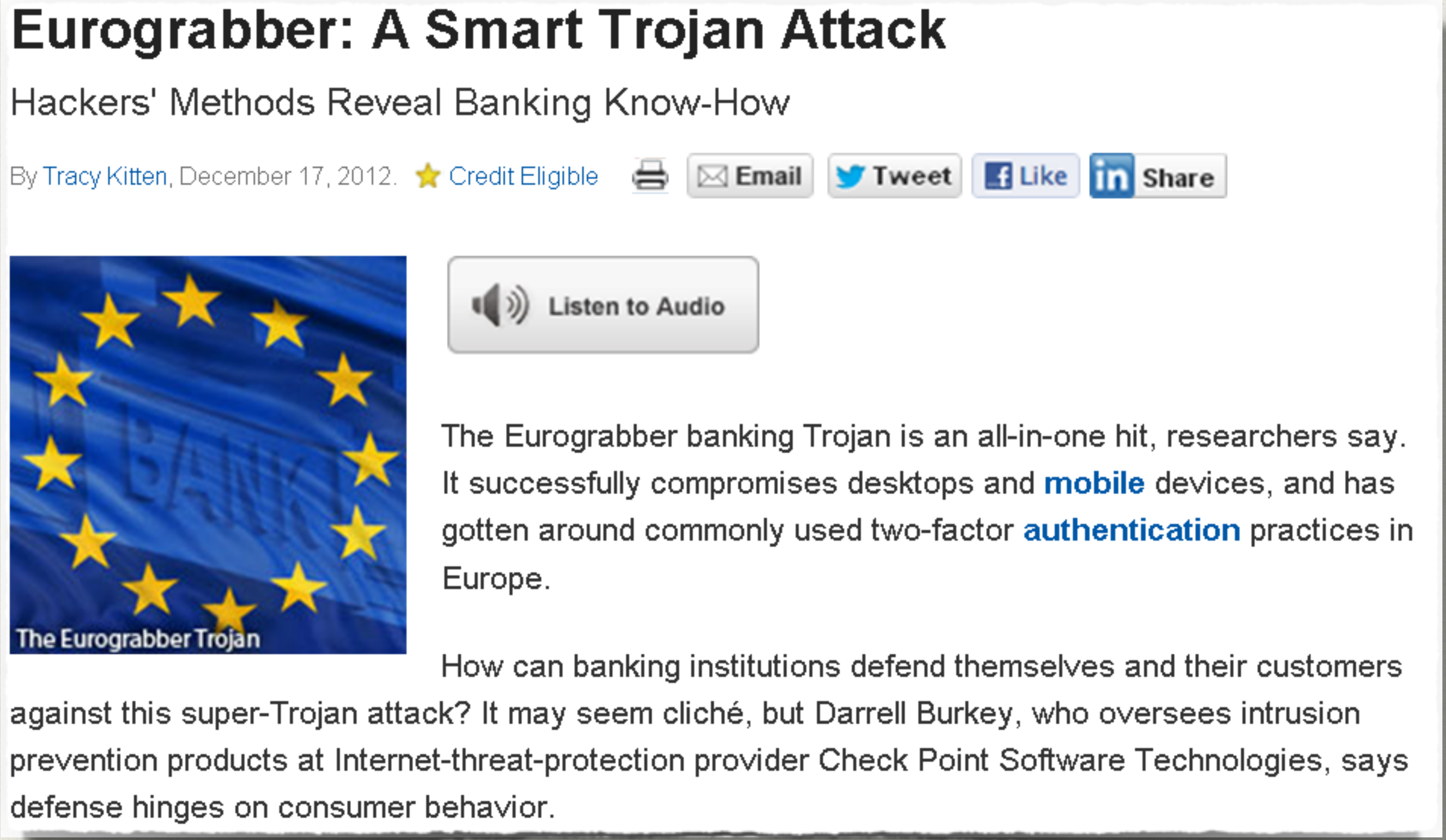
X-PLATFORM APT

Tomáš Rosa
Raiffeisenbank a.s.

X-PLATFORM ATTACK

Any fraudulent activity that exploits vulnerabilities across different computing platforms.

TRUE LIES



Eurograbber: A Smart Trojan Attack

Hackers' Methods Reveal Banking Know-How

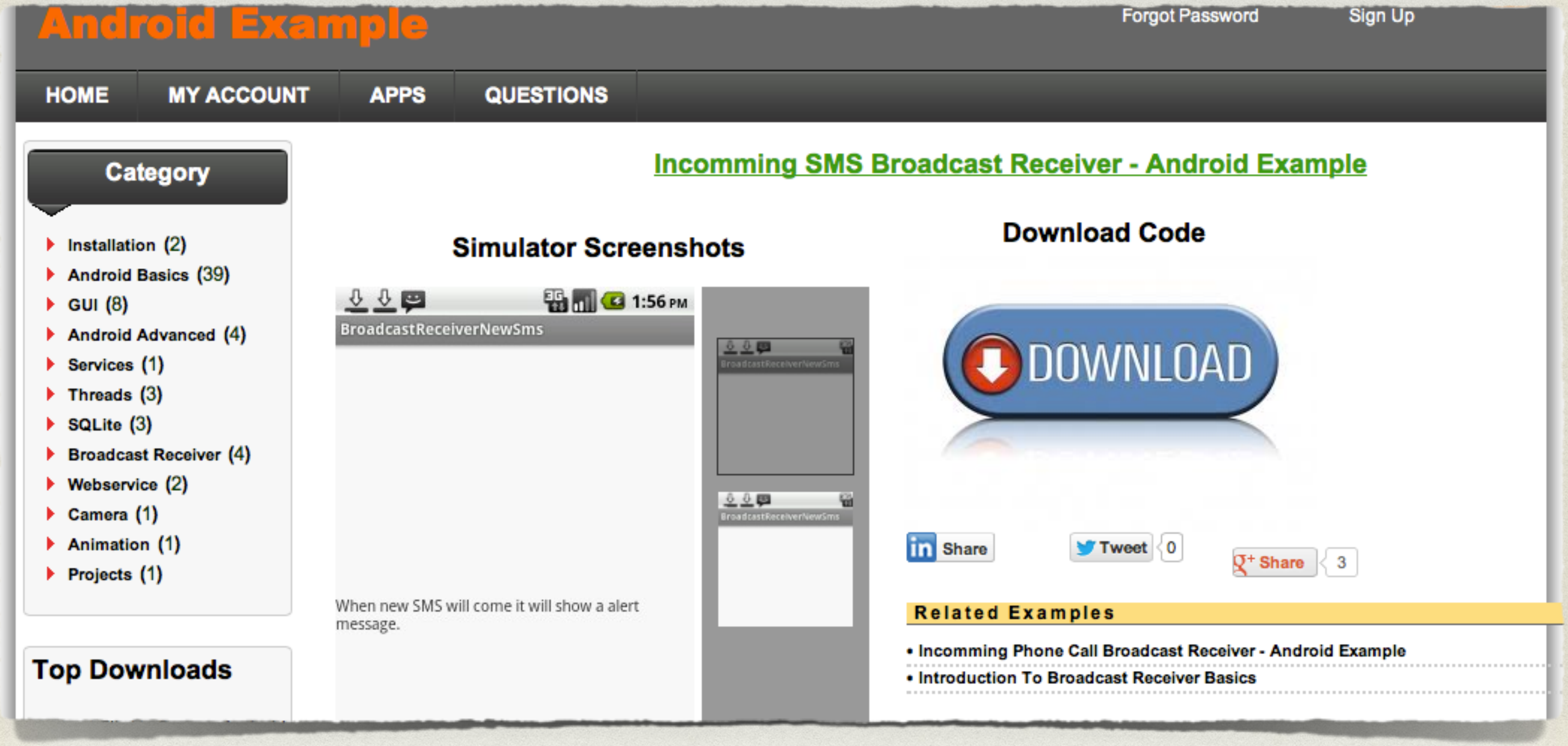
By Tracy Kitten, December 17, 2012. ★ Credit Eligible

The Eurograbber banking Trojan is an all-in-one hit, researchers say. It successfully compromises desktops and **mobile** devices, and has gotten around commonly used two-factor **authentication** practices in Europe.

How can banking institutions defend themselves and their customers against this super-Trojan attack? It may seem cliché, but Darrell Burkey, who oversees intrusion prevention products at Internet-threat-protection provider Check Point Software Technologies, says defense hinges on consumer behavior.

http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

LET'S FACE IT



Incomming SMS Broadcast Receiver - Android Example

- Installation (2)
- Android Basics (39)
- GUI (8)
- Android Advanced (4)
- Services (1)
- Threads (3)
- SQLite (3)
- Broadcast Receiver (4)
- Webservice (2)
- Camera (1)
- Animation (1)
- Projects (1)

Top Downloads

Simulator Screenshots

BroadcastReceiverNewSms

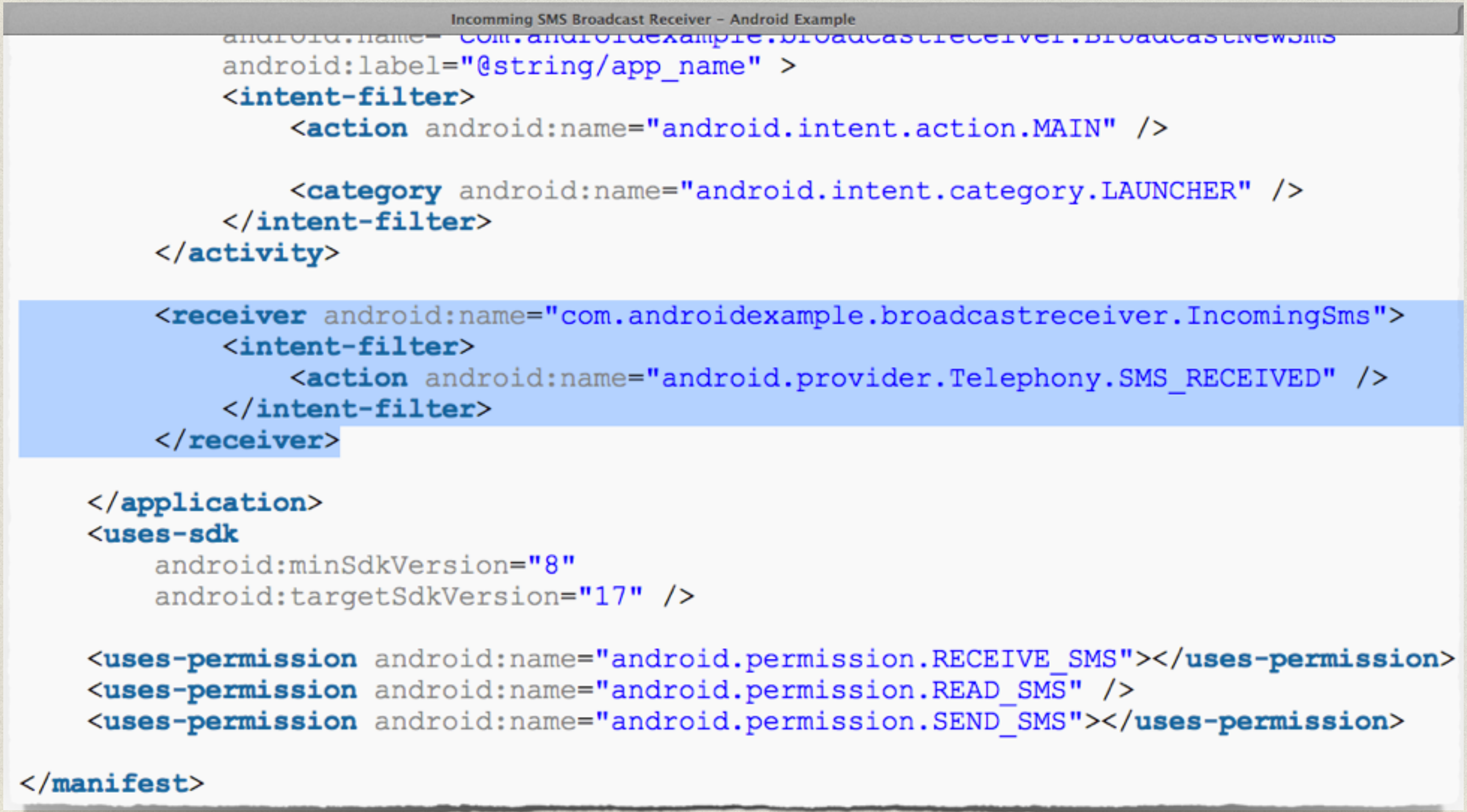
When new SMS will come it will show a alert message.

Download Code

Related Examples

- Incomming Phone Call Broadcast Receiver - Android Example
- Introduction To Broadcast Receiver Basics

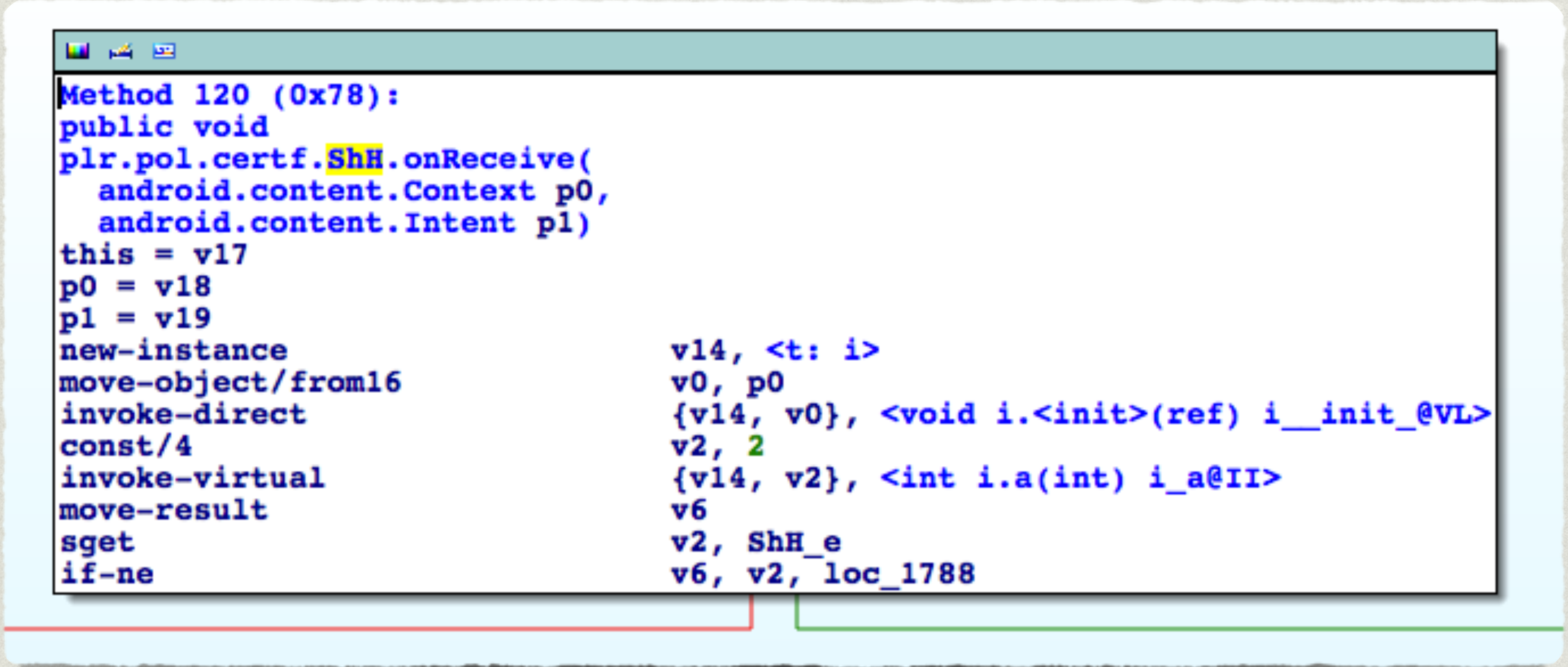
SLEEPING WITH THE ENEMY



Incomming SMS Broadcast Receiver – Android Example

```
            android:name="com.androidexample.broadcastreceiver.BroadcastNewSms"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

        <receiver android:name="com.androidexample.broadcastreceiver.IncomingSms">
            <intent-filter>
                <action android:name="android.provider.Telephony.SMS_RECEIVED" />
            </intent-filter>
        </receiver>

    </application>
    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />

    <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-permission>
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.SEND_SMS"></uses-permission>

</manifest>
```

SMS TRAP



```
Method 120 (0x78):
public void
plr.pol.certf.ShH.onReceive(
  android.content.Context p0,
  android.content.Intent p1)
this = v17
p0 = v18
p1 = v19
new-instance                    v14, <t: i>
move-object/from16              v0, p0
invoke-direct                   {v14, v0}, <void i.<init>(ref) i__init_@VL>
const/4                         v2, 2
invoke-virtual                  {v14, v2}, <int i.a(int) i_a@II>
move-result                     v6
sget                            v2, ShH_e
if-ne                           v6, v2, loc_1788
```

REAL X-PLATFORM STRIKE IN A NUTSHELL

It's here!!!

