GSM Debugging

Karsten Nohl, nohl@srlabs.de

Dieter Spaar, spaar@mirider.augusta.de

SECURITY
RESEARCH
LABS

Industry responds to GSM cracking attempts by creating new challenges

" the GSM **call has to be** identified and **recorded** from the radio interface. [] we strongly suspect **the team** developing the intercept approach **has underestimated its practical complexity**.
A hacker would need a radio receiver system and the **signal processing software** necessary to process the raw radio data."

– GSMA, Aug. '09

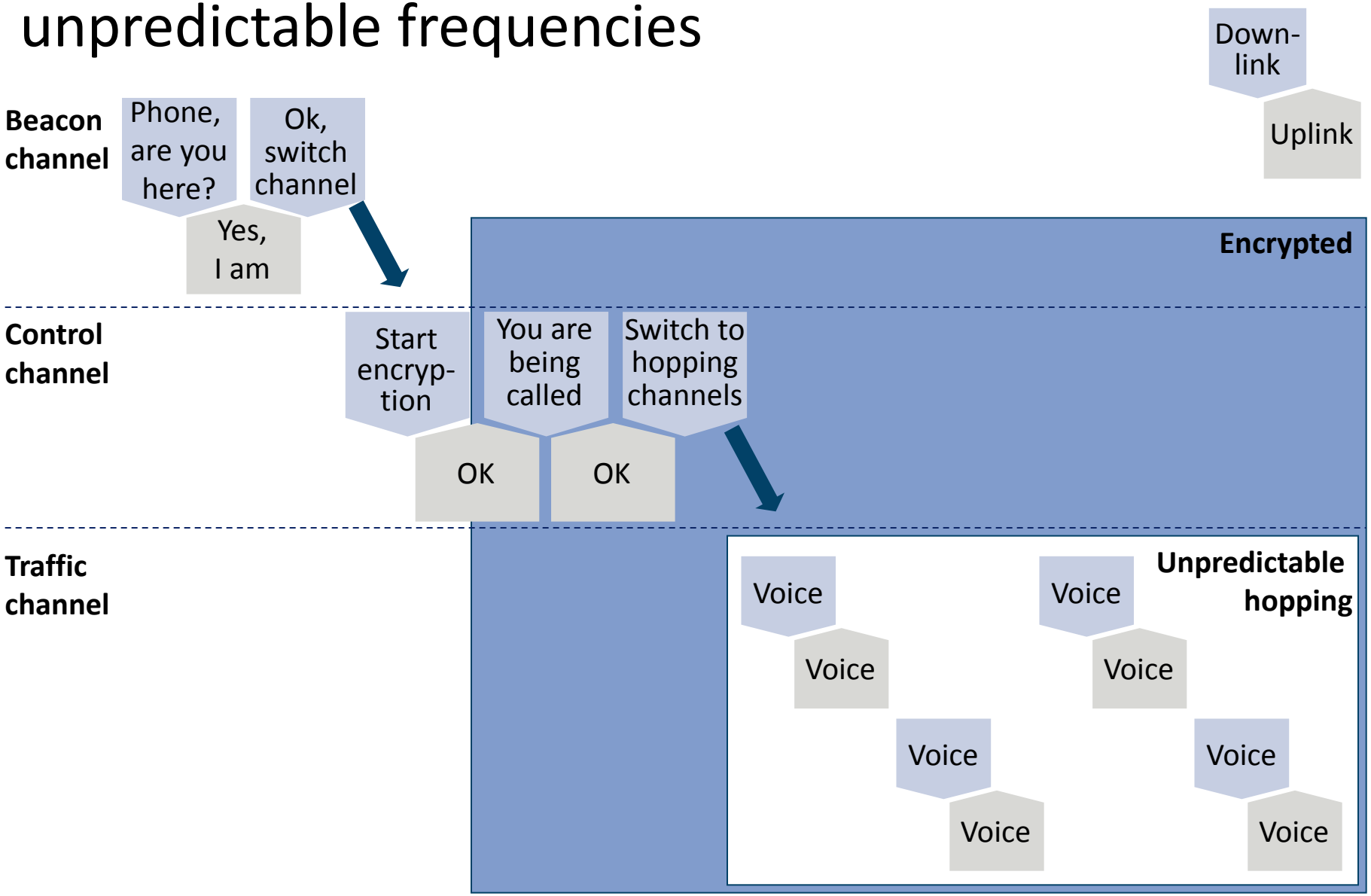
This talk demonstrates signal processing software to decode GSM uplink and downlink signals

