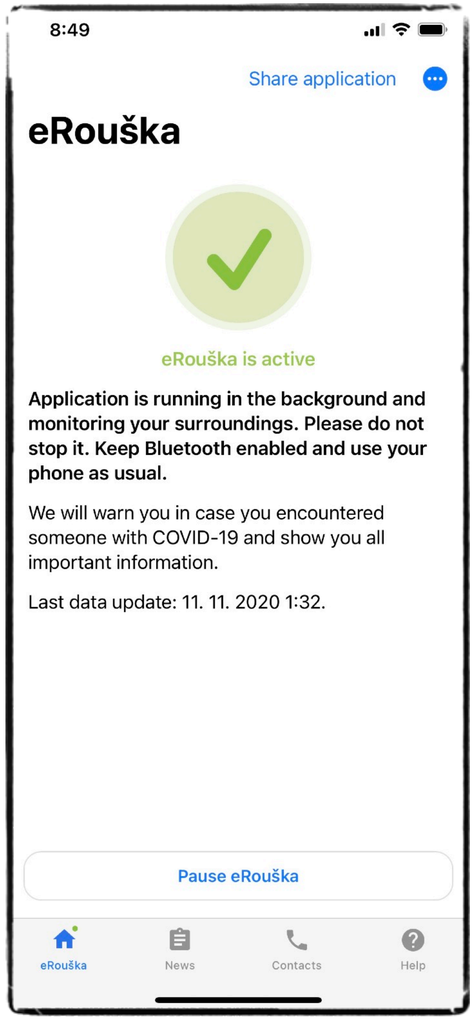
CYBER SECURITY CONFERENCE 2022

Unmasking the Signal of e-Mask Applications

Tomáš Rosa

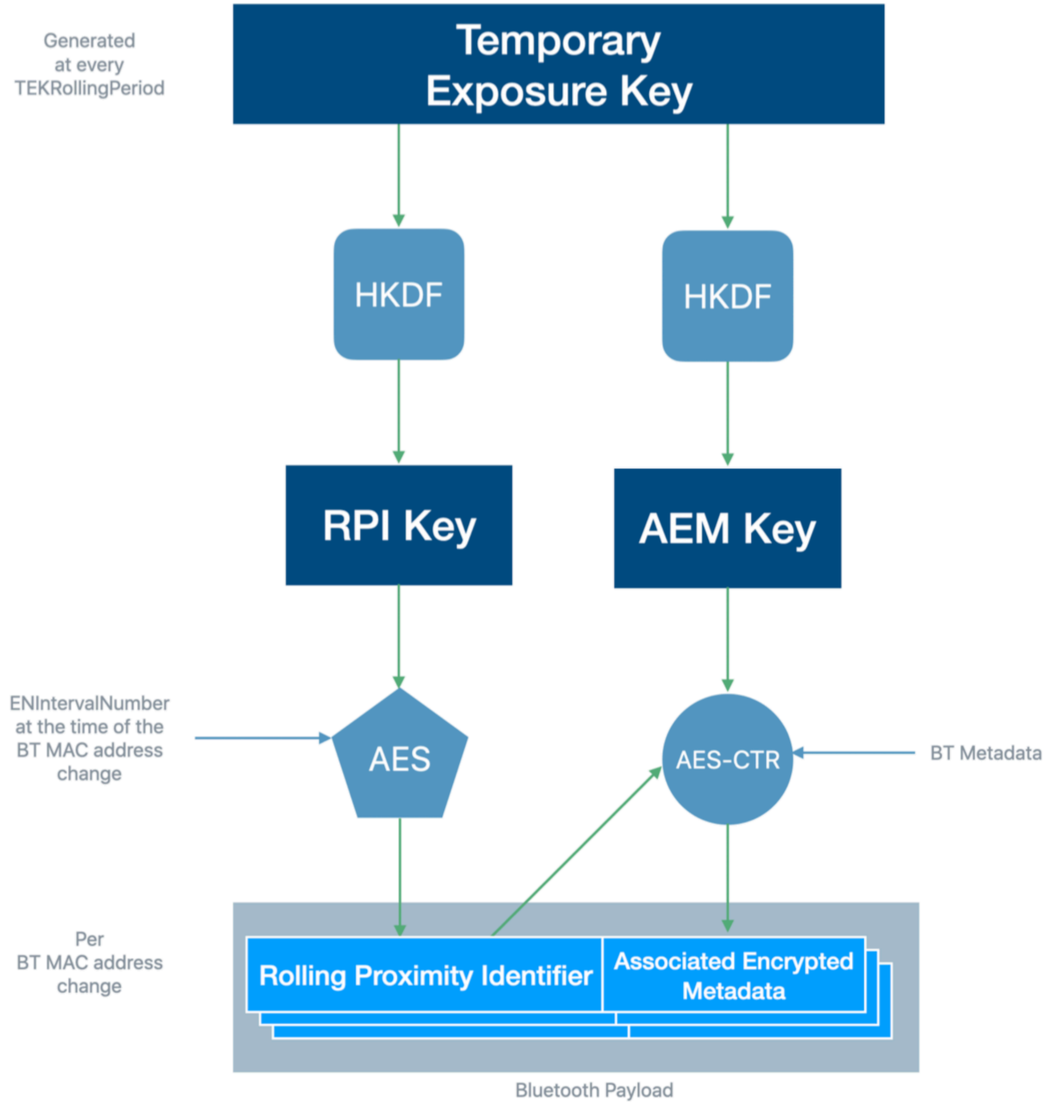
Cryptology and Biometrics Competence Centre, Raiffeisen BANK