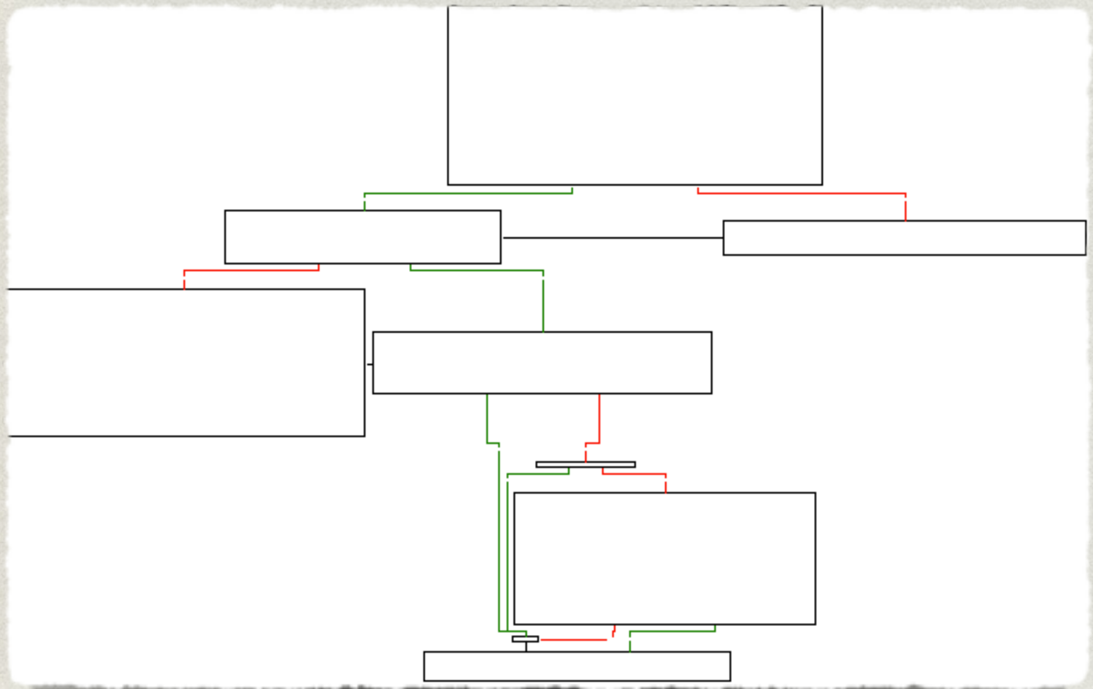
Experts Are Ready

CONSULTANTS EAGER TO HELP

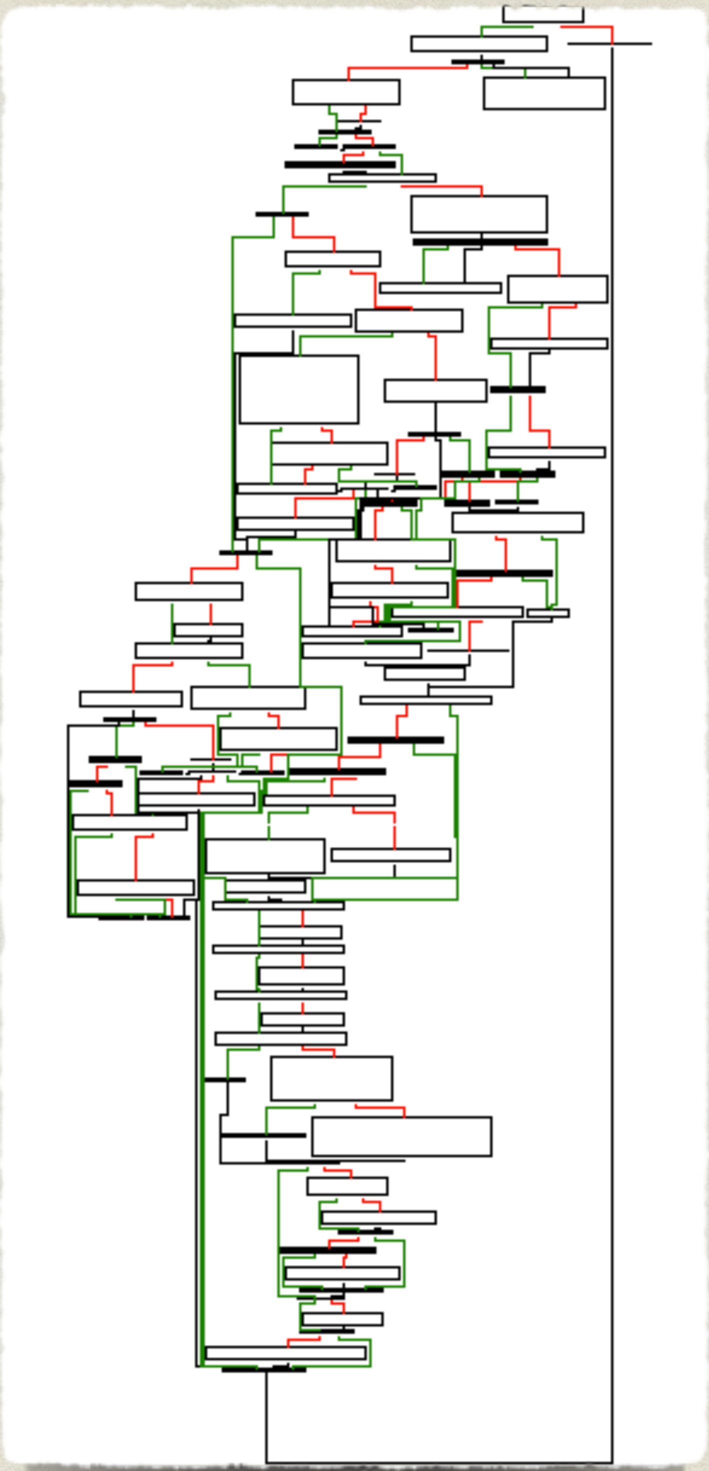
Clients Take It Seriously

CRIMINALS SHARPEN THEIR AXES

Evolution of the SMS broadcast receiver's "onReceive" method spotted in the wild

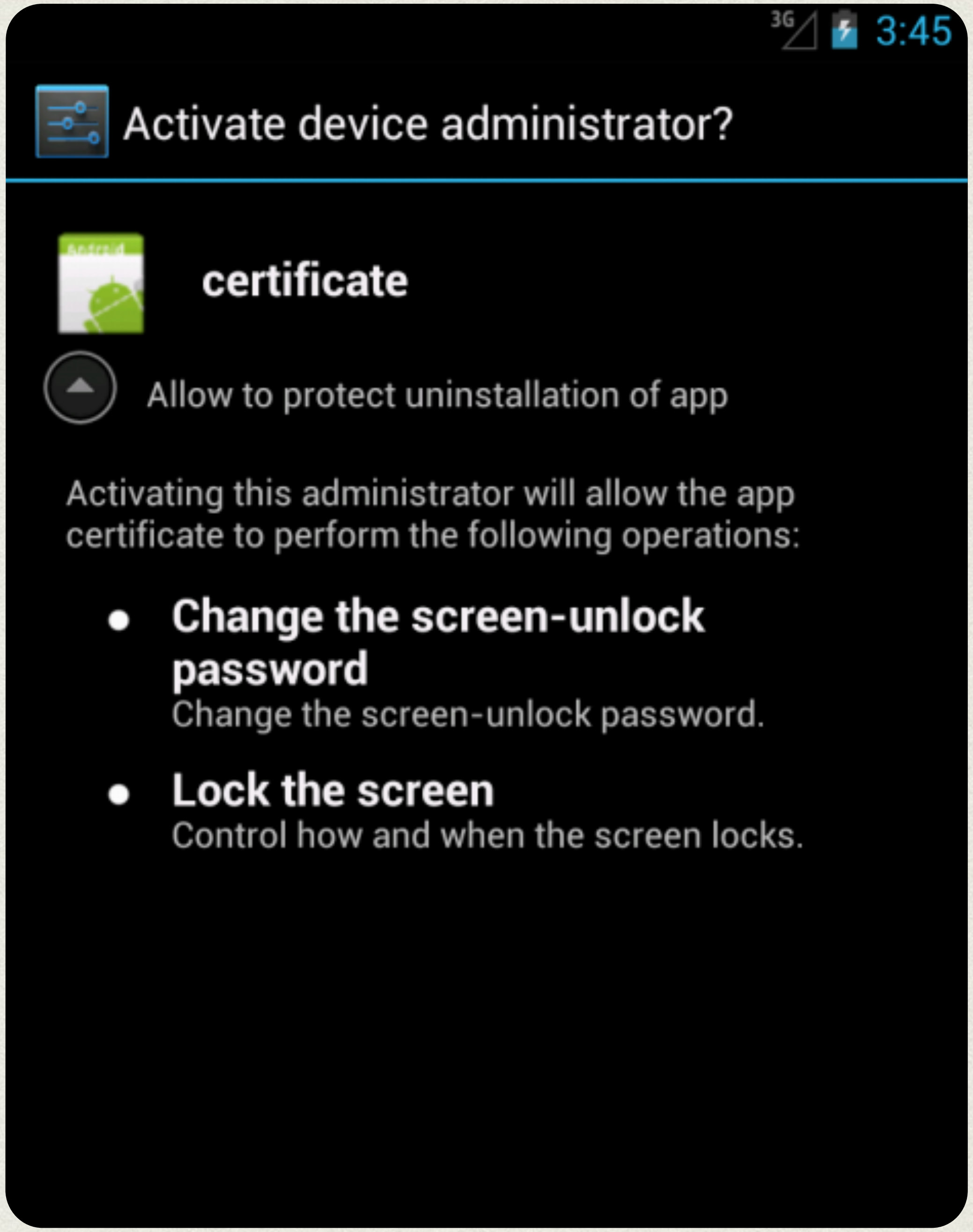


One Month



CHERRY ON THE CAKE

- This Trojan horse not only steals SMS
- It enforced the user to accept it as an Mobile Device Management plugin
- Note the permission to lock the screen with an arbitrary password...



Activate device administrator?

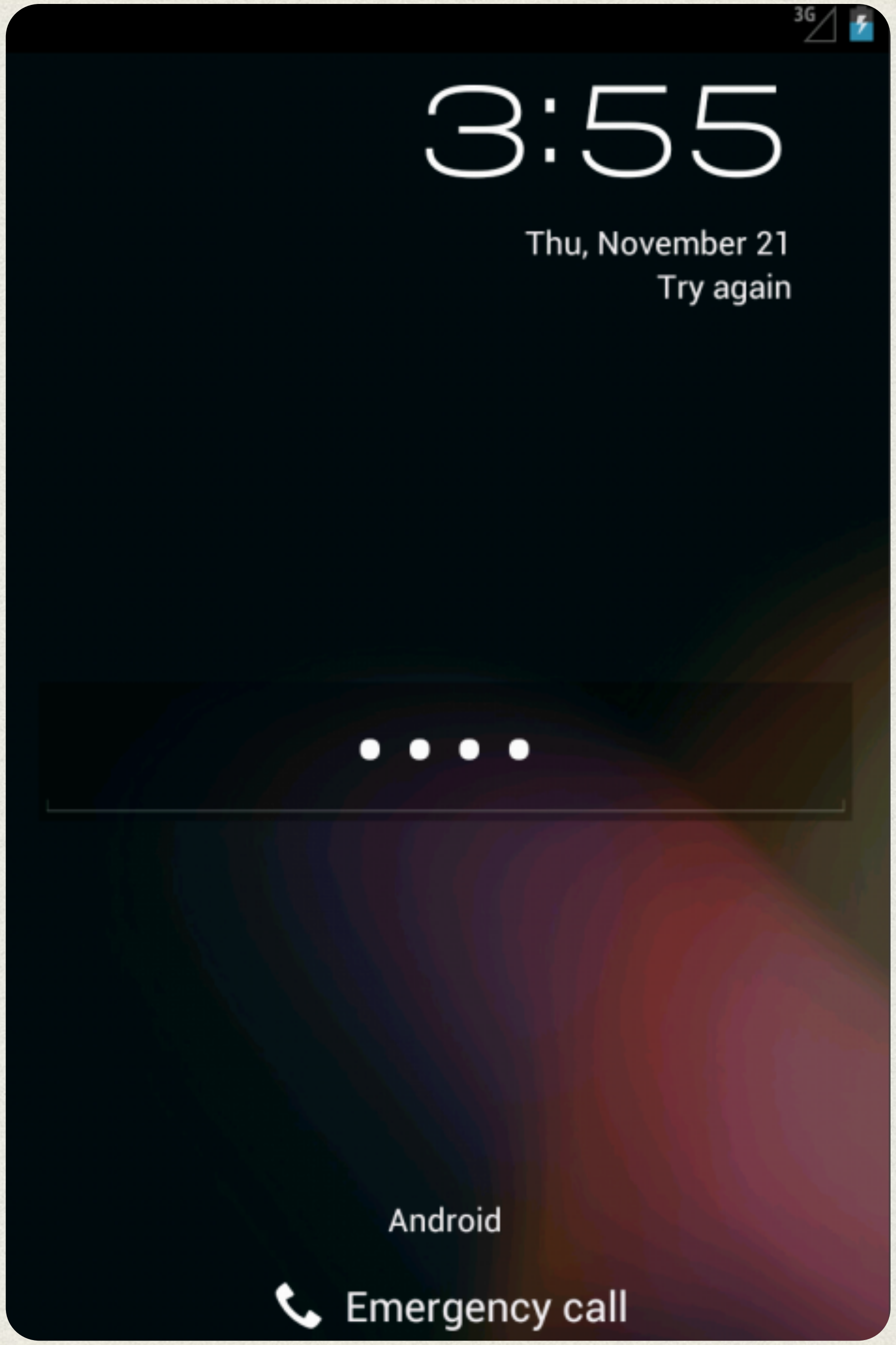
certificate

Allow to protect uninstallation of app

Activating this administrator will allow the app certificate to perform the following operations:

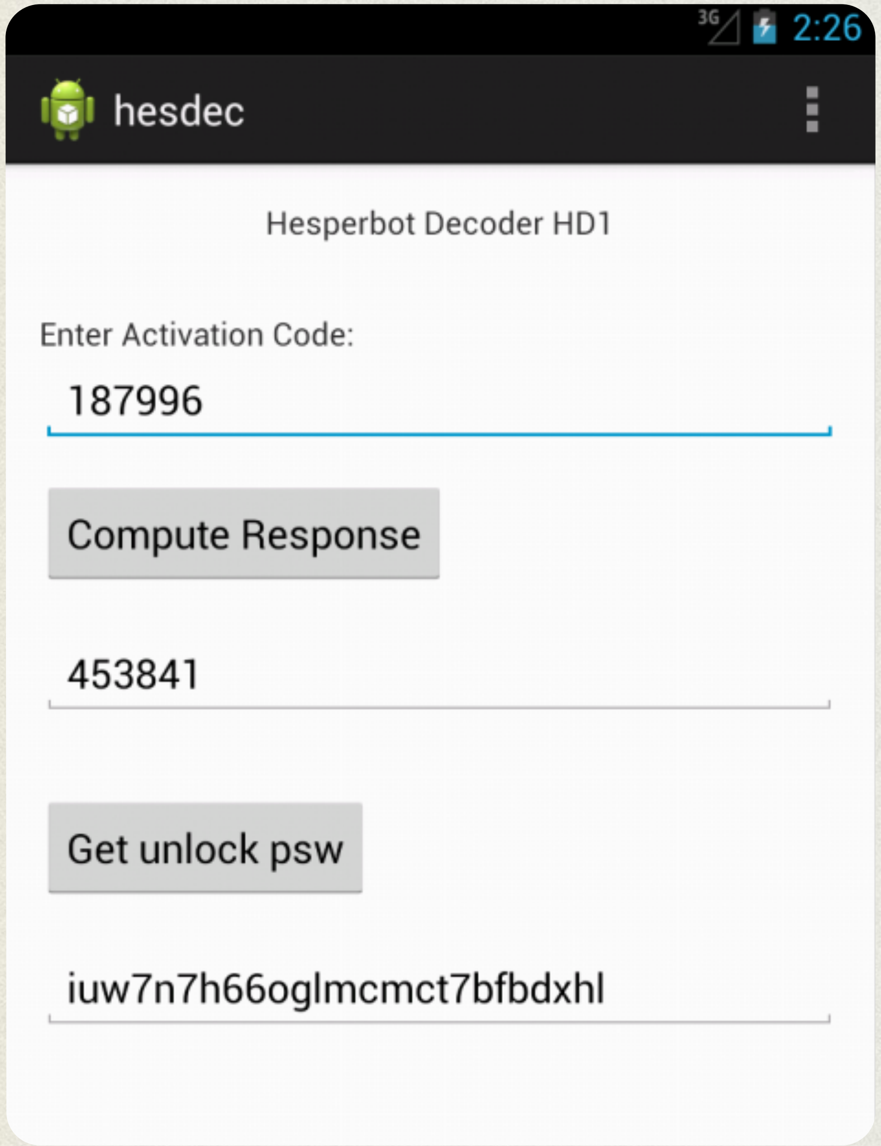
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Lock the screen**
  Control how and when the screen locks.