Source: GSMA press statement

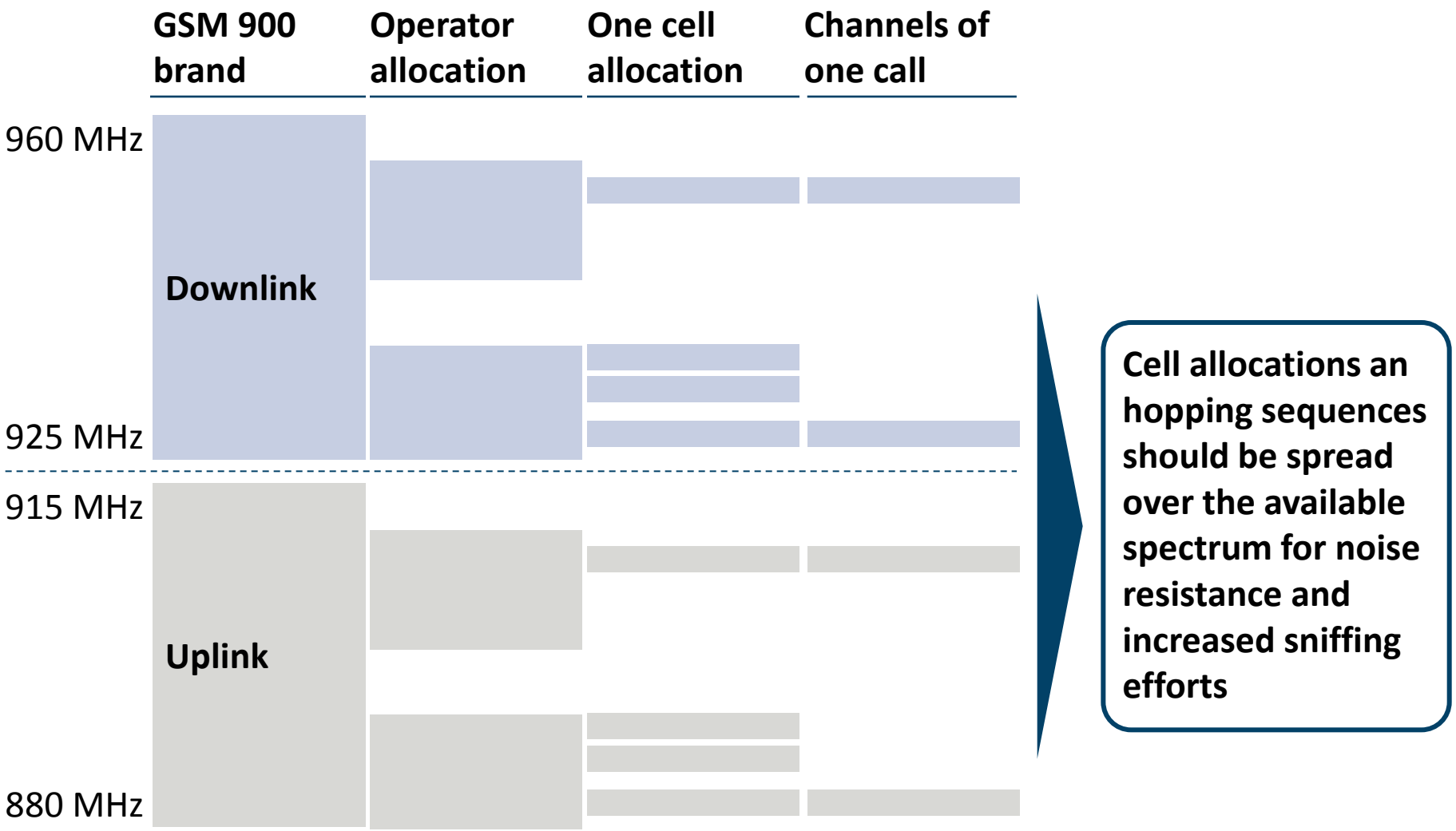
Agenda

- **GSM communication basics**
- Downlink sniffing: It works!
- Uplink sniffing: Getting close

GSM calls are transmitted encrypted over unpredictable frequencies



GSM spectrum is divided by operators and cells



GSM debugging tools have vastly different sepctrum coverage

Frequency coverage

