The BlueBag: A Mobile, Covert Bluetooth Attack and Infection Device

.:[From August 2006 to May 2007]:.

CONFidence 2007,
May 12-13 2007
Kraków, Poland

Luca "ikki" Carettoni
Claudio "paper" Merloni

Agenda

- Where did all of this start from?
- Bluetooth technology overview
- Bluetooth security threads
- Our 4 W: the Why, What, hoW and Wow of the BlueBag
- Surveying bluetooth devices
- Walking and blueprinting
- Going distributed
- Going malicious
- The Last Episode

@ 2007 - Secure Network S.r.l.

Where did all of this start from?

- Bluetooth is a geek technology
- More people than you would expect already rely on this technology. Businesses too...
- Up to some months ago, neither real data nor estimates about technology and devices spreading
- Interested in the evaluation of the exposure to worms and human aggressors

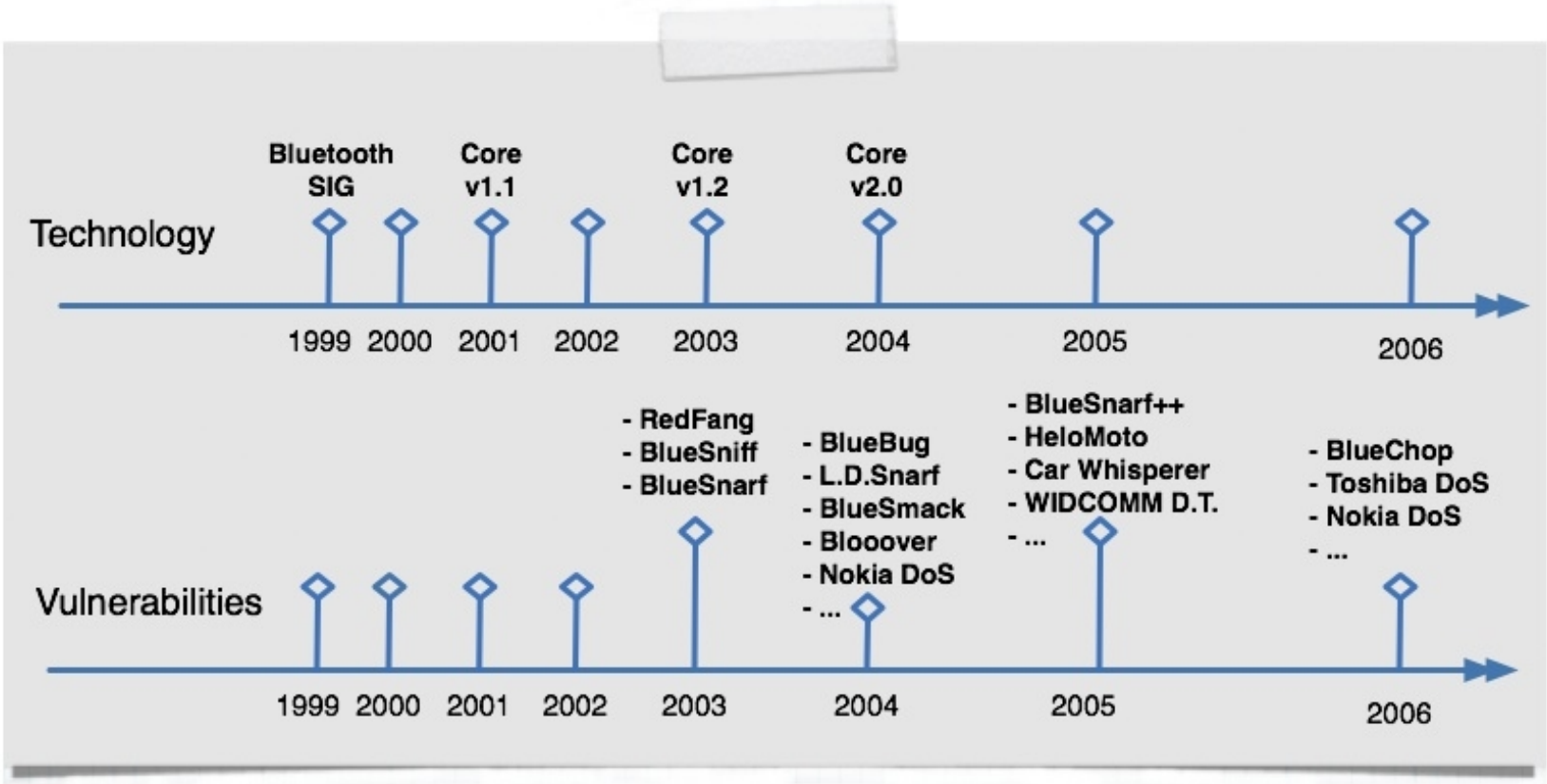
@ 2007 - Secure Network S.r.l.