PUNISHED FOR AN UNINSTALL



- Later on, when the client tried to uninstall the Trojan, it locked the screen with a cryptographically generated password
- The malware author, however, was still able to generate the unlock code
- We see a kind of ransomware extension

RANSOMWARE REVERSED



Hesperbot Decoder HD1

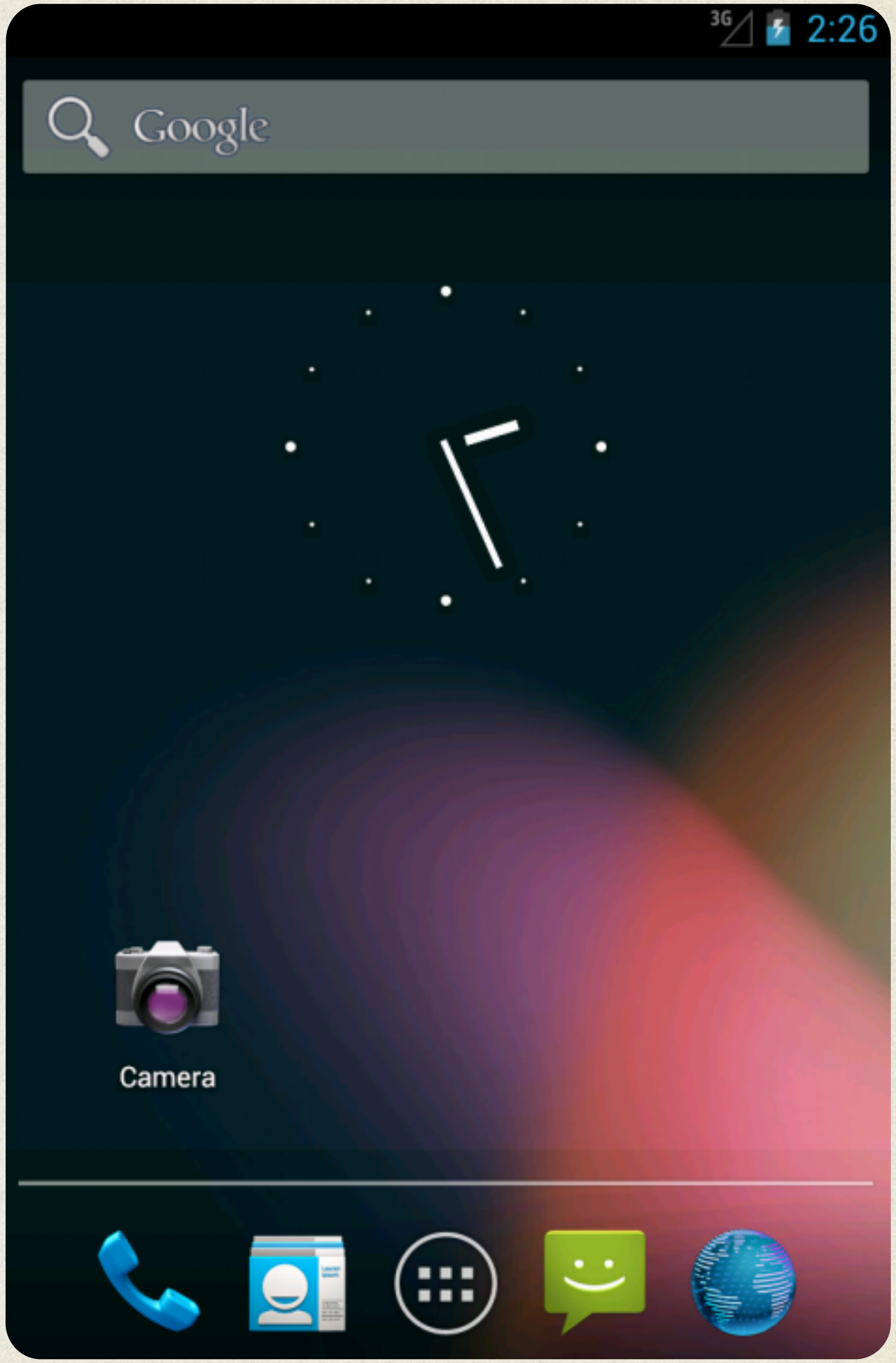
Enter Activation Code:

187996

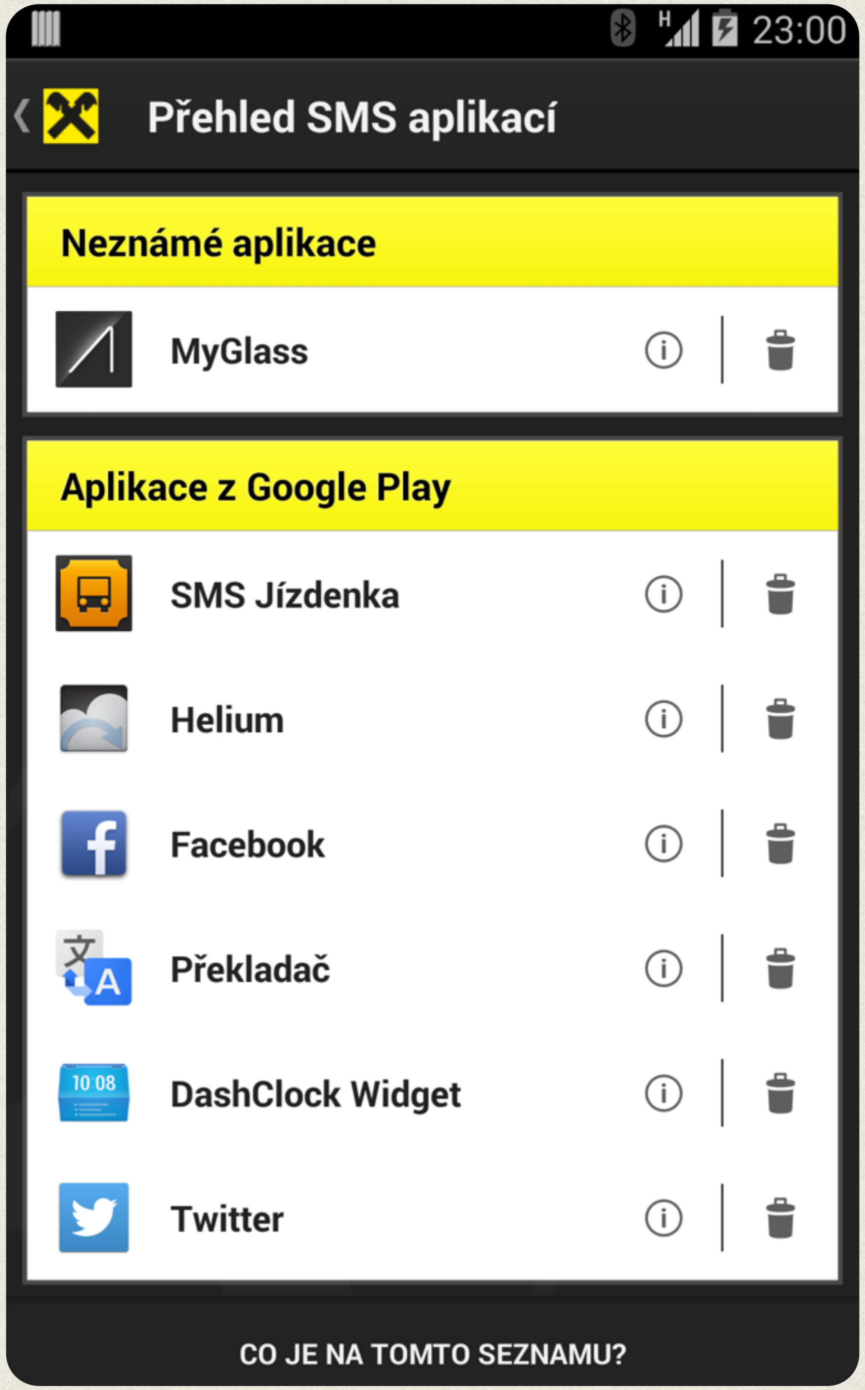
453841

iuw7n7h66oglmcmct7bfbdxhl

Voilà...



SYNERGY: S.A.S. EXTENSION



23:00

Přehled SMS aplikací

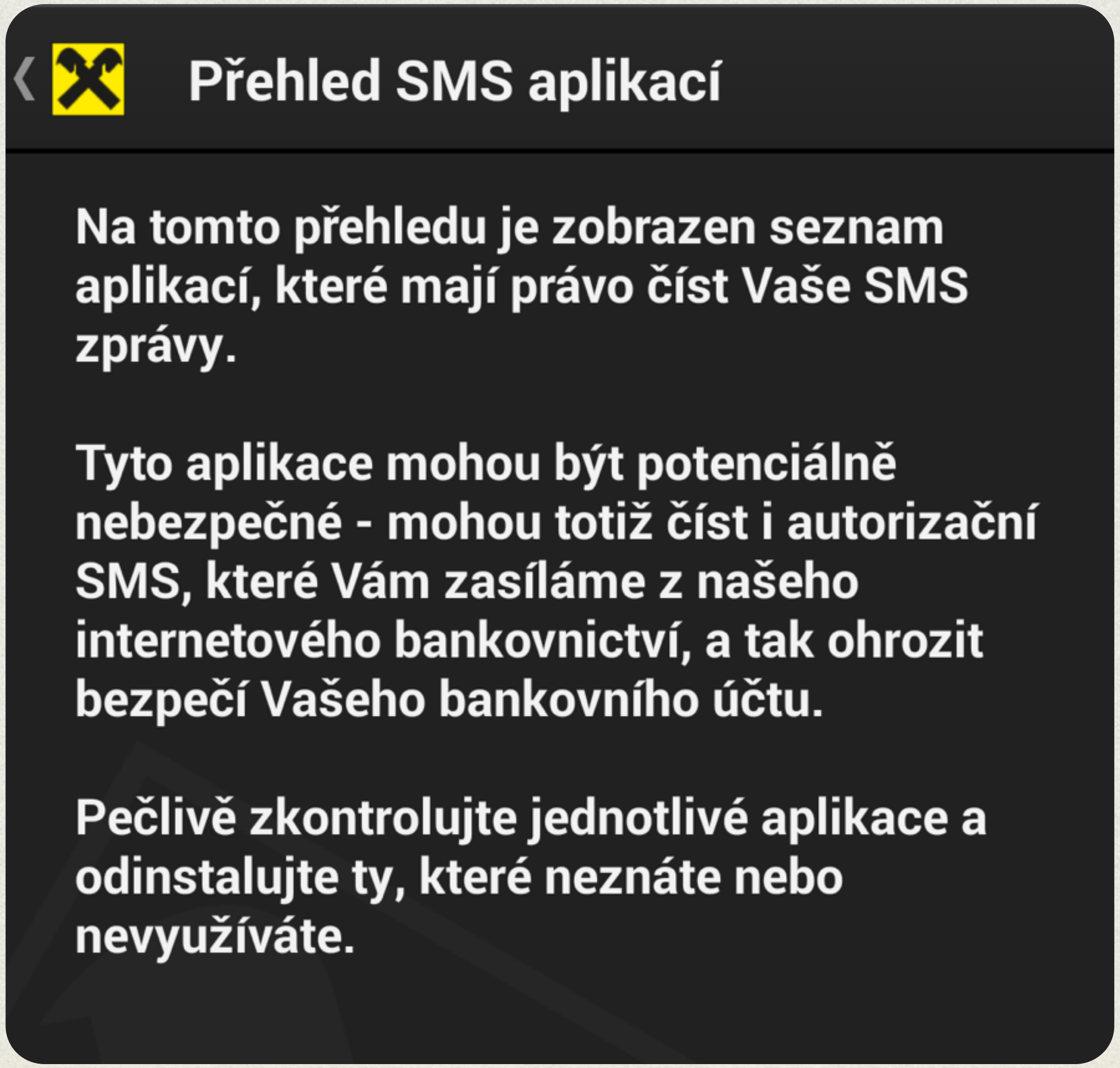
Neznámé aplikace

- MyGlass

Aplikace z Google Play

- SMS Jízdenka
- Helium
- Facebook
- Překladač
- DashClock Widget
- Twitter

CO JE NA TOMTO SEZNAMU?



Přehled SMS aplikací

Na tomto přehledu je zobrazen seznam aplikací, které mají právo číst Vaše SMS zprávy.

Tyto aplikace mohou být potenciálně nebezpečné - mohou totiž číst i autorizační SMS, které Vám zasíláme z našeho internetového bankovnictví, a tak ohrozit bezpečí Vašeho bankovního účtu.

Pečlivě zkontrolujte jednotlivé aplikace a odinstalujte ty, které neznáte nebo nevyužíváte.

X-PLATFORM EVOLUTION

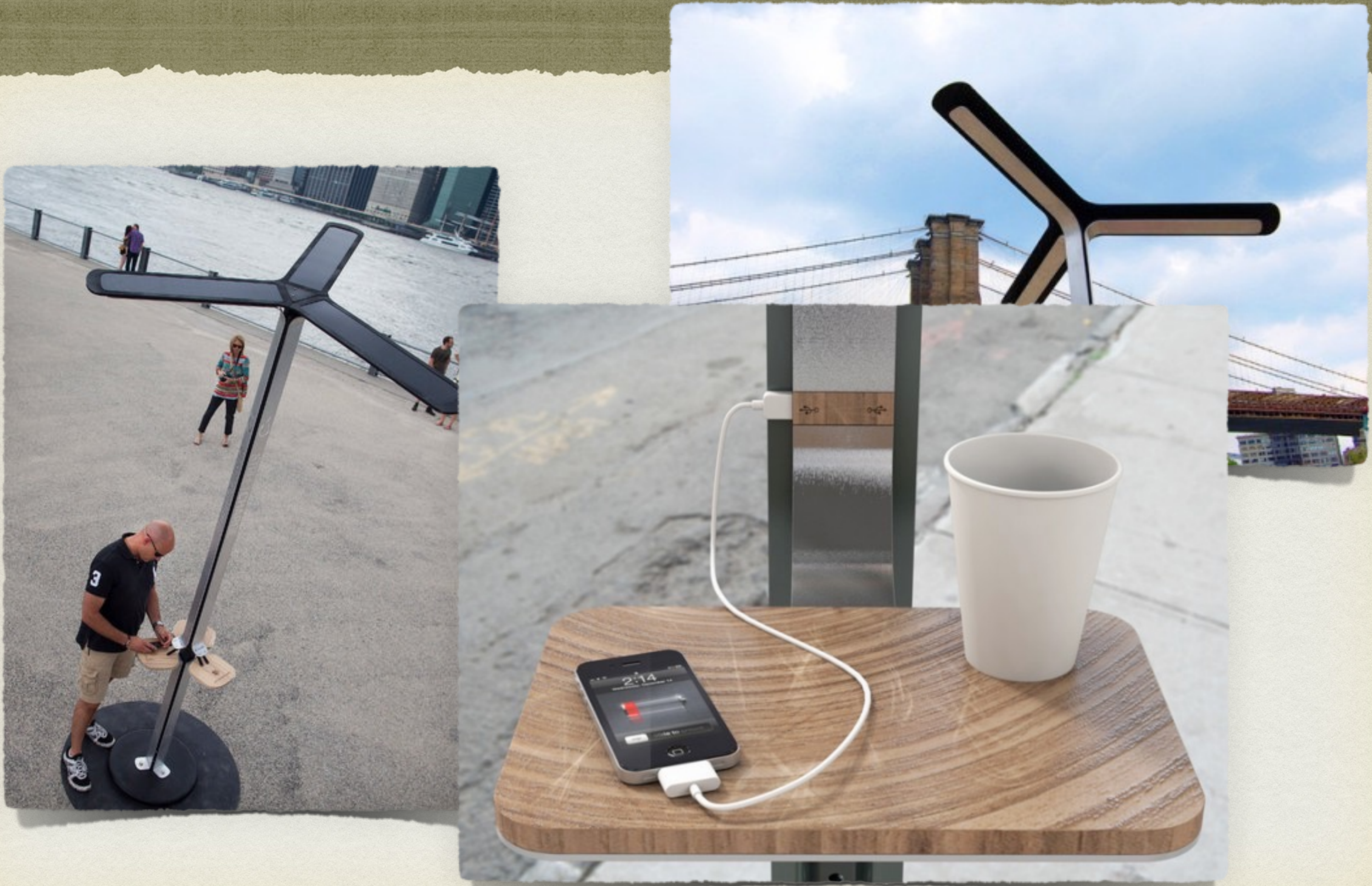
NO CLIENT COOPERATION REQUIRED

- Contrary to the pioneering approaches used by ZitMo, Spitmo, TinBa, and the Eurograbber scenario…
  - … the cross-platform infections reflected hereafter run smoothly with no points of particular cooperation with the client
  - we can think about generation-2 attacks