GSM debugging tools [sniffing bandwidth]

GSM 900 band

Channels of one call

OsmocomBB [200 kHz]

USRP-1 [8MHz]

USRP-2 [20MHz]

Commercial FPGA board [50 MHz]

Downlink

Uplink

Focus of this talk

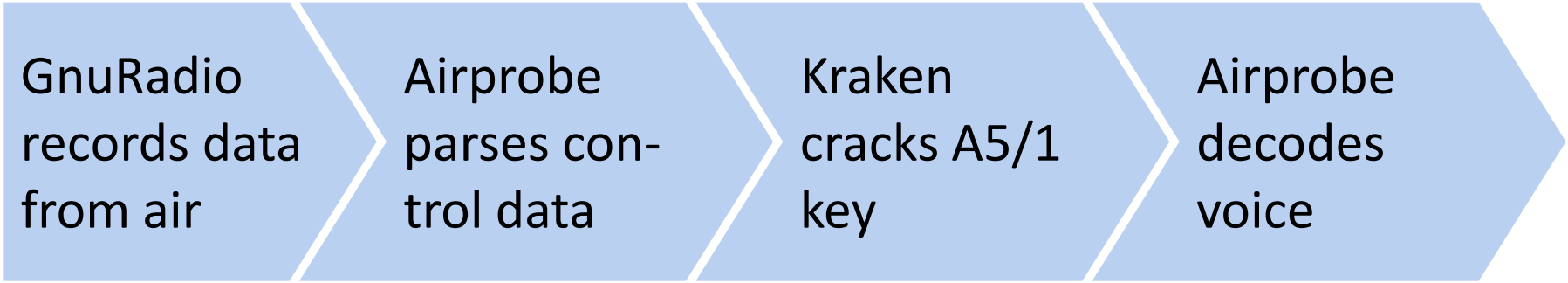
SECURITY RESEARCH LABS

Agenda

- GSM communication basics
- **Downlink sniffing: It works!**
- Uplink sniffing: Getting close

Demo: Downlink sniffing.