BT technology overview

- Developed as a technology replacement for low range wireless standards (eg. IrDA)
- Targeted to personal devices information exchange and networking (eg. vCard, PAN)
- Core specs v2.0 from Bluetooth SIG:
  - Hardware based radio system + Software stack
  - 2.4GHz ISM
  - Frequency Hopping Spread Spectrum (1600 hops/s on 79 channels)
  - Low power consumption, short range
  - Data rates: 2 and 3 Mbps (Enhanced Data Rate)

@ 2007 - Secure Network S.r.l.

Technology and flaws timeline



@ 2007 - Secure Network S.r.l.

Boring engineer like classification

- Unauthorized Access and Information Disclosure
  - *BlueSnarf, CarWhisperer, ...*
  - *BTCrack, ...*
- Unauthorized Read/Write Access
  - *HELOMoto, BlueBug, …*
- Denial of Service
  - *BlueSmack, BT Stack DoS, ...*
- Malware Infection
  - *Cabir, Inqtana, ...*

@ 2007 - Secure Network S.r.l.

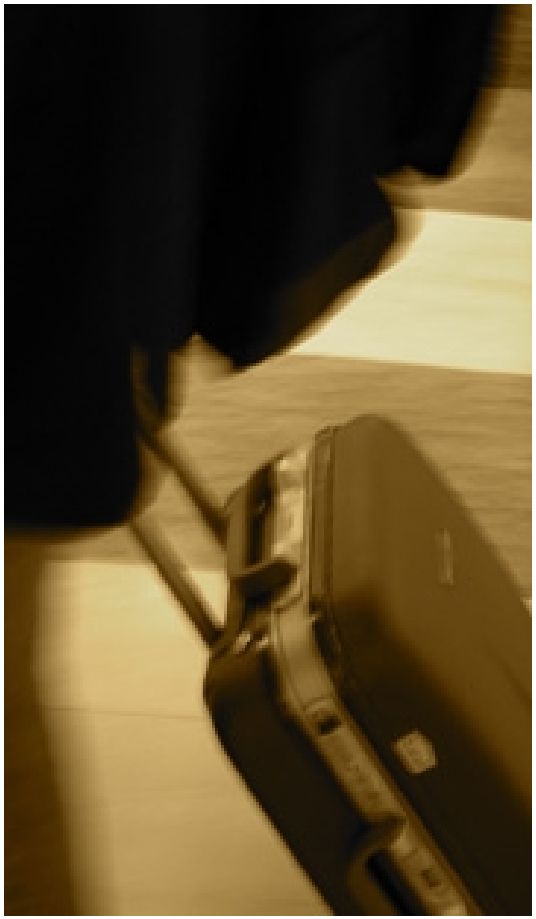
Playing in a real scenario

- The Trifinite guys @ trifinite.org showed us quite a lot of interesting things about vulnerabilities and abuses.
- **We focused on how an attacker could pose complex threats using existing knowledge and technologies**
- We need to consider implementation and protocol issues
- Vulnerability != Risk

@ 2007 - Secure Network S.r.l.