USB LINK
CROSS-PLATFORM INFECTION

- Exploits USB protocol stack vulnerabilities for infection spreading in both ways (CPI computer ↔ mobile)
  - [Stavrou and Wang at BlackHat DC 2011], [Lau, Jang, and Song at BlackHat US 2013]
- The original proof-of-concept can be further extended

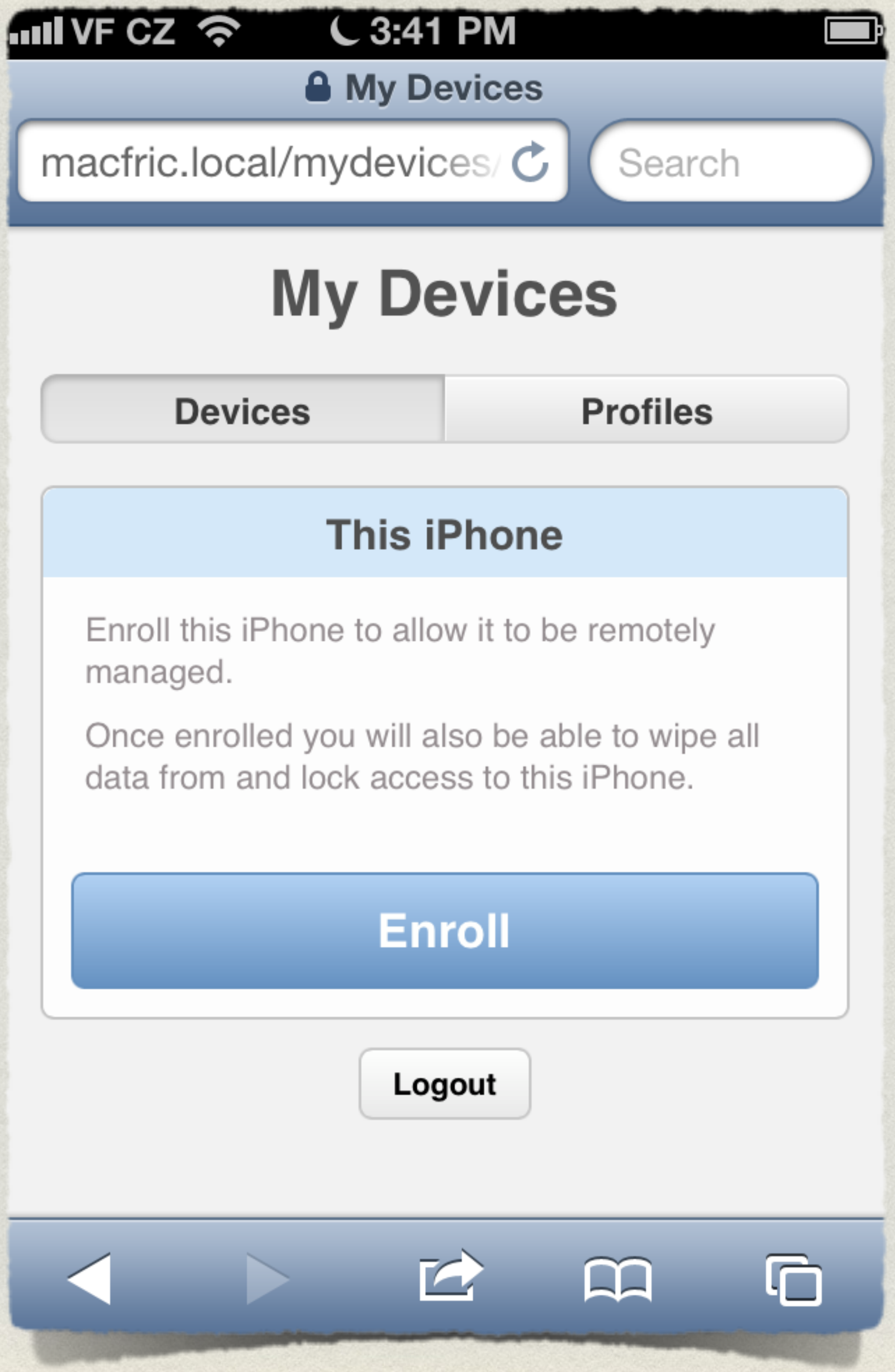
NY: SOLAR MALWARE



SHOW GOES ON...

- Gmail link X-platform infection
  - exploits Android services convergence at Google Play
  - [Rosa in 2011 - 2012]
    - http://crypto.hyperlink.cz/files/rosa_scforum12_v1.pdf
- Wi-Fi link X-platform infection
  - exploits implicit trust of WLAN devices
  - [Dmitrienko et al. at BlackHat AD 2012]

BRING YOUR OWN DEVICE



My Devices

This iPhone

Enroll this iPhone to allow it to be remotely managed.

Once enrolled you will also be able to wipe all data from and lock access to this iPhone.

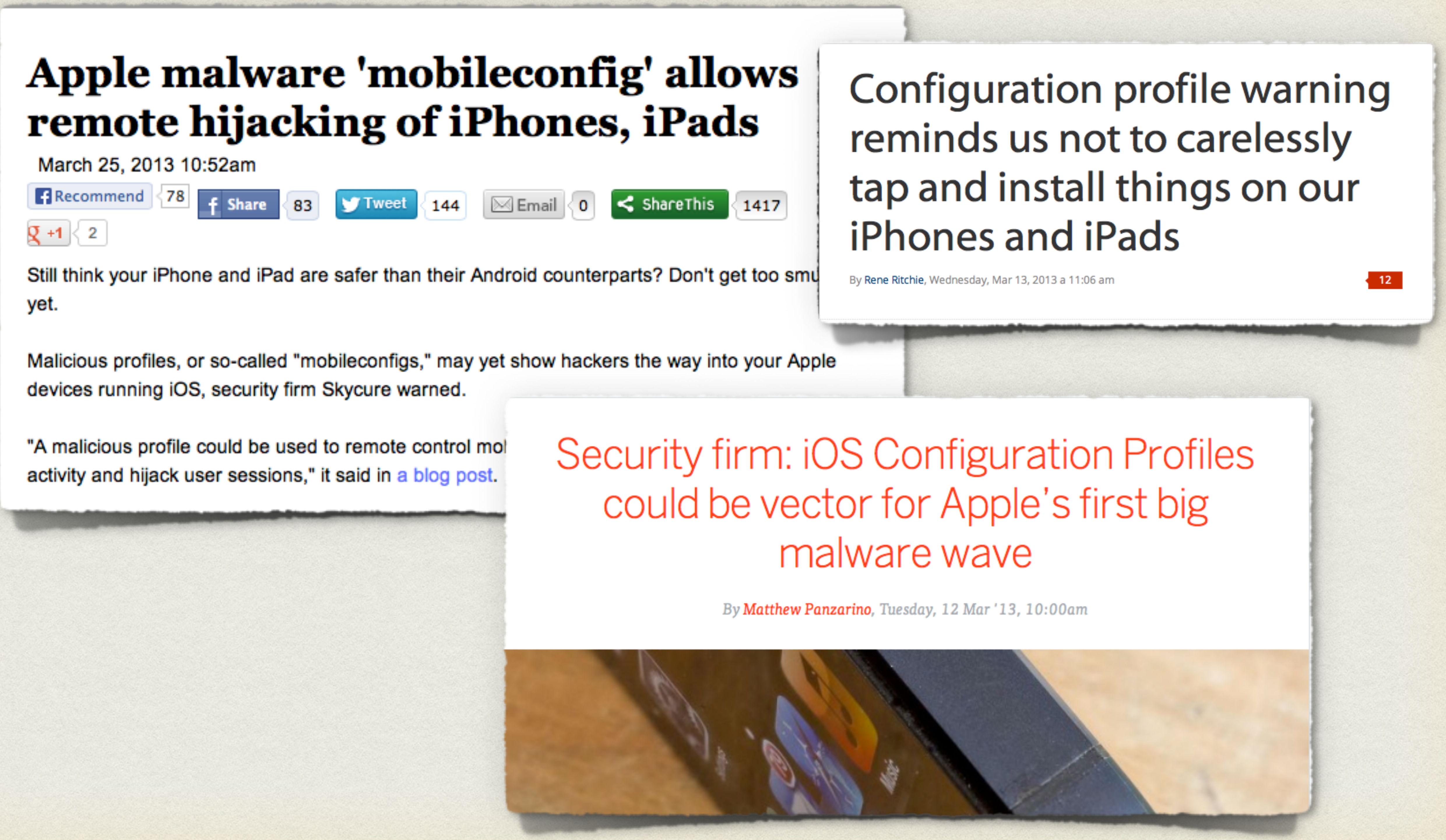
ON THE OTHER HAND
~~BRING~~ *BREAK* YOUR OWN DEVICE

- Since: "*By agreeing to the profile installation, the user’s device is automatically enrolled without further interaction.*“

-- http://images.apple.com/iphone/business/docs/iOS_6_MDM_Sep12.pdf

- Zdziarski in "*Hacking and Securing iOS Applications*", 2012
- Schuetz at BH US 2011 and Shmoocon 2012
- Sharabani at Herzliya 2013
- Medin at Shmoocon 2013

HACKERS ARE READY…



Apple malware 'mobileconfig' allows remote hijacking of iPhones, iPads

March 25, 2013 10:52am

Still think your iPhone and iPad are safer than their Android counterparts? Don't get too smu
yet.

Malicious profiles, or so-called "mobileconfigs," may yet show hackers the way into your Apple devices running iOS, security firm Skycure warned.

"A malicious profile could be used to remote control mo
activity and hijack user sessions," it said in a blog post.

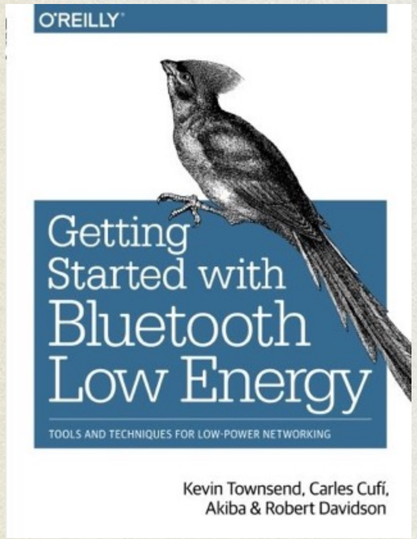
Configuration profile warning reminds us not to carelessly tap and install things on our iPhones and iPads

By Rene Ritchie, Wednesday, Mar 13, 2013 a 11:06 am

Security firm: iOS Configuration Profiles could be vector for Apple's first big malware wave

By Matthew Panzarino, Tuesday, 12 Mar '13, 10:00am

BLE ESSENTIALS



O'REILLY

Getting Started with Bluetooth Low Energy

TOOLS AND TECHNIQUES FOR LOW-POWER NETWORKING

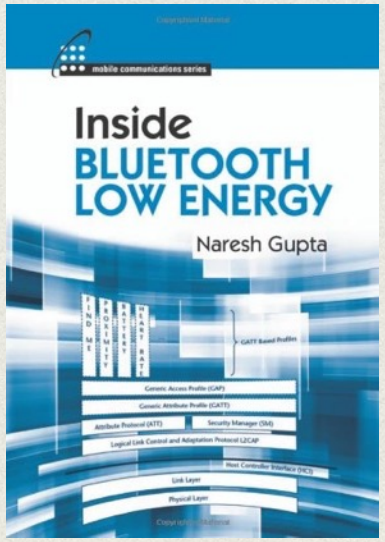
Kevin Townsend, Carles Cufí, Akiba & Robert Davidson

PRENTICE HALL

BLUETOOTH LOW ENERGY

THE DEVELOPER'S HANDBOOK

ROBIN HEYDON

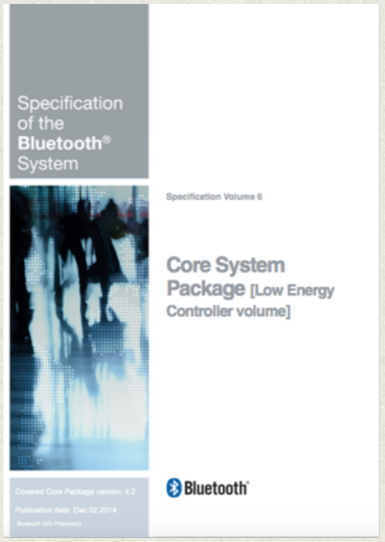


mobile communications series

Inside BLUETOOTH LOW ENERGY

Naresh Gupta

FIND ME
PROXIMITY
BATTERY
HEART RATE
GATT Based Profiles
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Attribute Protocol (ATT)
Security Manager (SM)
Logical Link Control and Adaptation Protocol L2CAP
Host Controller Interface (HCI)
Link Layer
Physical Layer



Specification of the Bluetooth® System

Specification Volume 6

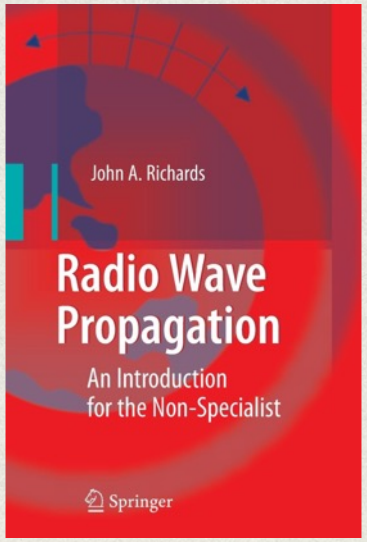
Core System Package [Low Energy Controller volume]

Covered Core Package version: 4.2

Publication date: Dec 02 2014

Bluetooth SIG Proprietary

Bluetooth

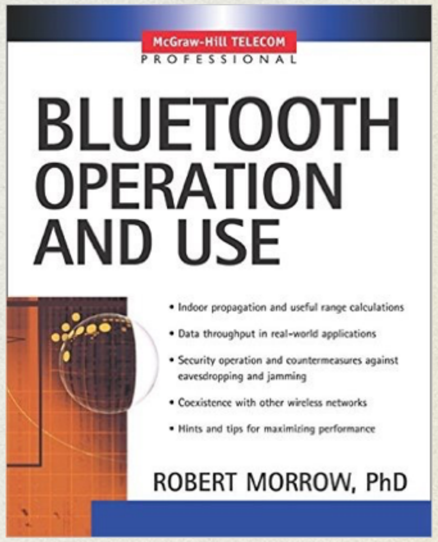


John A. Richards

Radio Wave Propagation

An Introduction for the Non-Specialist

Springer



McGraw-Hill TELECOM PROFESSIONAL

BLUETOOTH OPERATION AND USE

- Indoor propagation and useful range calculations
- Data throughput in real-world applications
- Security operation and countermeasures against eavesdropping and jamming
- Coexistence with other wireless networks
- Hints and tips for maximizing performance