eRouška - Covid-19 Contact Tracing Application of Czech Republic

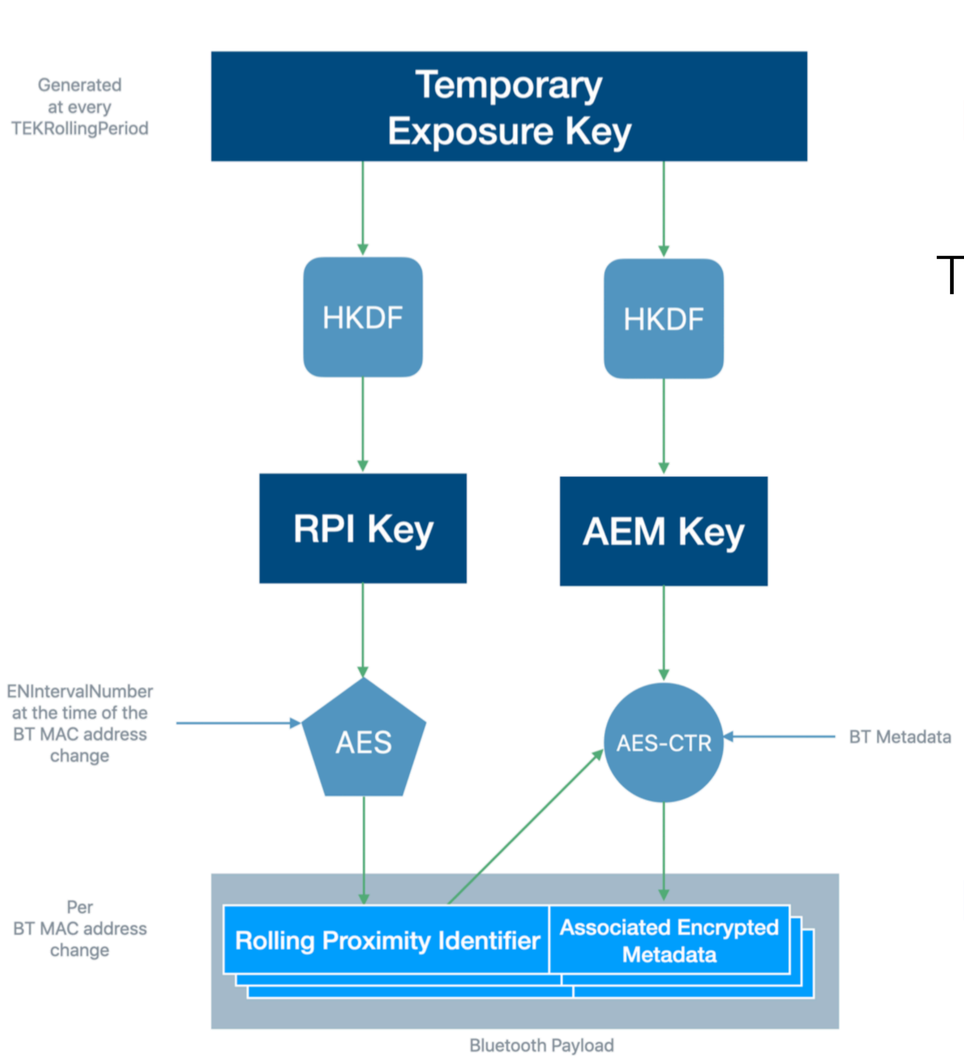


- Based on the Google-Apple Exposure Notification framework (GAEN)
- Framework is available and well-adopted worldwide
- Public health authorities of particular states can provide their own:
  - user interface application
  - risk assessment parameters
  - servers collecting keys of COVID-19 positive users

Privacy Preserving Cryptographic Protocol



One-to-One Exposure Tracing Infrastructure



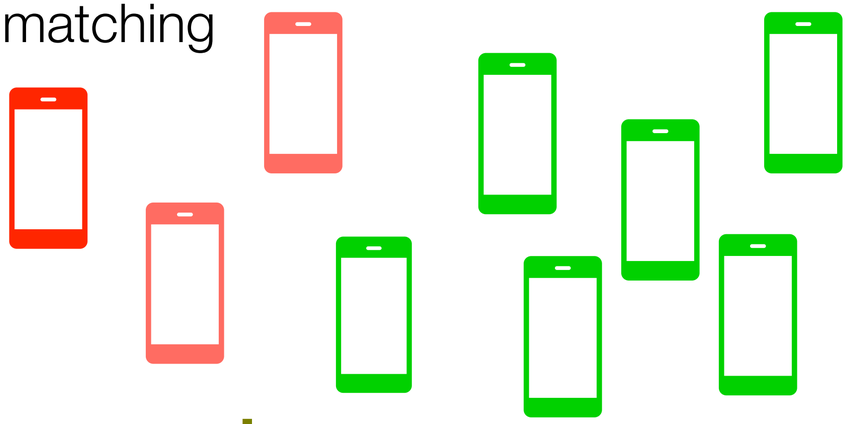
OTP-based
TCP/IP upload

Key Server
(Public Health Authority)