Open source components fit together in debugging GSM calls



Requires
- Software radio, ie. USRP
- Recommended for uplink: BURX board

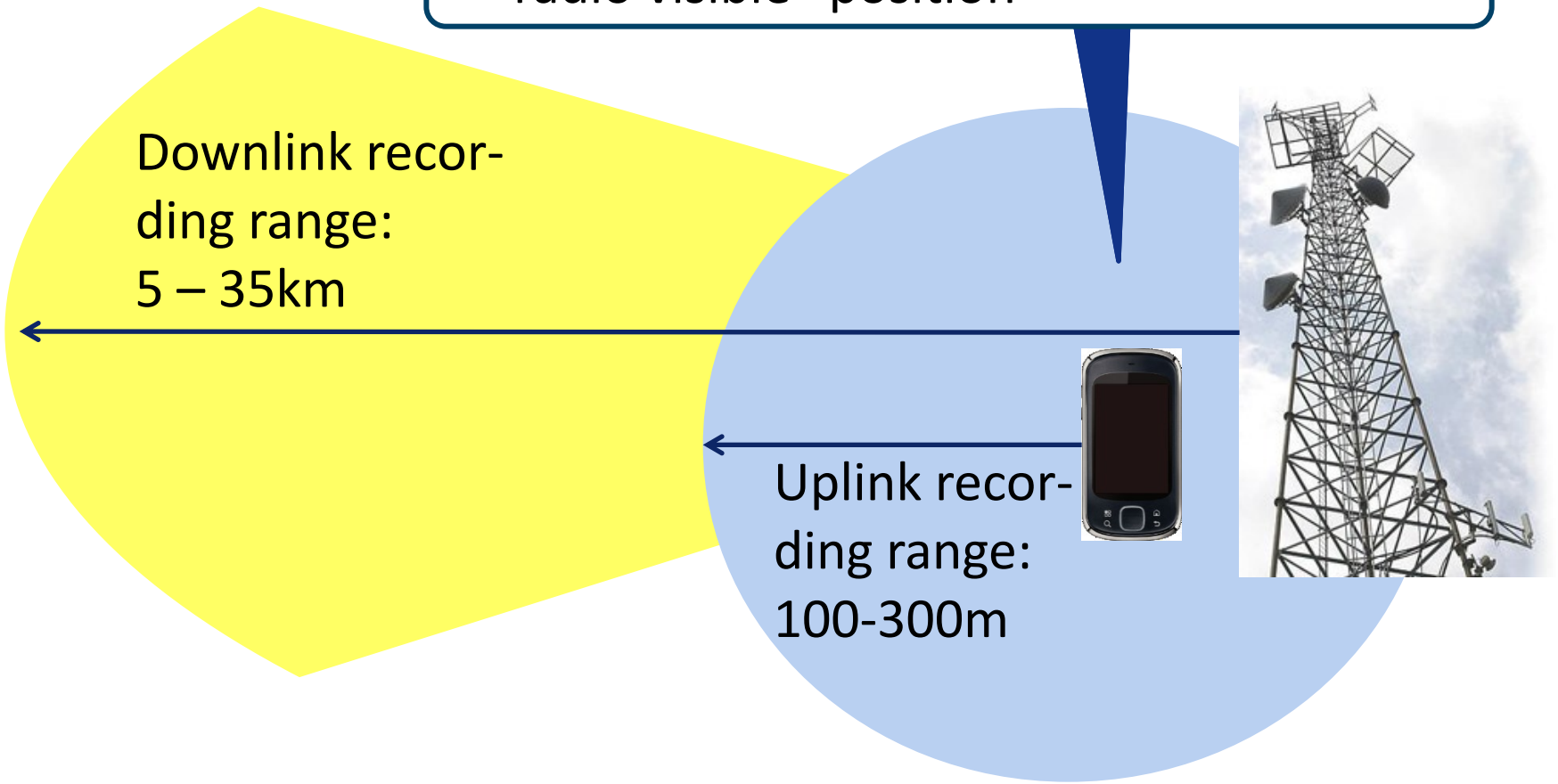
Requires
- 2TB of rainbow tables
- CPU or ATI graphics card
- SSD/RAID for fast cracking

Agenda

- GSM communication basics
- Downlink sniffing: It works!
- **Uplink sniffing: Getting close**

Downstream can be recorded from large distances

- Uplink is 10-30dB weaker than downlink
- Handset is typically in a much less "radio visible" position