ROBERT MORROW, PhD

ALL THOSE BLUE TEETH

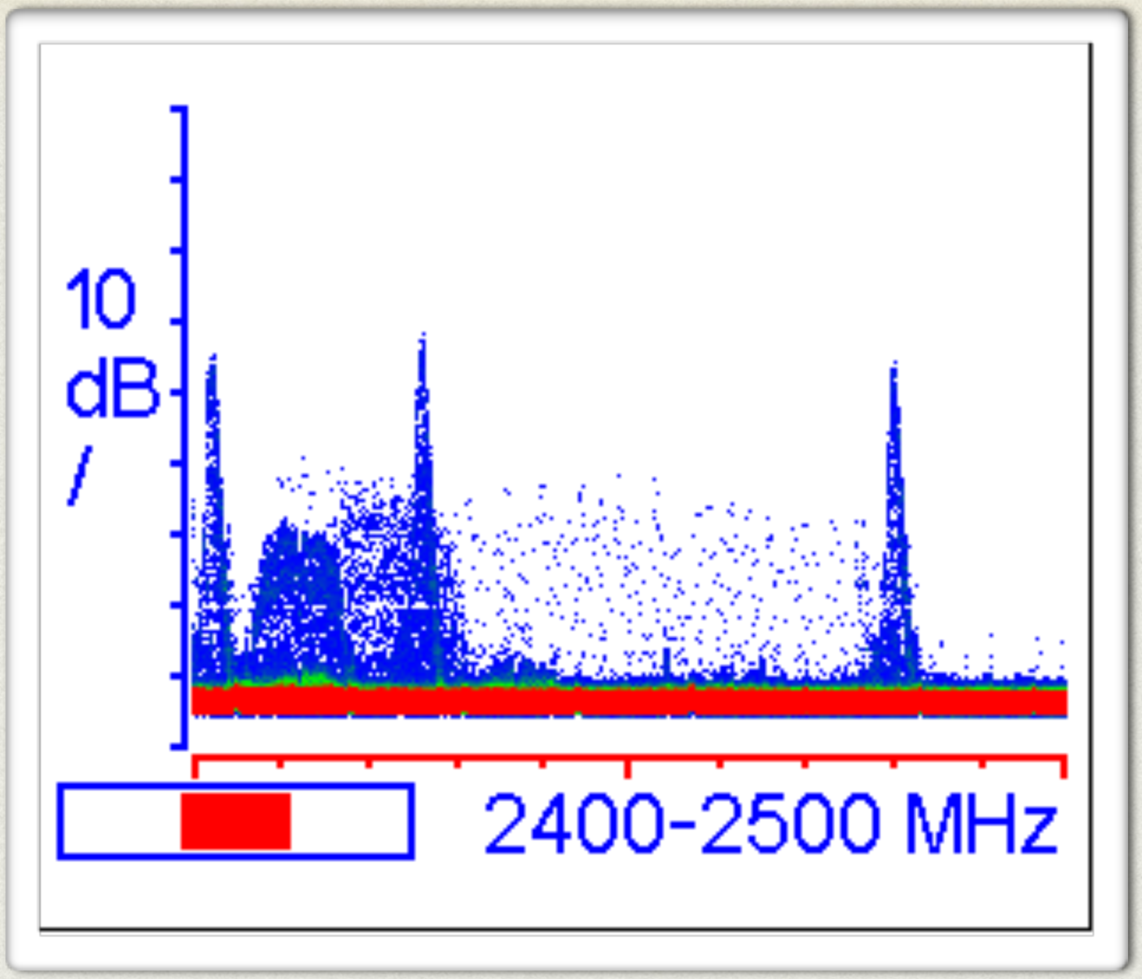
- Bluetooth **Basic Rate** (1 Mbps)
  - –core spec. 1.x, 1999-2003
- Bluetooth **Enhanced Data Rate** (2 or 3 Mbps)
  - –core spec. 2.x, 2004-2007
  - –taken together, BT BR/EDR is more or less a “serial link over the radio”

Bluetooth Classic

- Bluetooth **High Speed** (54 Mbps with 802.11)
  - –also called AMP ~ *Alternate MAC/PHY*
  - –core spec. 3.x, 2009
- Bluetooth **Low Energy**, a.k.a. Bluetooth Smart (1 Mbps, bulk-mode only)
  - –core spec. 4.x, 2010-2014

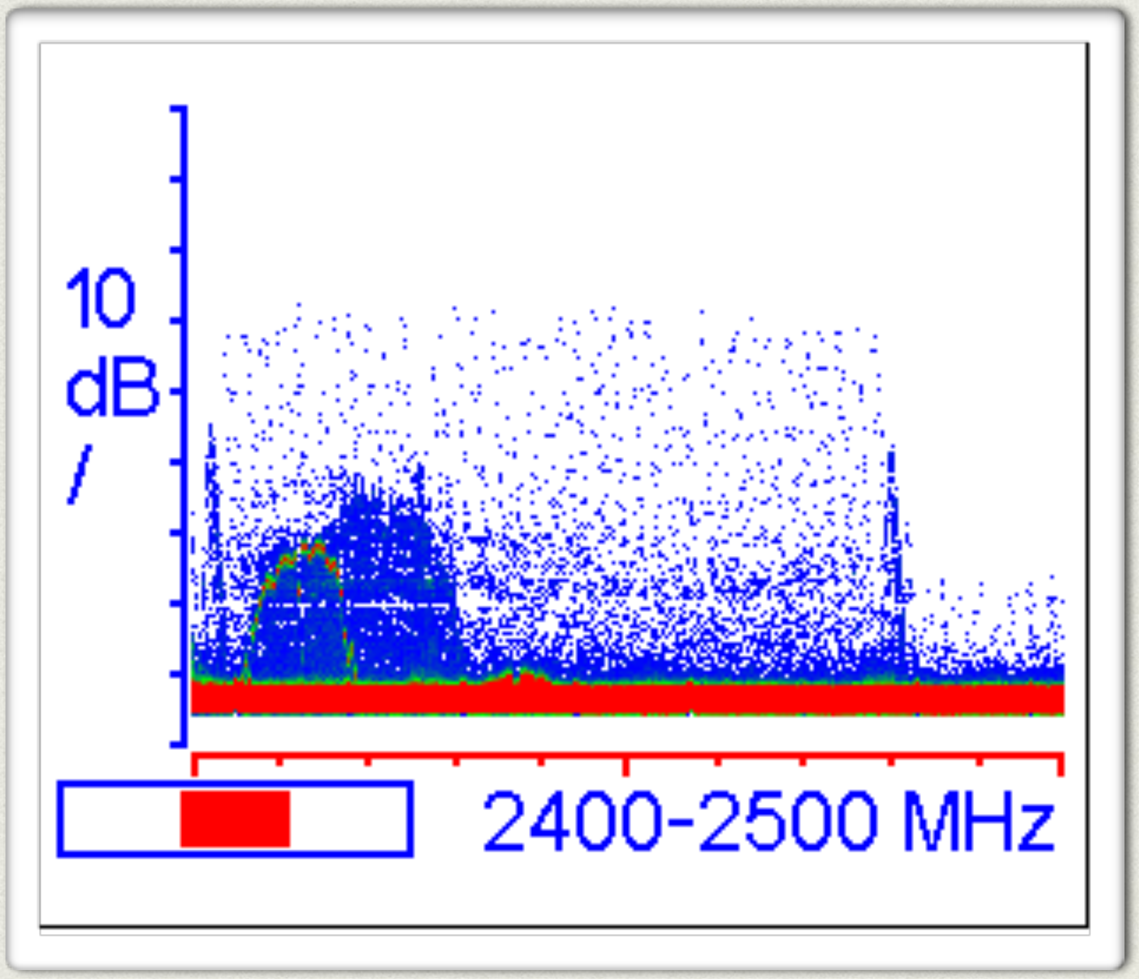
Bluetooth Smart

RF SPECTRUM

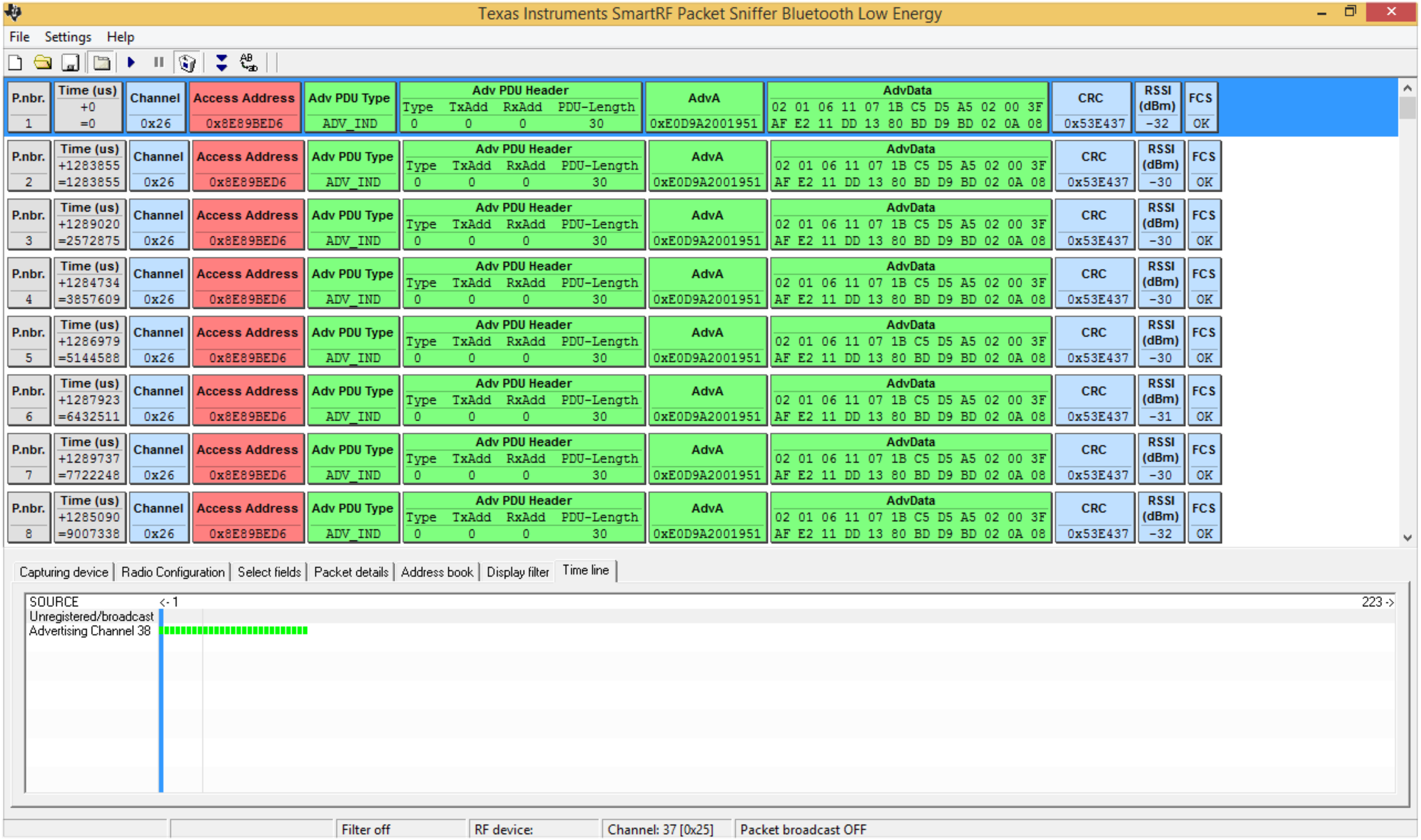


advertising

connection



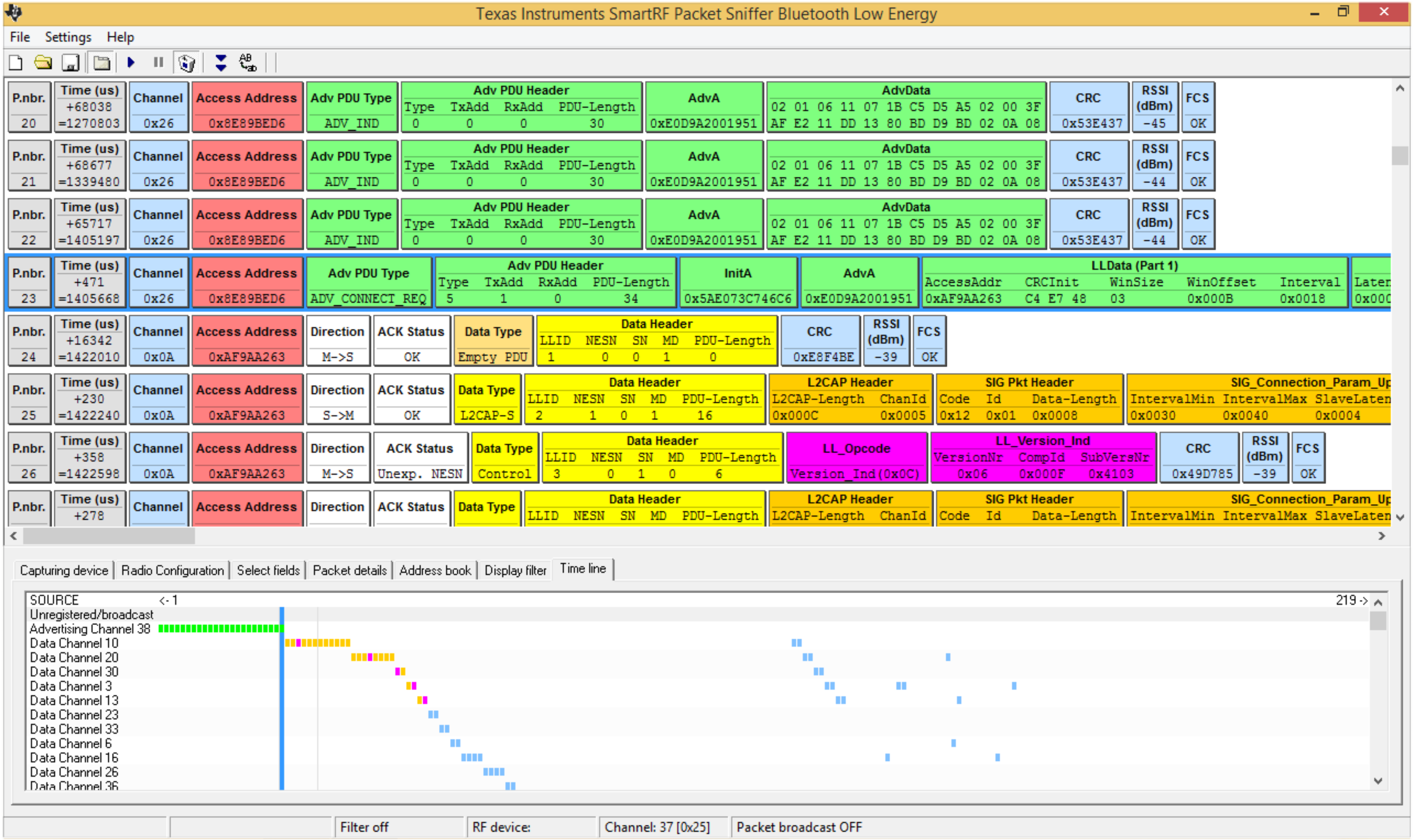
[Indicative wide-band RF scans by RigExpert IT-24 analyser for 2.4 GHz]



P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header Type	TxAdd	RxAdd	PDU-Length	AdvA	AdvData	CRC	RSSI (dBm)	FCS
1	+0 =0	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-32	OK
2	+1283855 =1283855	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-30	OK
3	+1289020 =2572875	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-30	OK
4	+1284734 =3857609	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-30	OK
5	+1286979 =5144588	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-30	OK
6	+1287923 =6432511	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-31	OK
7	+1289737 =7722248	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-30	OK
8	+1285090 =9007338	0x26	0x8E89BED6	ADV_IND	0	0	0	30	0xE0D9A2001951	02 01 06 11 07 1B C5 D5 A5 02 00 3F AF E2 11 DD 13 80 BD D9 BD 02 0A 08	0x53E437	-32	OK