TCP/IP download

local matching

Bluetooth



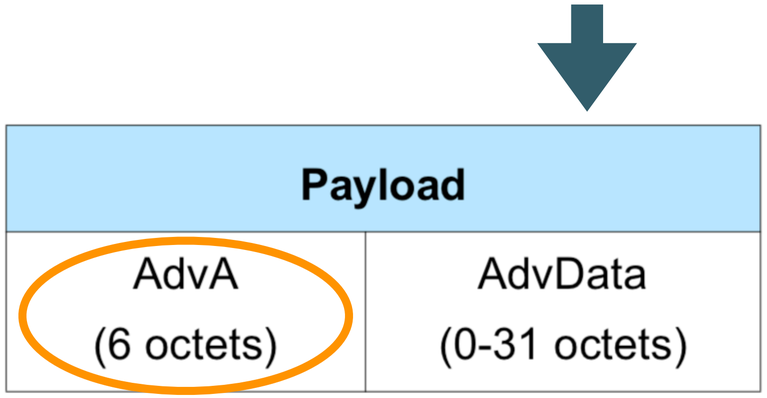
user phones

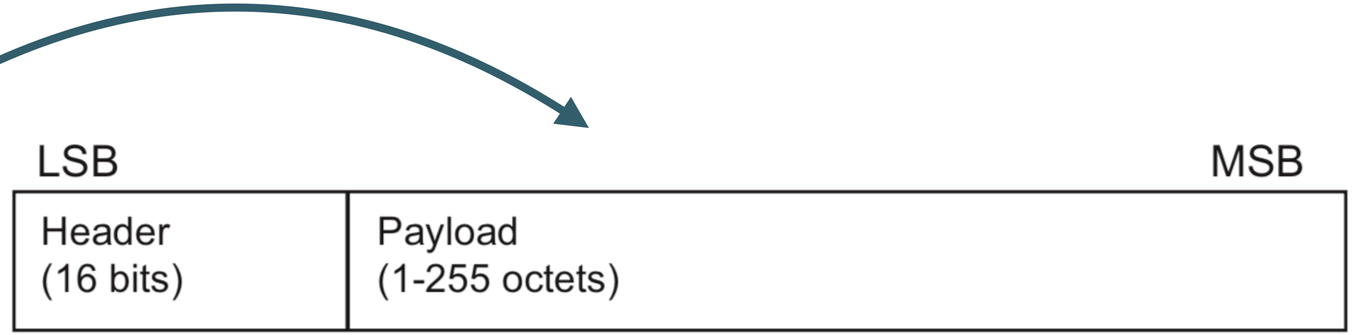
BLE Packet Payload

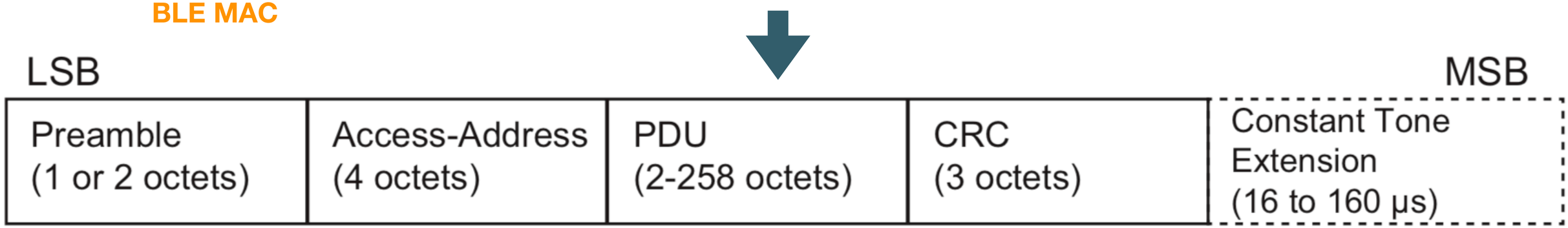
Flags			**Complete 16-bit Service UUID**			**Service Data - 16 bit UUID**				
Length	**Type**	**Flags**	**Length**	**Type**	**Service UUID**	**Length**	**Type**	**Service Data**		
0x02	0x01 (Flag)	0x1A	0x03	0x03 (Complete 16-bit Service UUID)	0xFD6F (Exposure Notification Service)	0x17	0x16 (Service Data - 16 bit UUID)	0xFD6F (Exposure Notification Service)	**16 bytes** **Rolling Proximity Identifier**	**4 bytes** **Associated Encrypted Metadata**