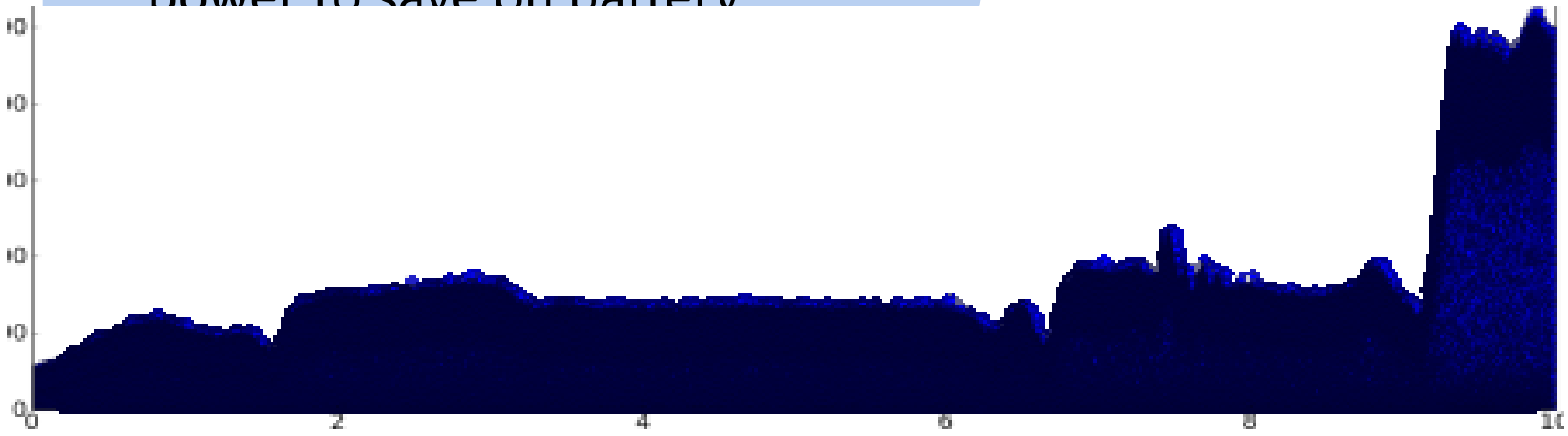


Uplink sniffing is a challenging RF problem

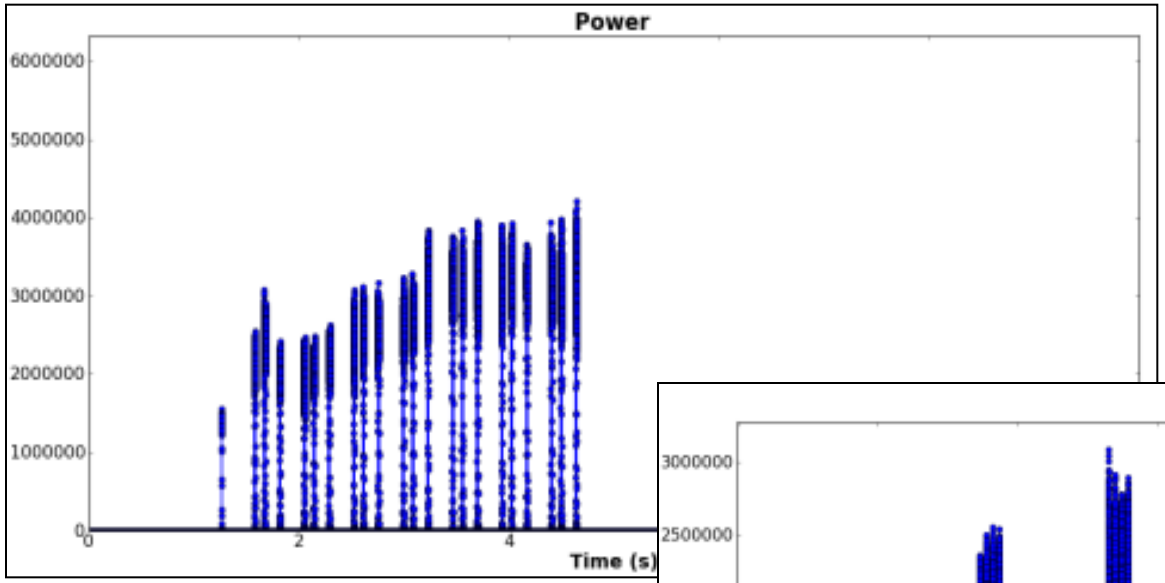
Uplink complications

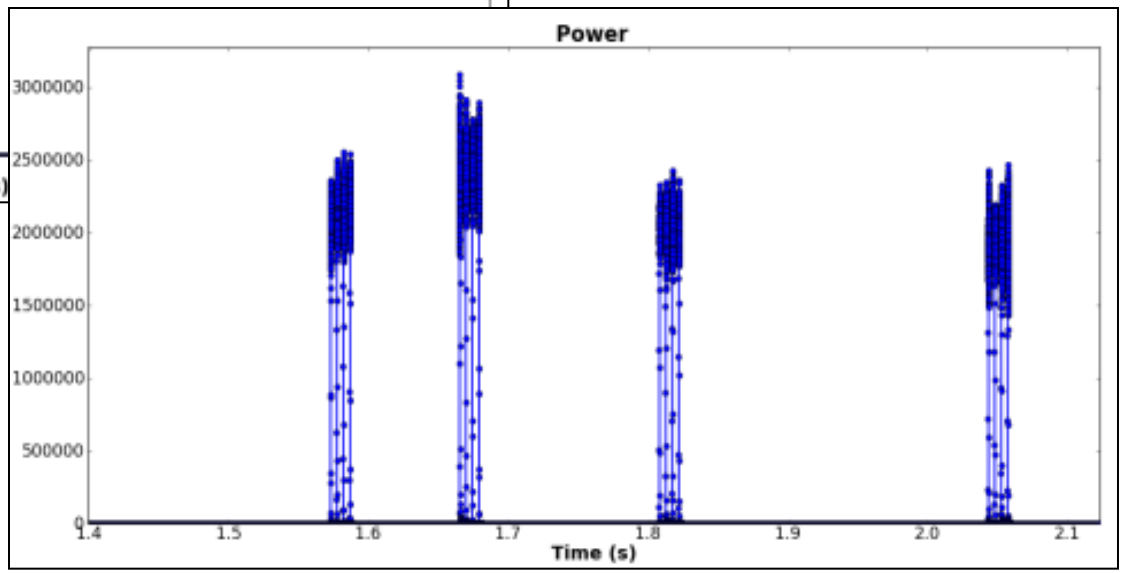
- Lower sending power strength than downlink
- Phones are hidden in buildings or in street gutter
- The phone varies its send power to save on battery

Weaker signal with higher variability



USRP+Airprobe provide the base for an open source uplink sniffer





Sniffed with USRP-1 and two daughter-boards for uplink / downlink

Demo: Uplink sniffing.

Engineering challenges remain towards reliable uplink sniffing

- Synchronization between uplink and downlink in Airprobe is not yet reliable (work in progress)
- Planned enhancements:
  1. Better demodulation algorithm
  2. Support for hopping channels
- There is plenty to do—Your chance to start contributing to the growing pool of GSM tools!

Demo: Key cracking.

Randomized padding would mitigate attack potential

Trace of SDCCH downlink	
238530	03 20 0d 06 35 11 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238581	03 42 45 13 05 1e 02 ea 81 5c 08 11 80 94 03 98 93 92 69 81 **2b 2b 2b**
238613	00 00 03 03 49 06 1d 9f 6d 18 10 80 00 00 00 00 00 00 00 00 00 00 00
238632	01 61 01 2b **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238683	01 81 01 2b **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238715	00 00 03 03 49 06 06 70 00 00 00 00 00 04 15 50 10 00 00 00 00 0a a8
238734	03 84 21 06 2e 0d 02 d5 00 63 01 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**
238785	03 03 01 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**