BlueBag: Why?

- Wide area survey
- 8+ hours power autonomy
- Covertness
- Easy carrying
- No human interaction
- Perfect for long sessions



@ 2007 - Secure Network S.r.l.

BlueBag: What? - 1

- VIA EPIA Mini-ITX motherboard
- iPod 1.8in HD
- #8 Class 1 BT dongles
- #1 modded Linksys BT dongle
- #1 omnidirectional 5dBi antenna
- PicoPSU power supply connected to a 12V-26Ah lead acid battery

  = 40W power consumption (max)

@ 2007 - Secure Network S.r.l.

BlueBag: What? - 2

Courtesy of Joris Evers/CNET News.com

- GNU/Linux Gentoo OS
- v2.6 kernel + BlueZ subsystem
- Custom python software
- MySQL database
- Apache/PHP Remote Interface

@ 2007 - Secure Network S.r.l.

BlueBag: What? - 3

@ 2007 - Secure Network S.r.l.

BlueBag: hoW?

- Making it reliable
- Firing it up
- Remote controlling
- Monitoring
- Data storage
- Data gathering in crowded places and related issues

@ 2007 - Secure Network S.r.l.

BlueBag: Wow! ;-)

@ 2007 - Secure Network S.r.l.

Testing on the road

- Focus on identifying active and visible BT devices
- Gathered info that can help pinpointing device types and models
- Different contexts and different users (eg. shopping mall, train station, airport)
- 1405 unique devices in less 24 hours

@ 2007 - Secure Network S.r.l.

Testing on the road - Result

- 93% mobile phones, 3% PCs, ~2% PDAs, ~1% GPS, ~1% other
  - 60% Nokia (12% 6680, 8% 6310i, 7.4% 6230i, 7.1% 6600)
  - 14% SonyEricsson/Ericsson
  - 7% Samsung
  - 1.8% Motorola
- “Visibility time”: shopping mall – 12.3s, university campus – 10.1s, airport – 23.1s, bank HQ - 14.4s

@ 2007 - Secure Network S.r.l.

Walking and Blueprinting

- Walking means going around with the BlueBag
- Blueprinting is a fingerprinting method for BT devices (think about nmap and TCP/IP).
- # sdptool browse --tree --l2cap 00:60:57:XX:XX:XX ---> **00:60:57@2621543**
- Using a “fuzzy” technique, we can use the data collected from our surveys in order to build a reliable blueprinting database.
  - Device_Name-Fingerprint association
  - Multiple Fingerprints match
  - BTW: Change your default device name!

@ 2007 - Secure Network S.r.l.

Looking for more data

- Getting a quantitative measure of the spreading power of Bluetooth worms
- Needed to implement mathematical spreading models and simulations
- Average number of “victims” reachable by a single wandering device
- Success rate of social engineering techniques

@ 2007 - Secure Network S.r.l.

Going distributed - 1

- The BlueBag, as any other surveying tool, has an intrinsic limit: m-to-n inquiry
- To get real data about worm propagation effectiveness we need to implement a distributed surveying framework
- Agents spread by the BlueBag, that propagate, do the inquiry and return results back

@ 2007 - Secure Network S.r.l.

Going distributed - 2

- Designing the agent:
  - Envelope:
    - Piece of software able to scan for Bluetooth devices and to propagate to found devices
    - It has a list of targets to propagate to, and a set of payloads that it can “deploy” on the targets
  - Payload:
    - To do the distributed survey this is just something that collects and logs data and sends the logs back to the BlueBag via Bluetooth

@ 2007 - Secure Network S.r.l.