BLE Advertisement Packet Assembly

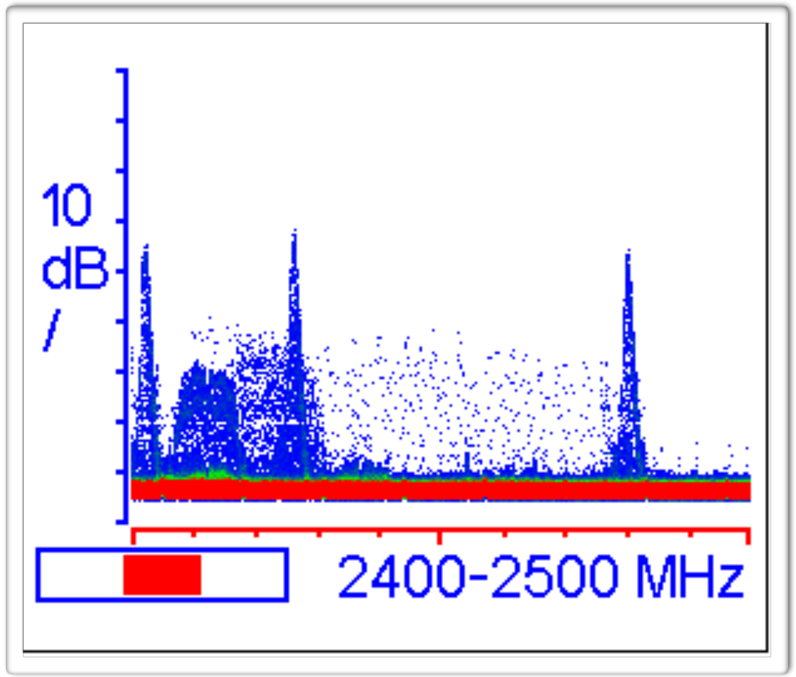
Flags			Complete 16-bit Service UUID			Service Data - 16 bit UUID				
Length	**Type**	**Flags**	**Length**	**Type**	**Service UUID**	**Length**	**Type**	**Service Data**		
0x02	0x01 (Flag)	0x1A	0x03	0x03 (Complete 16-bit Service UUID)	0xFD6F (Exposure Notification Service)	0x17	0x16 (Service Data - 16 bit UUID)	0xFD6F (Exposure Notification Service)	**16 bytes Rolling Proximity Identifier**	**4 bytes Associated Encrypted Metadata**