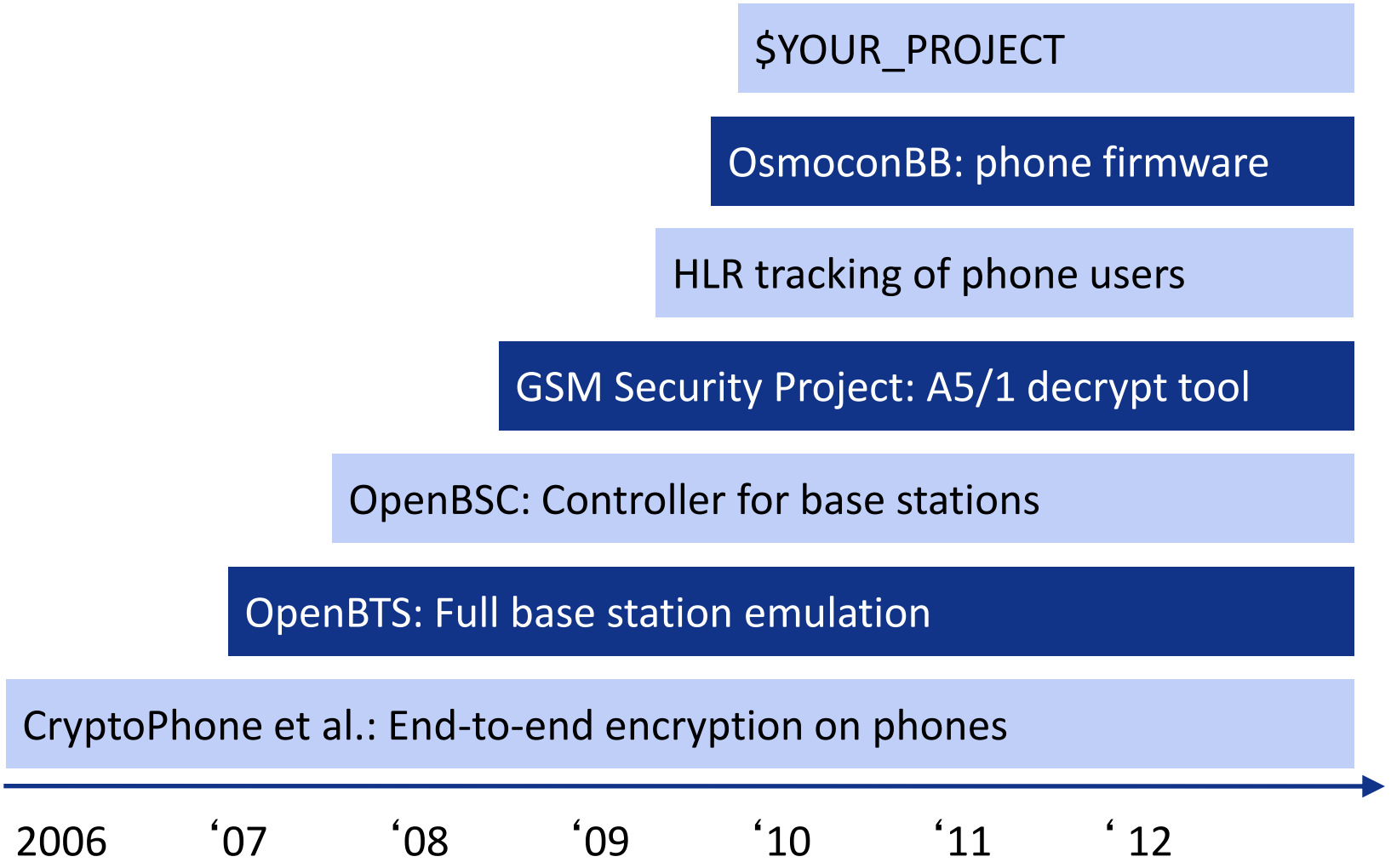
Padding in GSM has traditionally been predictable (2B)

Every byte of randomized padding increasing attack cost by two orders of magnitude!

Randomization was specified in 2008 (TS44.006) and should be implemented with high priority

Additionally needed: randomi-zation of system information msg.

Open research into GSM security grows exponentially and so will the attacks



Questions?

GSM project supported by

Airprobe, Kraken	srlabs.de

Karsten Nohl	**nohl@srlabs.de**
Dieter Spaar	**spaar@mirider.augusta.de**