Filter off | RF device: | Channel: 37 [0x25] | Packet broadcast OFF

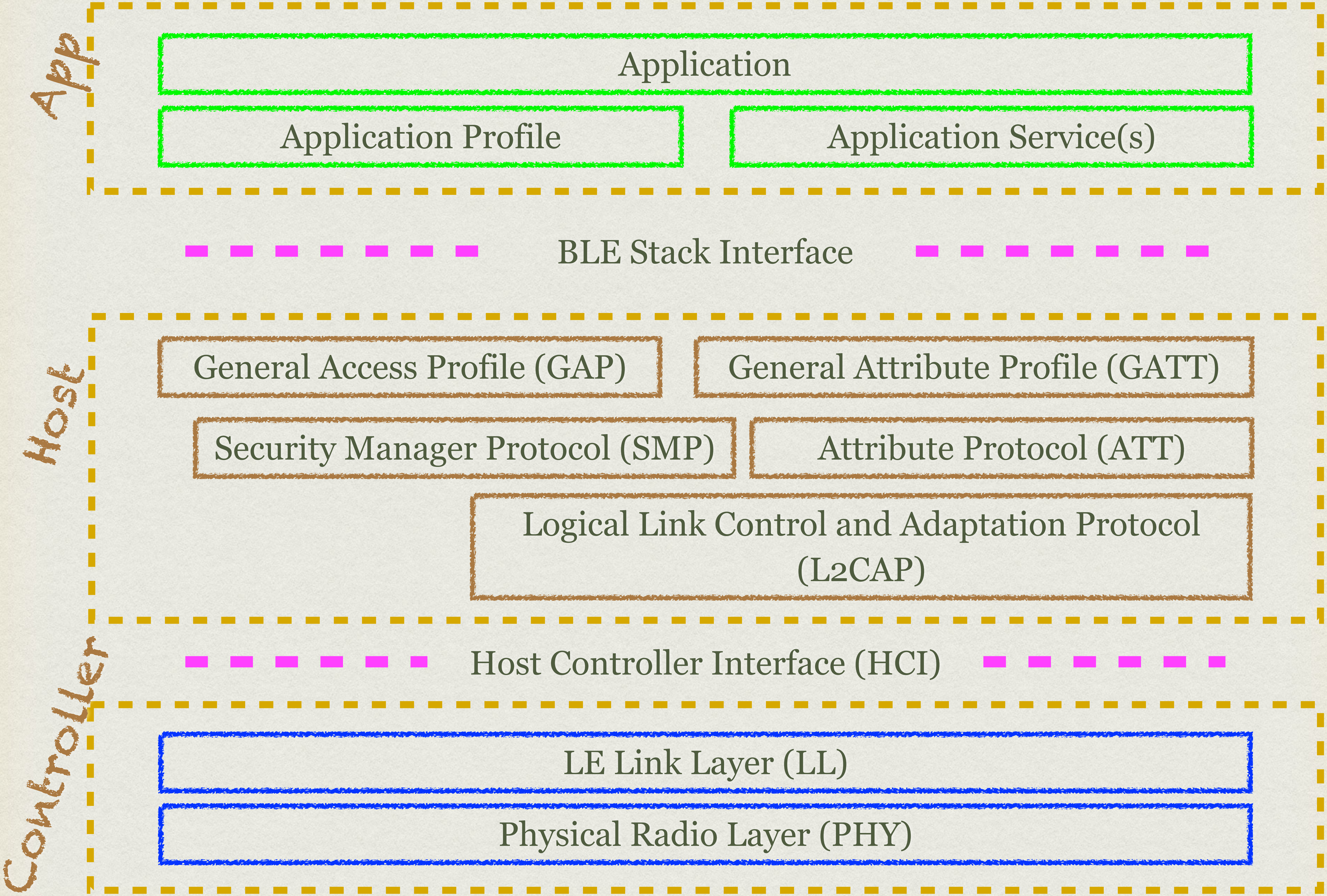
CC-2540-based BLE sniffer



```
P.nbr. | Time (us)  | Channel | Access Address | Adv PDU Type | Adv PDU Header                 | AdvA           | AdvData                              | CRC      | RSSI (dBm) | FCS
20     | +68038     | 0x26    | 0x8E89BED6     | ADV_IND      | Type TxAdd RxAdd PDU-Length    | 0xE0D9A2001951 | 02 01 06 11 07 1B C5 D5 A5 02 00 3F  | 0x53E437 | -45        | OK
       | =1270803   |         |                |              | 0    0     0     30            |                | AF E2 11 DD 13 80 BD D9 BD 02 0A 08  |          |            |

21     | +68677     | 0x26    | 0x8E89BED6     | ADV_IND      | Type TxAdd RxAdd PDU-Length    | 0xE0D9A2001951 | 02 01 06 11 07 1B C5 D5 A5 02 00 3F  | 0x53E437 | -44        | OK
       | =1339480   |         |                |              | 0    0     0     30            |                | AF E2 11 DD 13 80 BD D9 BD 02 0A 08  |          |            |

22     | +65717     | 0x26    | 0x8E89BED6     | ADV_IND      | Type TxAdd RxAdd PDU-Length    | 0xE0D9A2001951 | 02 01 06 11 07 1B C5 D5 A5 02 00 3F  | 0x53E437 | -44        | OK
       | =1405197   |         |                |              | 0    0     0     30            |                | AF E2 11 DD 13 80 BD D9 BD 02 0A 08  |          |            |

P.nbr. | Time (us)  | Channel | Access Address | Adv PDU Type    | Adv PDU Header              | InitA          | AdvA           | LLData (Part 1)
23     | +471       | 0x26    | 0x8E89BED6     | ADV_CONNECT_REQ | Type TxAdd RxAdd PDU-Length | 0x5AE073C746C6 | 0xE0D9A2001951 | AccessAddr  CRCInit   WinSize  WinOffset  Interval  Laten
       | =1405668   |         |                |                 | 5    1     0     34         |                |                | 0xAF9AA263  C4 E7 48  03       0x000B     0x0018    0x000

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header                  | CRC      | RSSI (dBm) | FCS
24     | +16342     | 0x0A    | 0xAF9AA263     | M->S      | OK         | Empty PDU | LLID NESN SN MD PDU-Length   | 0xE8F4BE | -39        | OK
       | =1422010   |         |                |           |            |           | 1    0    0  1  0            |          |            |

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header                  | L2CAP Header         | SIG Pkt Header          | SIG_Connection_Param_Up
25     | +230       | 0x0A    | 0xAF9AA263     | S->M      | OK         | L2CAP-S   | LLID NESN SN MD PDU-Length   | L2CAP-Length ChanId  | Code Id   Data-Length   | IntervalMin IntervalMax SlaveLaten
       | =1422240   |         |                |           |            |           | 2    1    0  1  16           | 0x000C       0x0005  | 0x12 0x01 0x0008        | 0x0030      0x0040      0x0004

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status  | Data Type | Data Header                | LL_Opcode           | LL_Version_Ind                  | CRC      | RSSI (dBm) | FCS
26     | +358       | 0x0A    | 0xAF9AA263     | M->S      | Unexp. NESN | Control   | LLID NESN SN MD PDU-Length | Version_Ind(0x0C)   | VersionNr CompId SubVersNr      | 0x49D785 | -39        | OK
       | =1422598   |         |                |           |             |           | 3    0    1  0  6          |                     | 0x06      0x000F 0x4103         |          |            |

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header                  | L2CAP Header         | SIG Pkt Header          | SIG_Connection_Param_Up
       | +278       |         |                |           |            |           | LLID NESN SN MD PDU-Length   | L2CAP-Length ChanId  | Code Id   Data-Length   | IntervalMin IntervalMax SlaveLaten
```

Filter off | RF device: | Channel: 37 [0x25] | Packet broadcast OFF

CC-2540-based BLE sniffer



App

Application

Application Profile

Application Service(s)

BLE Stack Interface

Host

General Access Profile (GAP)

General Attribute Profile (GATT)

Security Manager Protocol (SMP)

Attribute Protocol (ATT)

Logical Link Control and Adaptation Protocol (L2CAP)

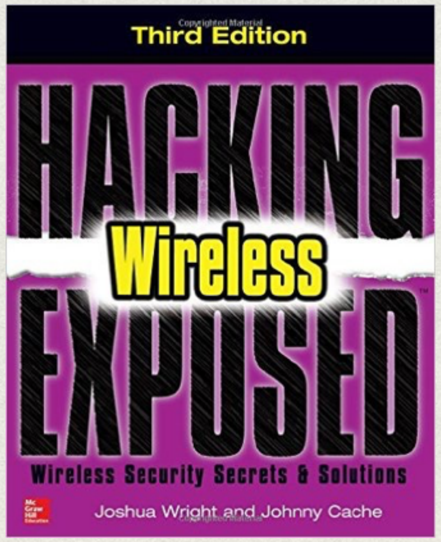
Host Controller Interface (HCI)

Controller

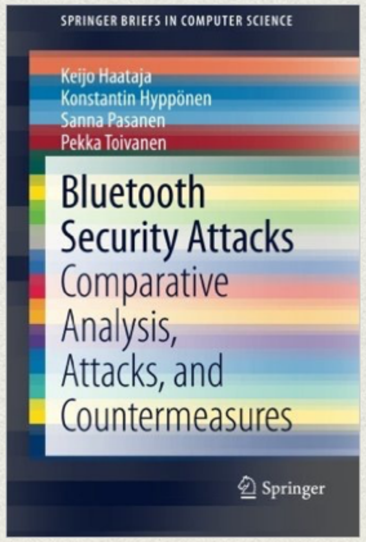
LE Link Layer (LL)

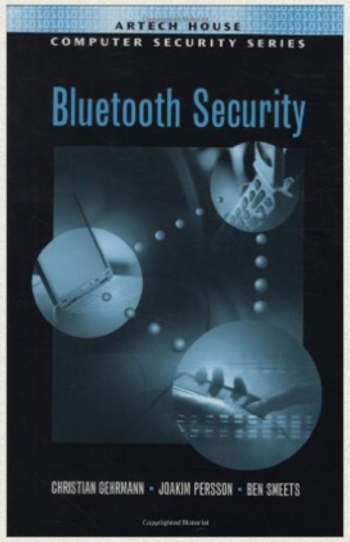
Physical Radio Layer (PHY)

BLE SECURITY


Copyrighted Material
Third Edition
HACKING Wireless EXPOSED
Wireless Security Secrets & Solutions
Joshua Wright and Johnny Cache

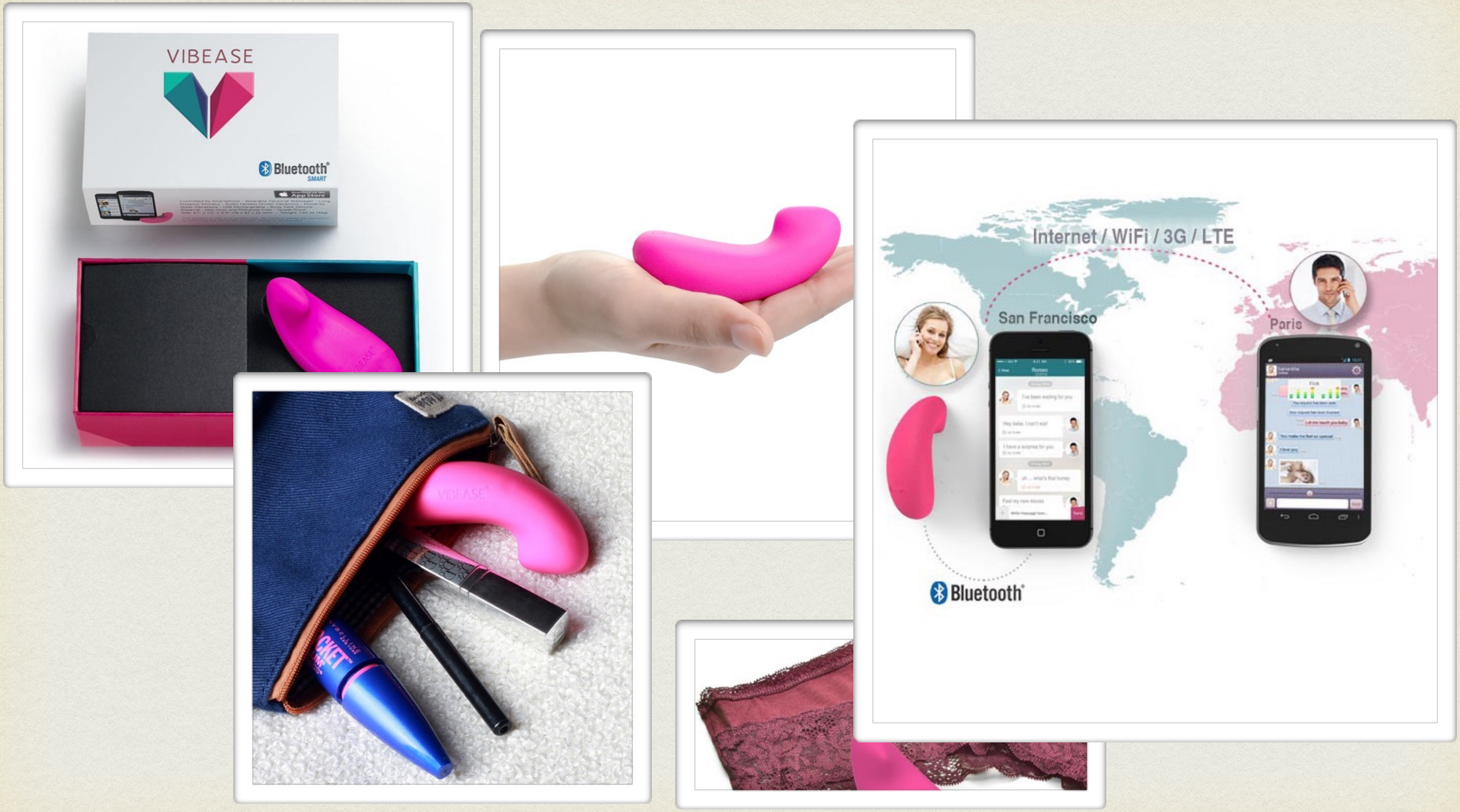
(


SPRINGER BRIEFS IN COMPUTER SCIENCE
Keijo Haataja
Konstantin Hyppönen
Sanna Pasanen
Pekka Toivanen
Bluetooth Security Attacks
Comparative Analysis, Attacks, and Countermeasures
Springer


ARTECH HOUSE
COMPUTER SECURITY SERIES
Bluetooth Security
CHRISTIAN GEHRMANN • JOAKIM PERSSON • BEN SMEETS
Copyrighted Material

)

BLE GETTING PERSONAL



BLE GETTING PERSONAL

now, clients can indeed feel the hacker is inside...

BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

BLE SECURITY GOALS - WHAT WAS PLANNED

AES-based address resolver

- *Privacy* - attacker cannot track user IDs
- *Confidentiality* - attacker cannot understand the data being exchanged
- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs

AES-based address resolver

- *Confidentiality* - attacker cannot understand the data being exchanged

AES-CCM

- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

BLE SECURITY GOALS - WHAT WAS PLANNED

- *Privacy* - attacker cannot track user IDs

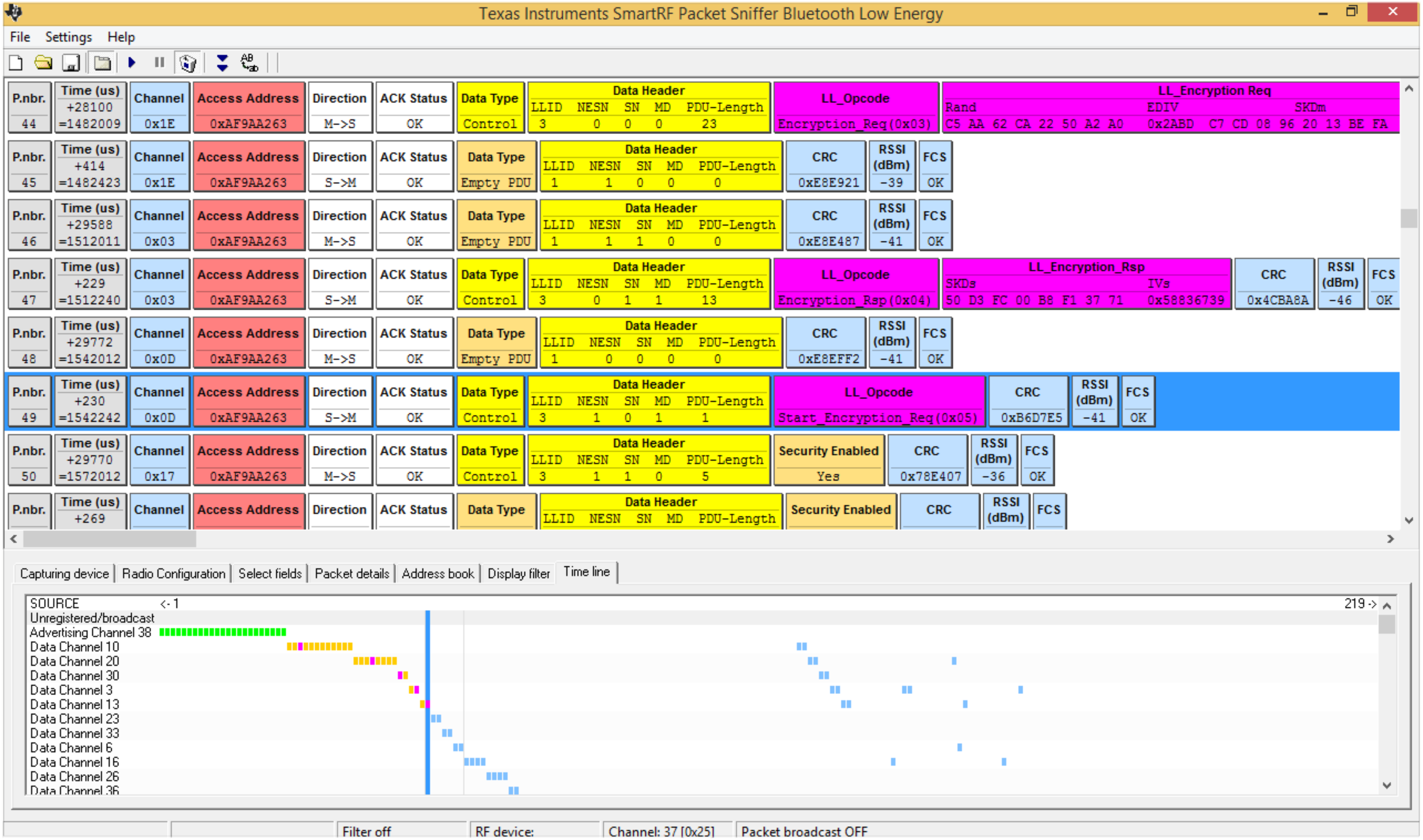
- *Confidentiality* - attacker cannot understand the data being exchanged