Going distributed - 3

Envelope

Main

```
If ( inTarget() ){
  P.run();
}else{
  while( true ){
    scanDevices();
    propagate();
  }
}
```

Payload

run(){ ... }

scanDevices()

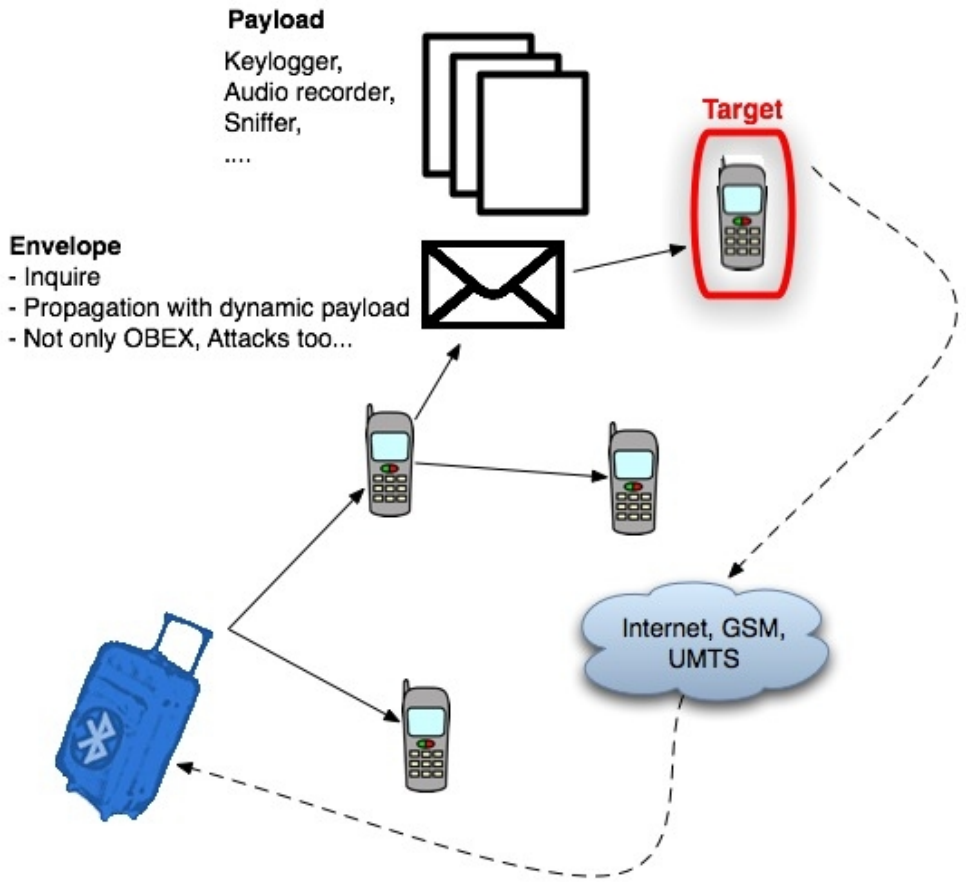
- Inquire for neighbours

propagate()

- Obex PUSH or Attacks Lib

targetsList[]

- Array of {bt_addr, payload, payload_parameters}



@ 2007 - Secure Network S.r.l.

How can agents propagate?

- Mobile Worm techniques:
  - 2004, Cabir.A, Symbian Series 60: OBEX Transfer to the first found BT device. The victim must accept the transfer
  - 2005, Lasco.A, Symbian Series 60: same type of BT propagation, but infect SIS files too
  - 2005, Commwarrior.A, Symbian Series 60: same type of BT propagation, but use also MMS
- At present they don't exploit any vulnerabilities
- Some factors tending to limit the real-world propagation: low scan capability, few propagation channels, different hw/sw platforms

@ 2007 - Secure Network S.r.l.

Now we have tools that...

- Can do quite massive BT scanning
- Can try to deploy agents to remote devices
- Can propagate like worms but could also use more effective techniques
- Can carry payloads to be launched on the target and return results back

@ 2007 - Secure Network S.r.l.