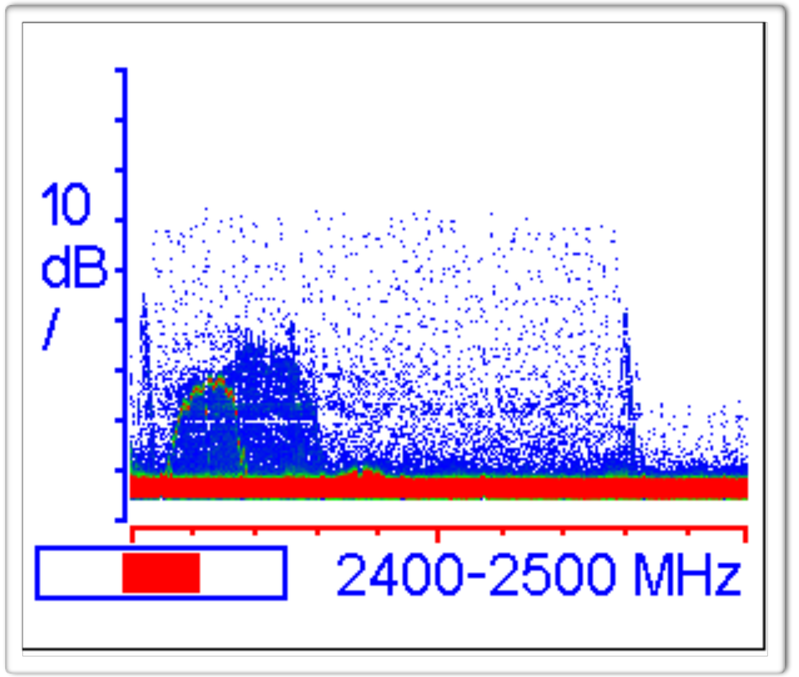


BLE Radio Spectrum



advertising

connection



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

All-to-Perimeter Exposure Tracing

- Besides instructing people to install the mobile application and follow its instructions, we can do more

  - install extra Bluetooth scanner(s) to capture the public anonymous advertisement packets in a broader perimeter area (up to cca 250 m radius for one scanner in free space)

  - download the temporary exposure keys on daily basis - the same way as regular mobile applications do

  - perform localised matching to disclose **the fluctuating number of risky encounters in the whole perimeter on timely basis**

  - these devices can also help to **detect large-scale radio attacks**, such as false alarms and suspicious jamming

Raspberry Pi Zero W Based Scanner - Alpha

Raspberry Pi Zero W Based Scanner - Beta (Autumn 2020)

Coalesced & Sorted Exposure Notifications (Bluetooth Channel)

```
(base) macwell:adv tom$ head -n 200 QTH-Petrovice/2020-11-12-1.adv | tail -n 20
1A03D3EC6CD84304E2E3BD6DFA0C77CB -90 239
1A2668643B886B303FF9083E44371CCF -87 11
1A44BF5486660A68CEE5BA27D8B3E906 -82 58
1AD6F166D46B9748F73427CF6E7CF6BF -89 6
1B166452EEA0A9B62C9415099D22FAD8 -84 9
1B5A04BAF5ED70FAC199E8206E3095D8 -76 242
1B640D0E9F06D389F1F0530348A16761 -84 4
1BA6A70850AA93A92001517E5FD41F5C -86 1
1BEB810145572B7792FAF73F0226D919 -77 32
1BF4CFBCCABD47807F4B5EB2E5CC4446 -88 1
1C06AA94E8C96CD1DAF5DE86CB632FB8 -67 4057
1C181C202CAA2C4F209050A07E6F1758 -65 3970
1C3913C6F995DC5B4AE2AD02669C8F1D -83 74
1C57A9FB507F86763E52616183783E9F -88 6
1CA6AC08440395652D67924657E7179B -81 29
1CD2130342B54EF950CFBD7F42F69C0D -79 166
1CDA8E4B863D6972730C28E47698A44B -83 16
1CEB5B083B53E615316D99671C428CED -87 16
1CFEAE6E0408A801E6A5A776C67EA7A6 -93 1
1D06E3C193367651A46DA4F0F2869557 -91 2
```