- *Authentication* - attacker cannot impersonate a peer device or spoof its data response

AES-based address resolver

AES-CCM

AES-based bit commitment together with ECDHE



```
P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | LL_Opcode                  | LL_Encryption Req: Rand / EDIV / SKDm
44     | +28100 =1482009 | 0x1E | 0xAF9AA263 | M->S | OK | Control   | 3 0 0 0 23 | Encryption_Req(0x03) | C5 AA 62 CA 22 50 A2 A0 / 0x2ABD / C7 CD 08 96 20 13 BE FA

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | CRC | RSSI (dBm) | FCS
45     | +414 =1482423 | 0x1E | 0xAF9AA263 | S->M | OK | Empty PDU | 1 1 0 0 0 | 0xE8E921 | -39 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | CRC | RSSI (dBm) | FCS
46     | +29588 =1512011 | 0x03 | 0xAF9AA263 | M->S | OK | Empty PDU | 1 1 1 0 0 | 0xE8E487 | -41 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | LL_Opcode | LL_Encryption_Rsp: SKDs / IVs | CRC | RSSI (dBm) | FCS
47     | +229 =1512240 | 0x03 | 0xAF9AA263 | S->M | OK | Control | 3 0 1 1 13 | Encryption_Rsp(0x04) | 50 D3 FC 00 B8 F1 37 71 / 0x58836739 | 0x4CBA8A | -46 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | CRC | RSSI (dBm) | FCS
48     | +29772 =1542012 | 0x0D | 0xAF9AA263 | M->S | OK | Empty PDU | 1 0 0 0 0 | 0xE8EFF2 | -41 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | LL_Opcode | CRC | RSSI (dBm) | FCS
49     | +230 =1542242 | 0x0D | 0xAF9AA263 | S->M | OK | Control | 3 1 0 1 1 | Start_Encryption_Req(0x05) | 0xB6D7E5 | -41 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | Security Enabled | CRC | RSSI (dBm) | FCS
50     | +29770 =1572012 | 0x17 | 0xAF9AA263 | M->S | OK | Control | 3 1 1 0 5 | Yes | 0x78E407 | -36 | OK

P.nbr. | Time (us)  | Channel | Access Address | Direction | ACK Status | Data Type | Data Header: LLID NESN SN MD PDU-Length | Security Enabled | CRC | RSSI (dBm) | FCS
       | +269
```

```
SOURCE              <- 1                                   219 ->
Unregistered/broadcast
Advertising Channel 38
Data Channel 10
Data Channel 20
Data Channel 30
Data Channel 3
Data Channel 13
Data Channel 23
Data Channel 33
Data Channel 6
Data Channel 16
Data Channel 26
Data Channel 36
```

```
Filter off | RF device: | Channel: 37 [0x25] | Packet broadcast OFF
```

CC-2540-based BLE sniffer

BLE LEGACY PAIRING

- Vulnerable to passive eavesdropping
  - –basically the same problem as with BT BR/EDR PIN-based link key generation
- Vulnerable to active impersonation
  - –works even for a one-time PIN
- Vulnerable to MITM
  - –different cryptographic flaw, but at the end, it is again a similar situation to that of the PIN-based link key generation in BT BR/EDR

BLE LEGACY PAIRING

- Vulnerable to passive eavesdropping
  - –basically the same problem as with BT BR/ED k key generation
- Vulnerable to active impersona
  - –works even for a o
- Vulnerabl
  - –differe graphic flaw, but at the end, it is again a similar situation that of the PIN-based link key generation in BT BR/EDR

excellent for pairing in a well shielded secret chamber

BLE SECURE CONNECTIONS

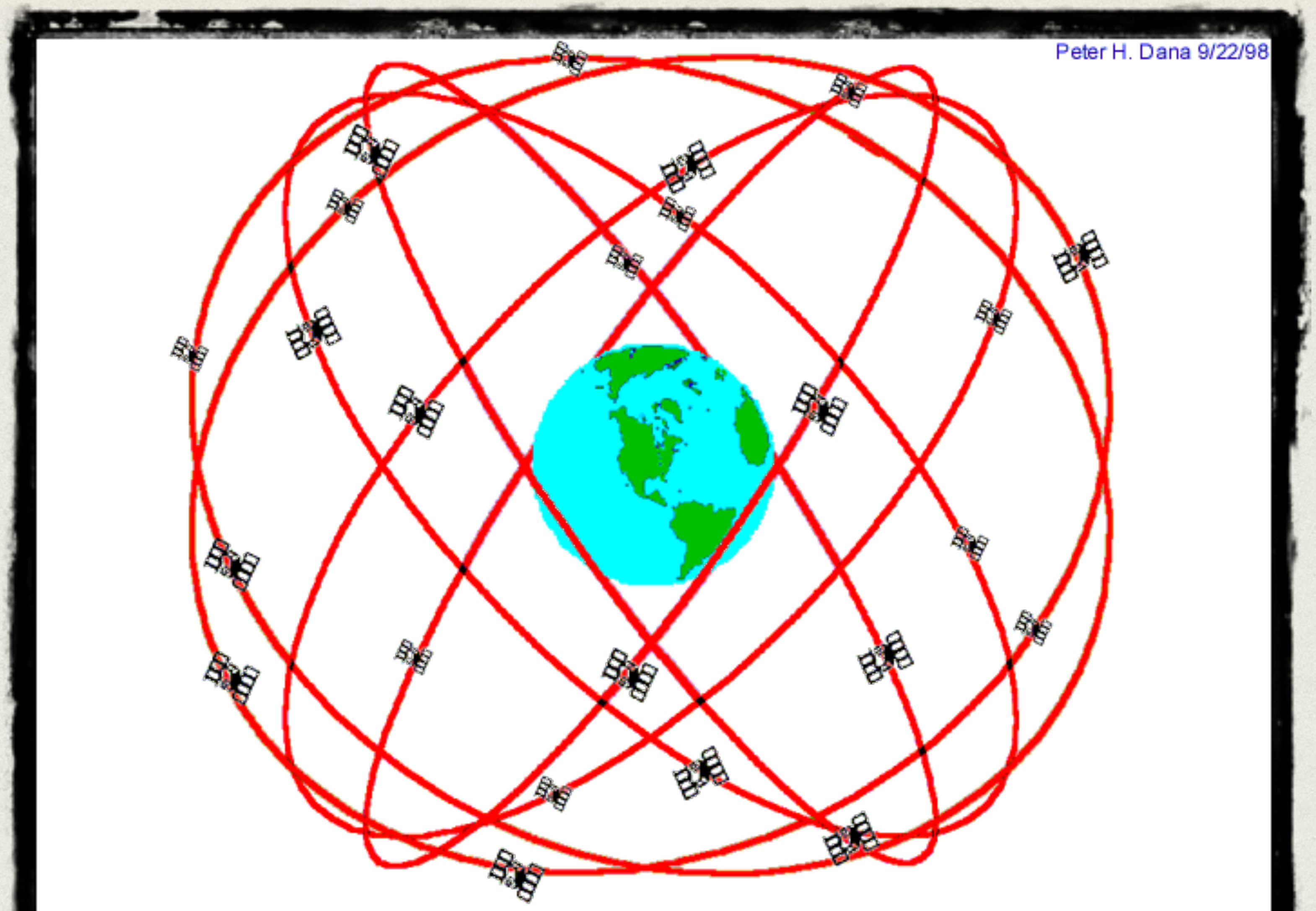
- Designed as an enhancement of the *Legacy Pairing*
  - –in the very same way as *Secure Simple Pairing* for BT BR/EDR replaced the insufficient PIN-based link key generation and authentication
- Cryptographically speaking, it fails to protect namely:
  - – against the passive eavesdropping of the authentication PIN
  - – against the active MITM based on device capabilities spoofing

  (in the very same way as *Secure Simple Pairing* does NOT do for BT BR/EDR...)
- Anyway, we can still revert to the *Out Of Band* mode of *Legacy Pairing* to provide our own authenticated key agreement protocol
  - – similarly, we can (shall) explicitly insist on the device capabilities that were reported/used

REALLY, DO THE PENTEST!

X-PLATFORM APT IN A PLANETARY SCALE

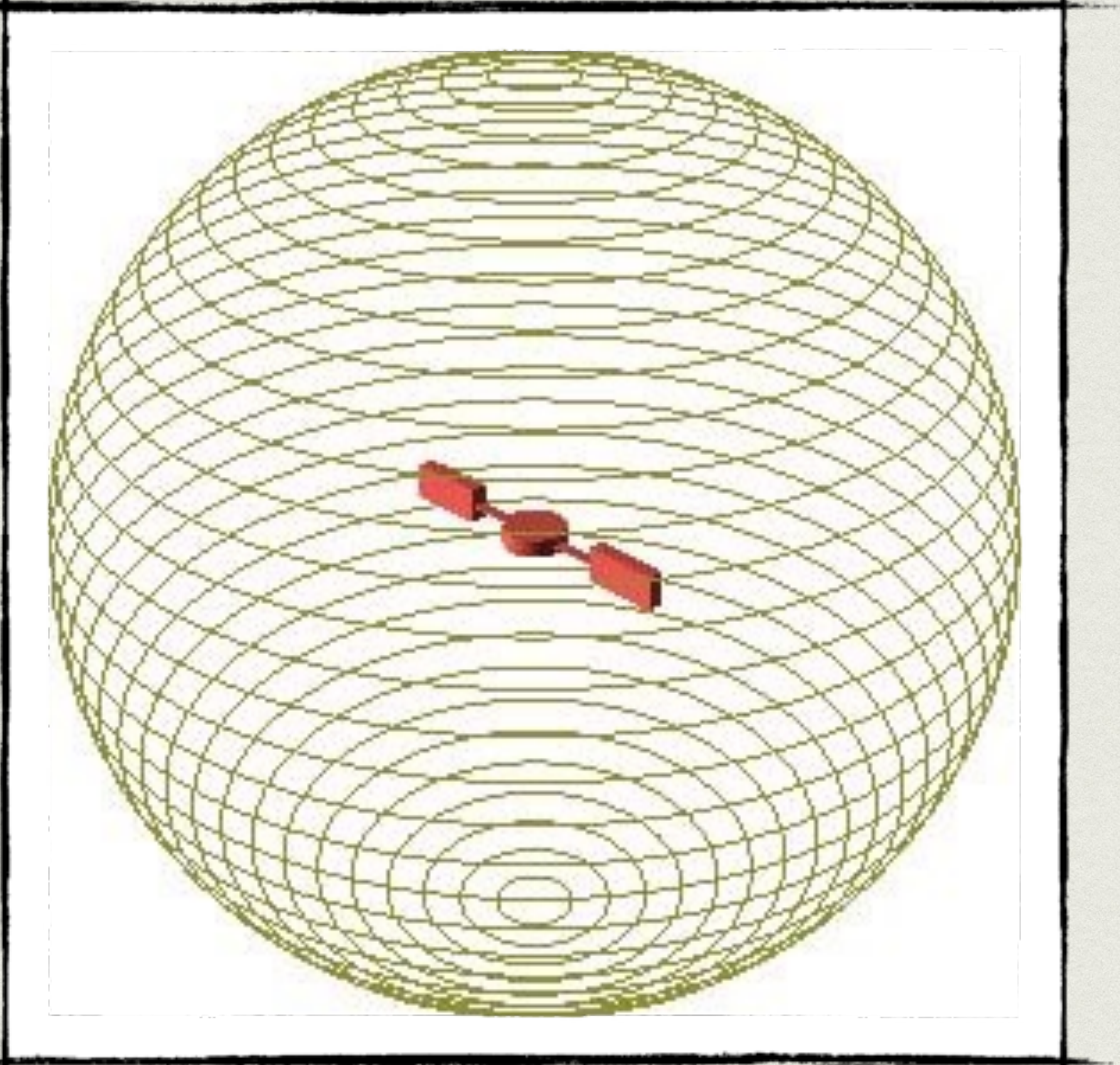
GPS SPACE SEGMENT



Peter H. Dana 9/22/98

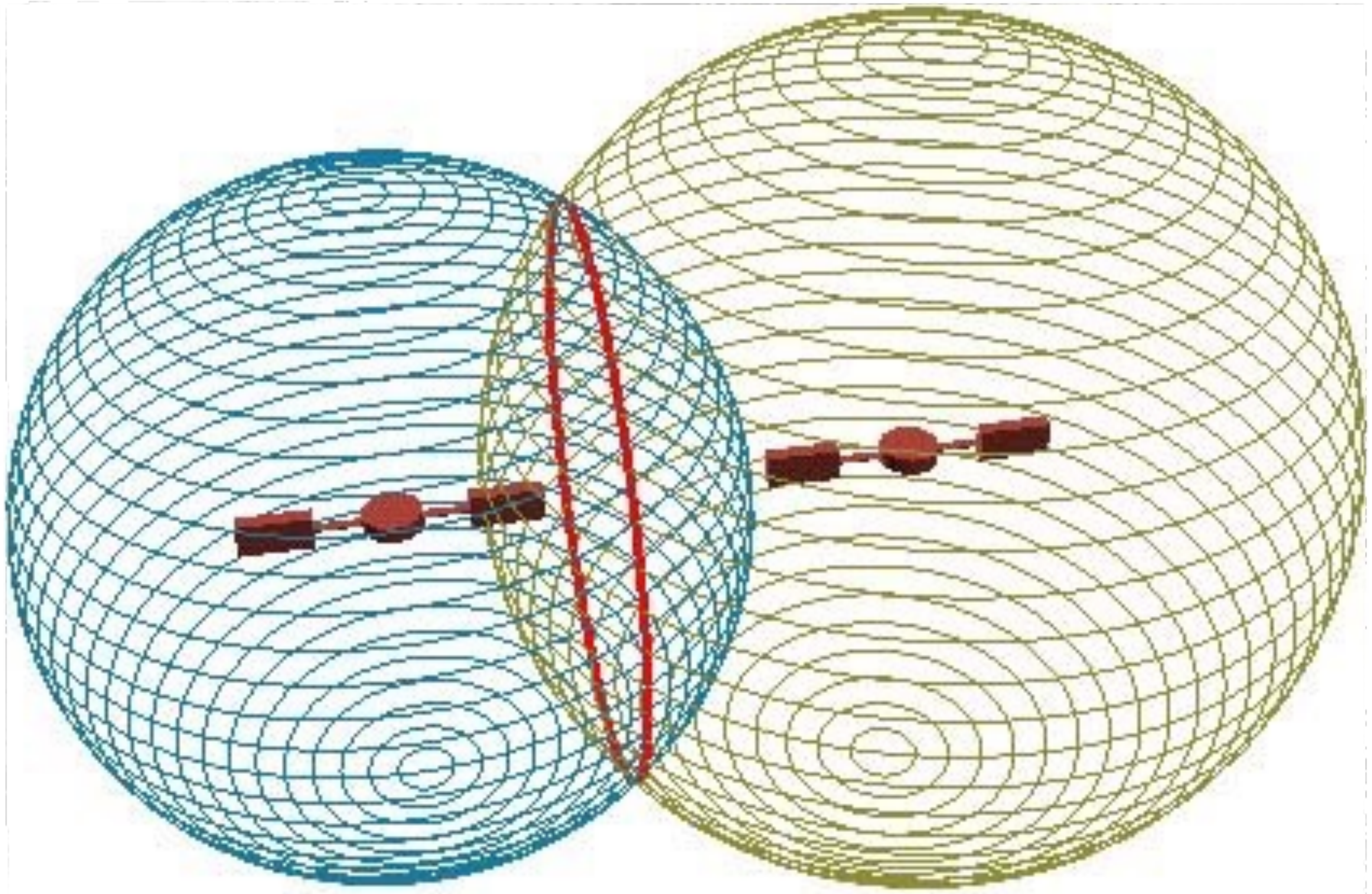
GPS Nominal Constellation
24 Satellites in 6 Orbital Planes
4 Satellites in each Plane
20,200 km Altitudes, 55 Degree Inclination