Going evil ;)

- We could then:
  - Give our agents a specific target
  - Tell them to use different payloads on different victims doing evil things:
    - Keylogger
    - Sniffer (see Acallno.A)
    - Audio recorder
  - Tell them to give us data back using any victim device capability
  - Maybe without ever getting into the victims device Bluetooth TX range

@ 2007 - Secure Network S.r.l.

Propagation model

- Models from epidemiology have been applied to computer viruses
- Kermack and McKendrick mathematical models:
  - Homogeneous environment (E.g. Internet)
  - No locality
- These hypotheses doesn't apply in our context ...
- ... then we go down the simulation path!

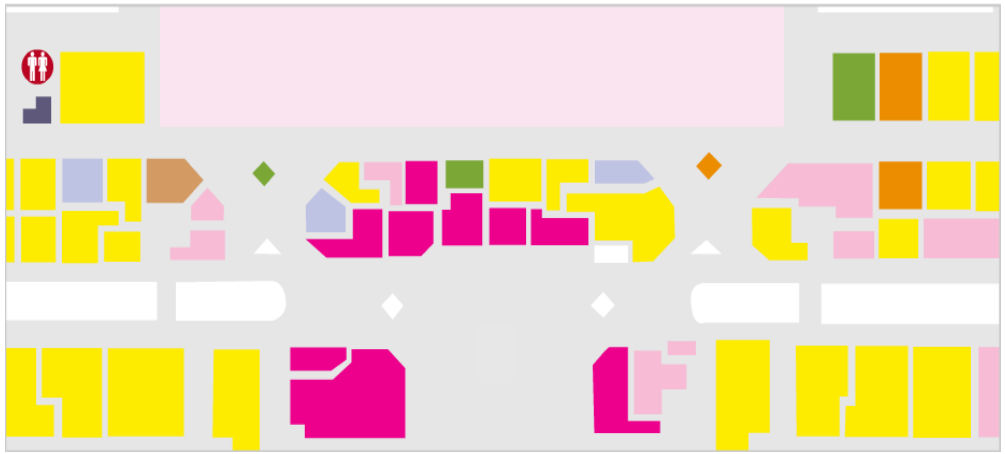
@ 2007 - Secure Network S.r.l.

Putting it all together

- We must choose a propagation scenario and fix the parameters from the data collected.
- What we need now is a way to estimate how effective would be that kind of targeted self-propagating malware...
- To build a realistic scenario we need to describe how devices would displace in a physical area:
  - “A Community based Mobility Model for Ad Hoc Network Research” by Mirco Musolesi and Cecilia Mascolo
- We built a simulator that receive the traces as input and mimic the behaviour of an advanced bluetooth worm

@ 2007 - Secure Network S.r.l.

Simulation context



- Shopping mall
- 250m x 100m surface
- 78 shops

- Number of devices: 184
- “Vulnerable” individuals: 7.5%
- Bluetooth range: 15m
- Link bandwidth: 0.3Mbps
- Payload size: 42Kb

@ 2007 - Secure Network S.r.l.

Simulation results

- Setting that tries to mimic the behaviour of people walking in and out of shops
- After 30 minutes the average percentage of (vulnerable) infected devices is 82.4%
- Every vulnerable device is infected after an average time of 35 min

- Setting that tries to mimic the behaviour of people inside lunch areas
- After 30 minutes the average percentage of (vulnerable) infected devices is 100%
- Every vulnerable device is infected after an average time of 12 min