Daily Temporary Exposure Keys Export Batch

```
(base) macwell:cz tom$ ../../../bin/kfsp < 1605312000-1605398400-00001-export.bin | head -n 20
[+] -------- Temporary Key Export --------
[*] 2020-11-14 01:00 (local) 2020-11-15 01:00 (local) CZ 1 1
[+] --------
000162133CF00D3ADF63F97468F2E34E 2 2674080 [2020-11-04,01:00] 144 1 -5
0004E41FC86A5415A849D473BB90F363 2 2673792 [2020-11-02,01:00] 144 1 -10
001CDF6C7C6FEBF549638D7D0FE74C38 2 2674080 [2020-11-04,01:00] 144 1 -8
0058D9BCC9E088A9E09FABB7121428C1 2 2673792 [2020-11-02,01:00] 144 1 -10
005C9CB54881376634C1A2D0A7B6DE0D 2 2674800 [2020-11-09,01:00] 144 1 -3
007E8CA38BC363FADC33081CF4C82A70 2 2673936 [2020-11-03,01:00] 144 1 -8
00A03DD2B08EE4D4BEEE0C3740E281C0 2 2675376 [2020-11-13,01:00] 144 1 3
00A6A0A72A15C39DBA591AA07385B286 2 2673648 [2020-11-01,01:00] 144 1 -2
00CC1ACEE564E0EB7BCC48828152A30E 2 2674656 [2020-11-08,01:00] 144 1 -4
00DDFB94F975AD0FB81EFACD9FE73764 2 2673648 [2020-11-01,01:00] 144 1 -12
00FC55ED1B73C7B121E2D55BF6156F2A 2 2674224 [2020-11-05,01:00] 144 1 ?
010D1AE37D96F9200EC7E294294D0FF1 2 2674368 [2020-11-06,01:00] 144 1 0
01136CEB5905B105C94460F40038C2A7 2 2673936 [2020-11-03,01:00] 144 1 -9
0145ED6A53DCAF1B86E8D10EF6D96FDE 2 2674368 [2020-11-06,01:00] 144 1 -5
014973333D1FFD602488DB9375CBFF85 2 2674224 [2020-11-05,01:00] 144 1 -4
016665E391AF3BB563C9E9C5DB2844EB 2 2675088 [2020-11-11,01:00] 144 1 2
0178FF9829B6CCD0DB5E8A8364B2614B 2 2674944 [2020-11-10,01:00] 144 1 -2
```

Real Match

```
(base) macwell:cz tom$ ../../../bin/kfsp < 1605312000-1605398400…
...
7FC18B829AE9F91B0CA1870C5C253C8C 2 2673504 [2020-10-31,01:00] 144 1 -11
7FC206064BA6F5F9D666D16FF116E7E0 2 2674800 [2020-11-09,01:00] 144 1 0
7FCFB233659F5E79057F2CF5191A5D34 2 2674656 [2020-11-08,01:00] 144 1 -4
7FD5BC66FB6D59A6E16B3DEA7CE348D5 2 2674656 [2020-11-08,01:00] 144 1 -4
...
```

daily key export

```
(base) macwell:adv tom$ cat QTH-Petrovice/2020-11-09-1.adv
...
035A6EC1C5916B1B881C6ADC273C46FE -92 4
03F82E7A6A3951E0EA27200F2C8B31EB -84 1
0415DFE65EACD88769BD33B9CCC4A42D -82 25
042AF6B7C44131B721147D83BADCDA34 -83 14
...
1F324B33C004BA505A78BC8DE8FAE3B5 -82 96
1F3C10FC4025FB6166DA0A7190AC033E -83 223
1F3C963CA5B177D0B4F
...
24211A70A7969270A39
2480BE59291D66698DB
24C616A59E08DCDE9BE
24D5BD7E8CB3AC70BA2
...
```