TRILATERATION I



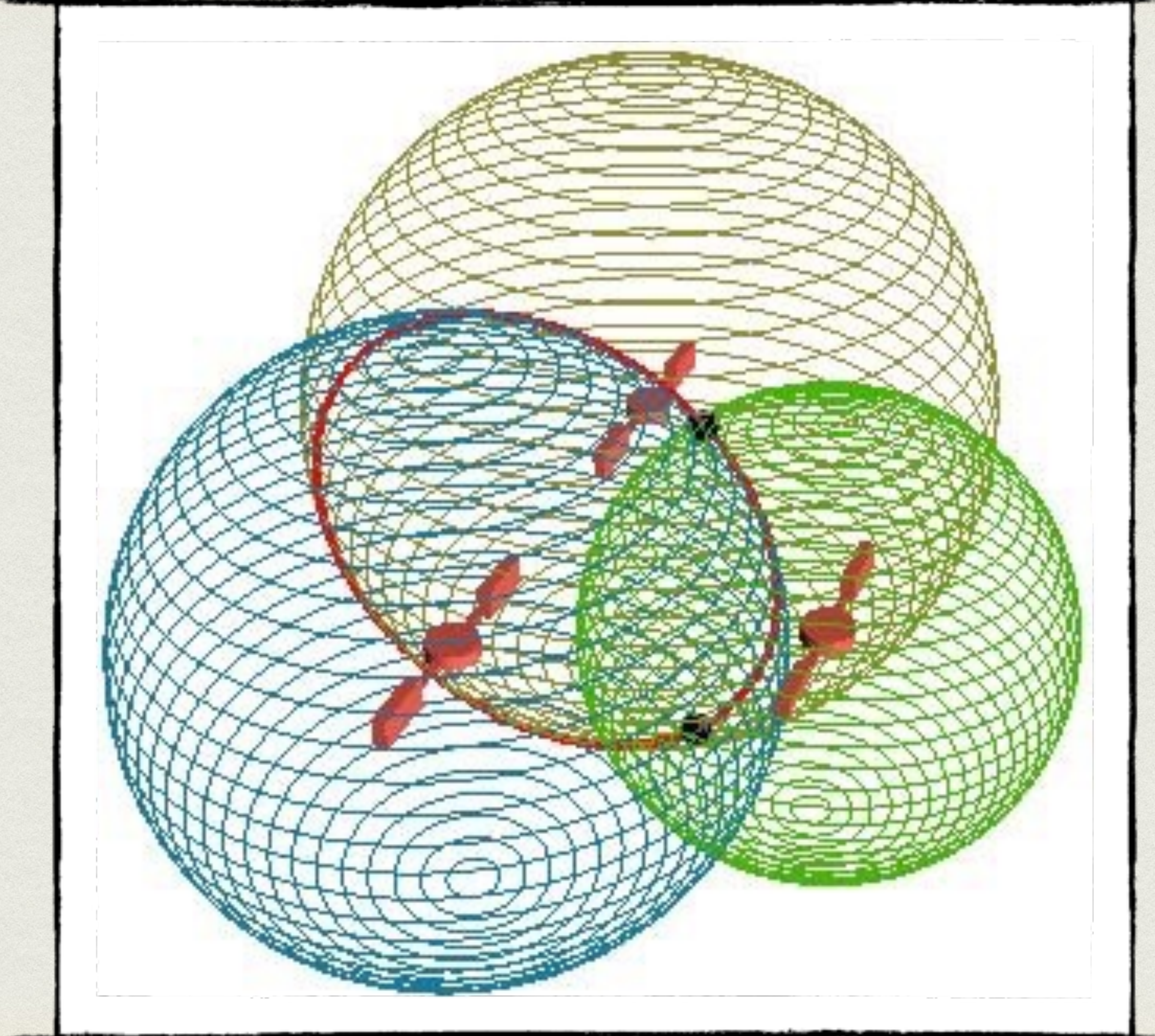
http://courses.washington.edu/gis250/lessons/gps/

TRILATERATION II



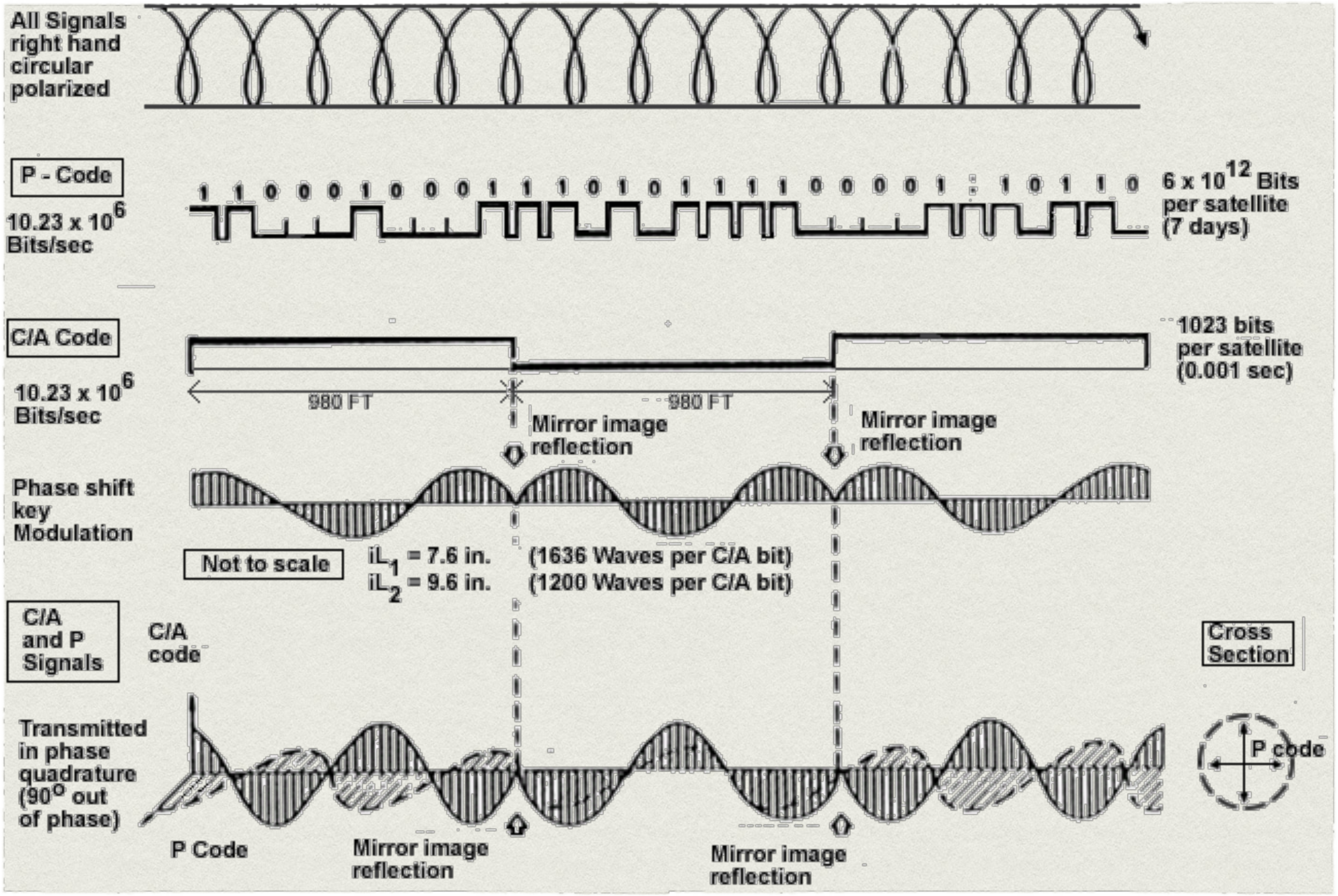
http://courses.washington.edu/gis250/lessons/gps/

TRILATERATION III



http://courses.washington.edu/gis250/lessons/gps/

GPS L1 C/A & P(Y)



Kulshreshta, 1997

SATELLITE CLOCK REPLICAS EXPOSE THE TIME DELAYS

$t_{\text{sent\_sv1}}$

$t_{\text{sent\_sv2}}$

$t_{\text{sent\_sv3}}$

$t_{\text{sent\_sv4}}$

four SVs to get X, Y, Z, and t_{bias}

$t_{\text{rec}}+t_{\text{bias}}$

CIVIL GPS IN SERIOUS APPLICATIONS

NTP server

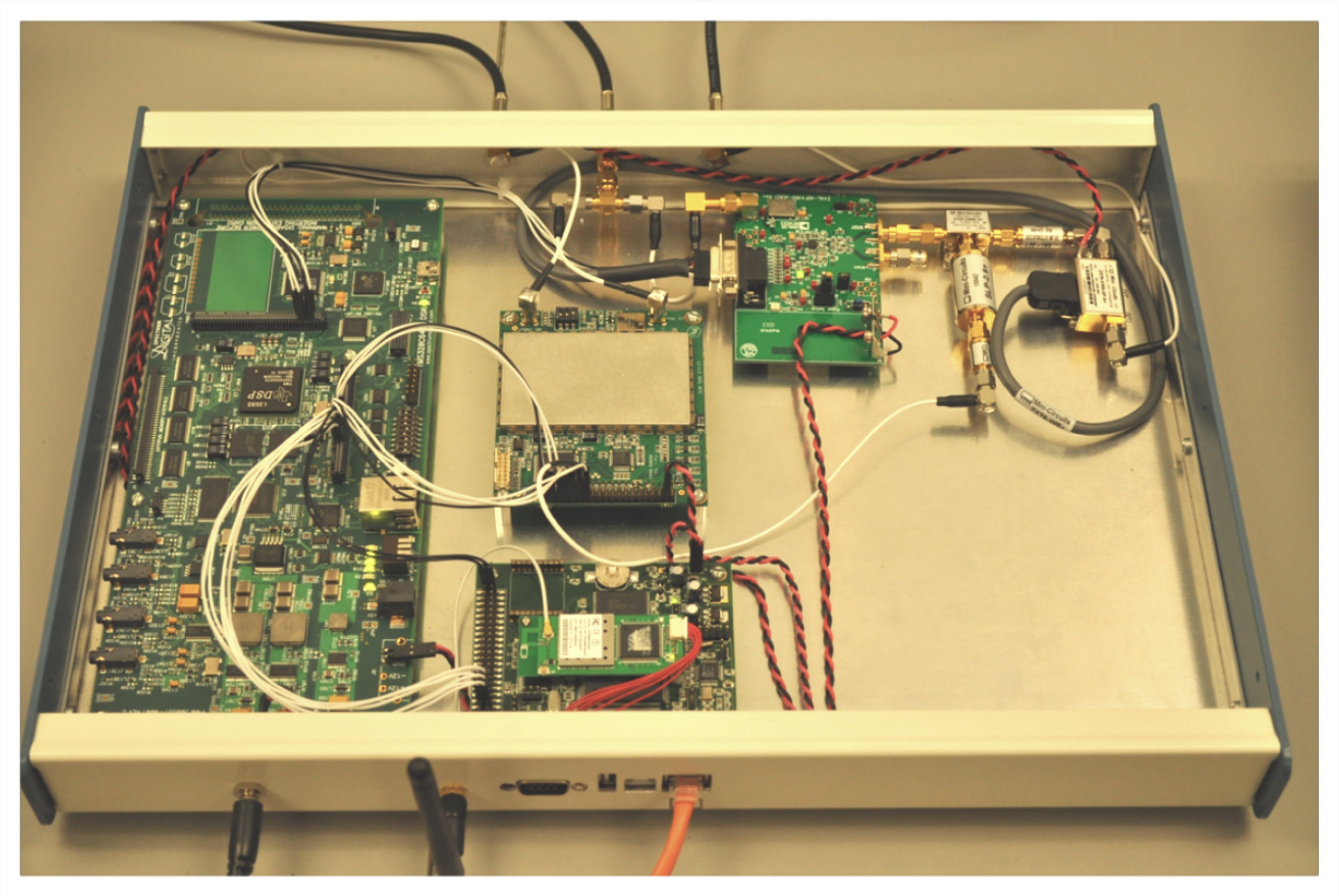
L1 C/A SIGNAL

- CDMA at the common carrier frequency of 1575.42 MHz
- Satellites distinguished by their unique chipping sequence (Gold codes)
- Allows creation of a delayed replica clock of the particular satellite (implicit time synchronisation)
- Carries 37 500 bits of navigation data for the particular satellite (explicit time synchronisation and position computation)
- Includes corrections according to the General Theory of Relativity
- … does not include any cryptographic protection

L1 C/A SECURITY

- Position/Velocity/Time (PVT) spoofing is accessible to a moderate-level attacker
  - real-life scenario seems to be that "**Iran–U.S. RQ-170 incident**"
  - actually, a GPS "replay attack" is a standard advanced tutorial for the LabView platform using the USRP Software Defined Radio (SDR)
- OK, this signal was never meant as a military-grade service and the lack of protection here can hardly be called a "discovery"
- On the other hand, a lot of commercial applications have grown up to be vital parts of our critical infrastructure today…

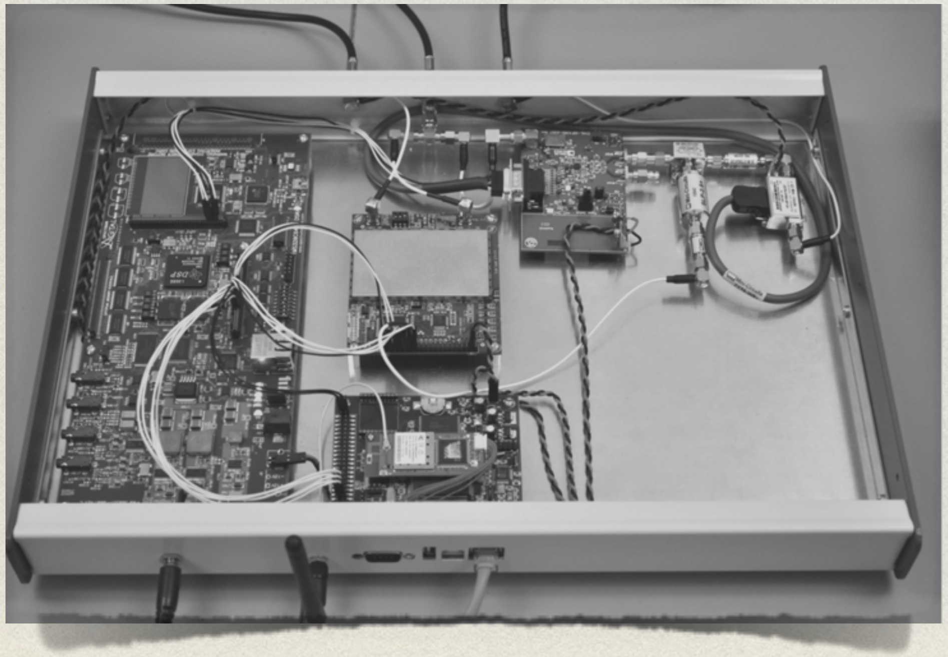
CIVIL GPS UNDER SERIOUS ATTACK



[Humphreys, Ledvina, and Shepard, 2008-2011]

PRECISE SDR SPOOFER

- receiver-spoofer architecture
- tracks original L1 C/A and L2C
- manipulates individual SV signal channels of L1 C/A (up to 12)
- re-mixes and re-transmits the spoofed signal
- precise phase sync for a smooth take over
- SDR architecture; someday it could be just downloaded and run
- HW parts were off-the-shelf components of approx. $1500 (2008)



[Humphreys, Ledvina, and Shepard, 2008-2011]

THE NEXT TARGET?

- Recall those 37 500 bits of navigation data transmitted on each and every L1 C/A channel

- It has been observed the baseband processors in GPS user modules seldom care about the integrity of this data as well as of the plausibility of PVT results obtained

  - [Sheppard and Humphreys, 2011], [Nighswander et al., 2012]

- Interestingly, this suggests a new infection vector allowing malware installation right into the GPS receiver…

THE “HIDDEN CRYPTO” SYNDROME

- Commercial “secret algorithm” designs get usually broken as soon as they get available for a serious cryptanalytic research

- Similarly, applications that are well-known for not checking their inputs get usually “pwned” as soon as somebody cares about fuzz-testing them seriously

GOING DEEPER

- Let us assume that, by spoofing the L1 C/A signal, we have successfully installed a malware into the GPS baseband processor
- What do we want to break next?
- Naturally, there is an application processor that consumes the PVT data from the baseband processor
- Now, does the application processor validate its input properly?
  - In other words, did the programmer have a reason to assume this can be an infection vector?

ANYWAY

- L1 C/A signal spoofing poses an advanced threat to many systems of our critical infrastructure
    - so called “civil” GPS seems to be truly ubiquitous today
- Also, this is an X-platform attack example
    - PVT spoofing can trigger hidden vulnerabilities in the consumer system
    - taking to the extreme, raw navigation data manipulation can allow malware installation into the baseband GPS processor
    - the infection can then spread deeper into the system as far as there is an implicit trust to the data integrity produced by the preceding modules

CONCLUSION

- The whole system is ~~as strong as~~ *no stronger than* its weakest component
- X-platform attacks show we shall assess all the individual components *together* rather than “per partes”
- Actually, the whole system can be far weaker than its weakest component itself