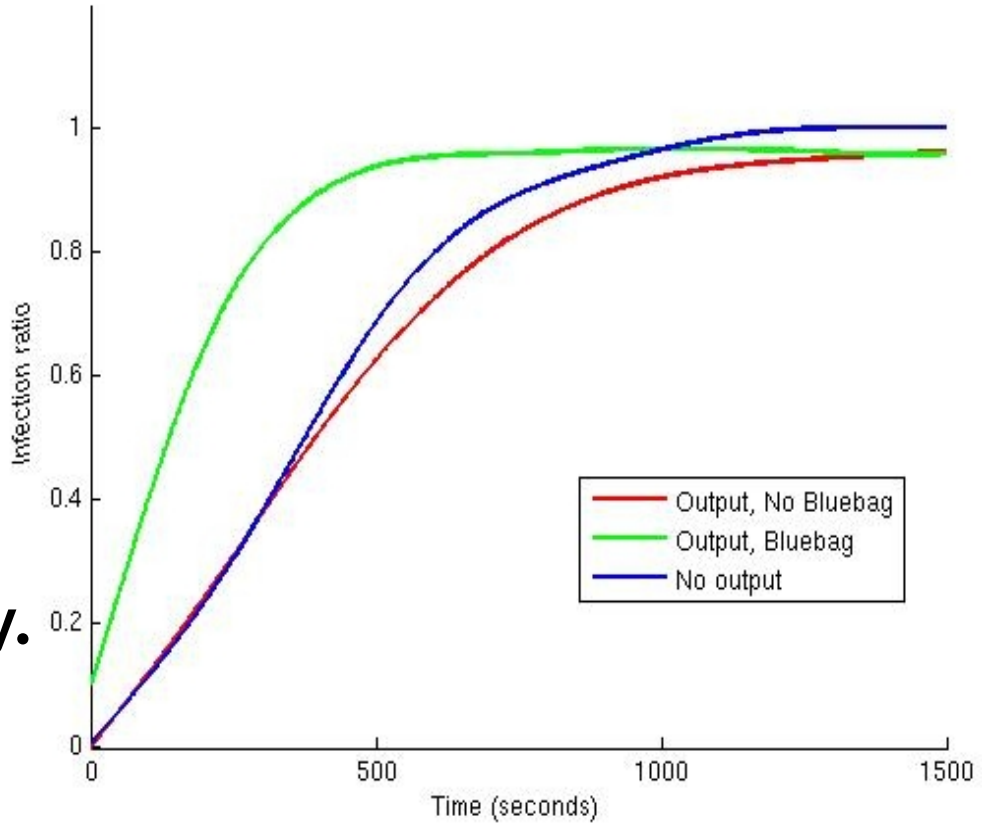
@ 2007 - Secure Network S.r.l.

New ideas, new experiments

- With and Without the BlueBag as propagation device
- Variable or constant population
- Looking for more informations?

  IEEE Security&Privacy March/April 2007

  http://doi.ieeecomputersociety.org/10.1109/MSP.2007.43



@ 2007 - Secure Network S.r.l.

Summing up - 1

- Bluetooth technology is not only for geeks
- People aren't conscious of potential threats: visible mode, easy pairing, default dev name, etc.
- Different spreading techniques can be combined to propagate more efficiently to specific devices
- A complex attack scenario, combining distributed and targeted propagation, exploiting known Bluetooth flaws and social engineering seems to be more than an idea

@ 2007 - Secure Network S.r.l.

Summing up - 2

- The collected data, the BlueBag, our tools and what we've shown today can help to understand that the risk is definitely real
- How many ways to return back data?
- We're working on ...
  - ... improving worm auto-execution and process hiding
  - ... using the data collected in order to build a reliable bluetooth honeypot
- See you with the next *Blue** project

@ 2007 - Secure Network S.r.l.

References

- Bluetooth SIG technical reference:
  https://www.bluetooth.org/
- Linux kernel official implementation:
  http://www.bluez.org/
- Bluetooth security:
  http://trifinite.org/trifinite_org.html
- OBEX opensource implementation:
  http://openobex.triq.net/
- Mobility model for ad-hoc networks:
  http://www.cs.ucl.ac.uk/staff/m.musolesi/mobilitymodels
- NS - Network Simulator:
  http://www.isi.edu/nsnam/ns/

@ 2007 - Secure Network S.r.l.

Thank you!

Any question?

We would greatly
appreciate your feedback.

Claudio Merloni - c.merloni@securenetwork.it

Luca Carettoni - l.carettoni@securenetwork.it

@ 2007 - Secure Network S.r.l.