Bluetooth scan

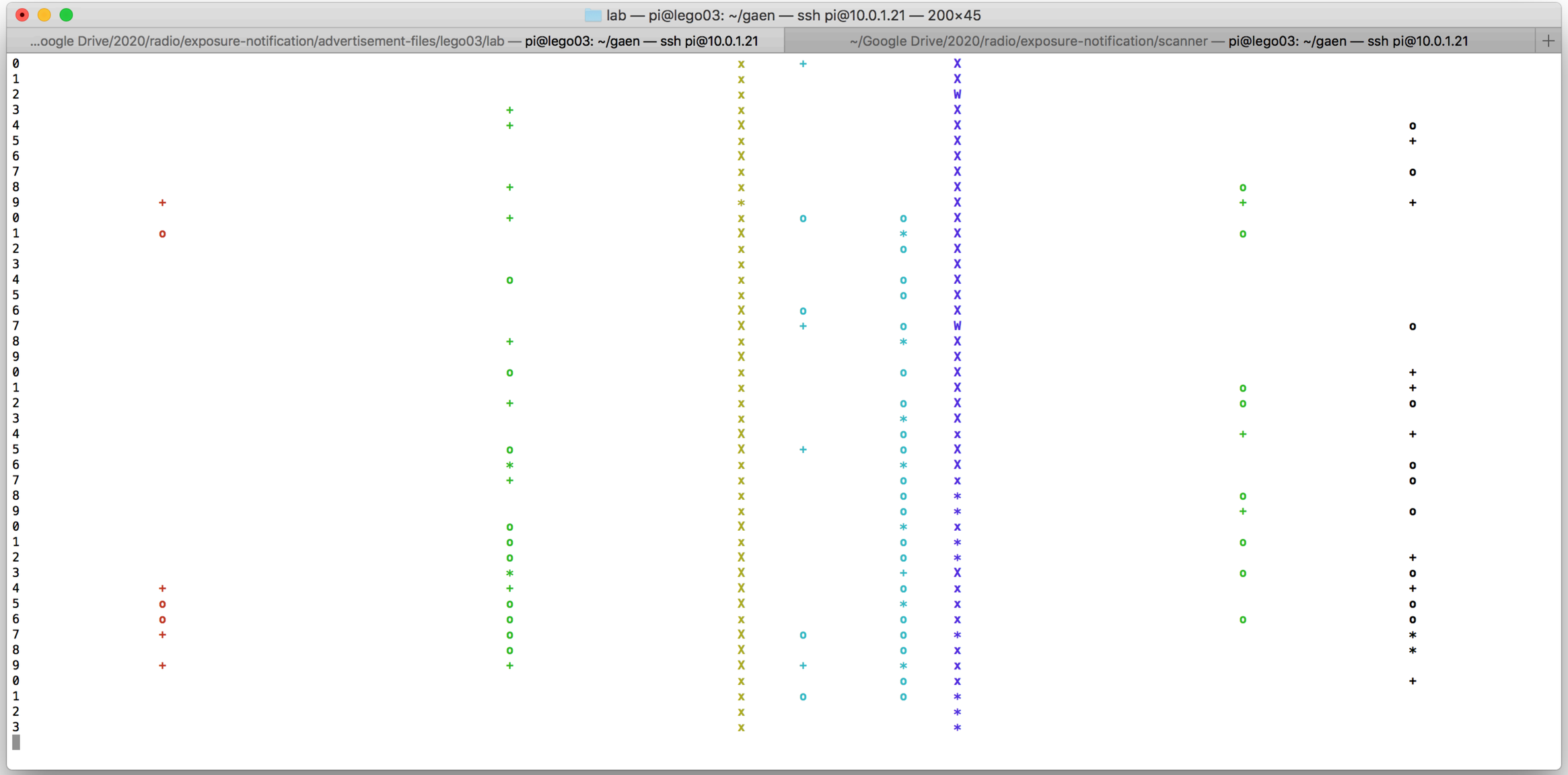
derive

compare

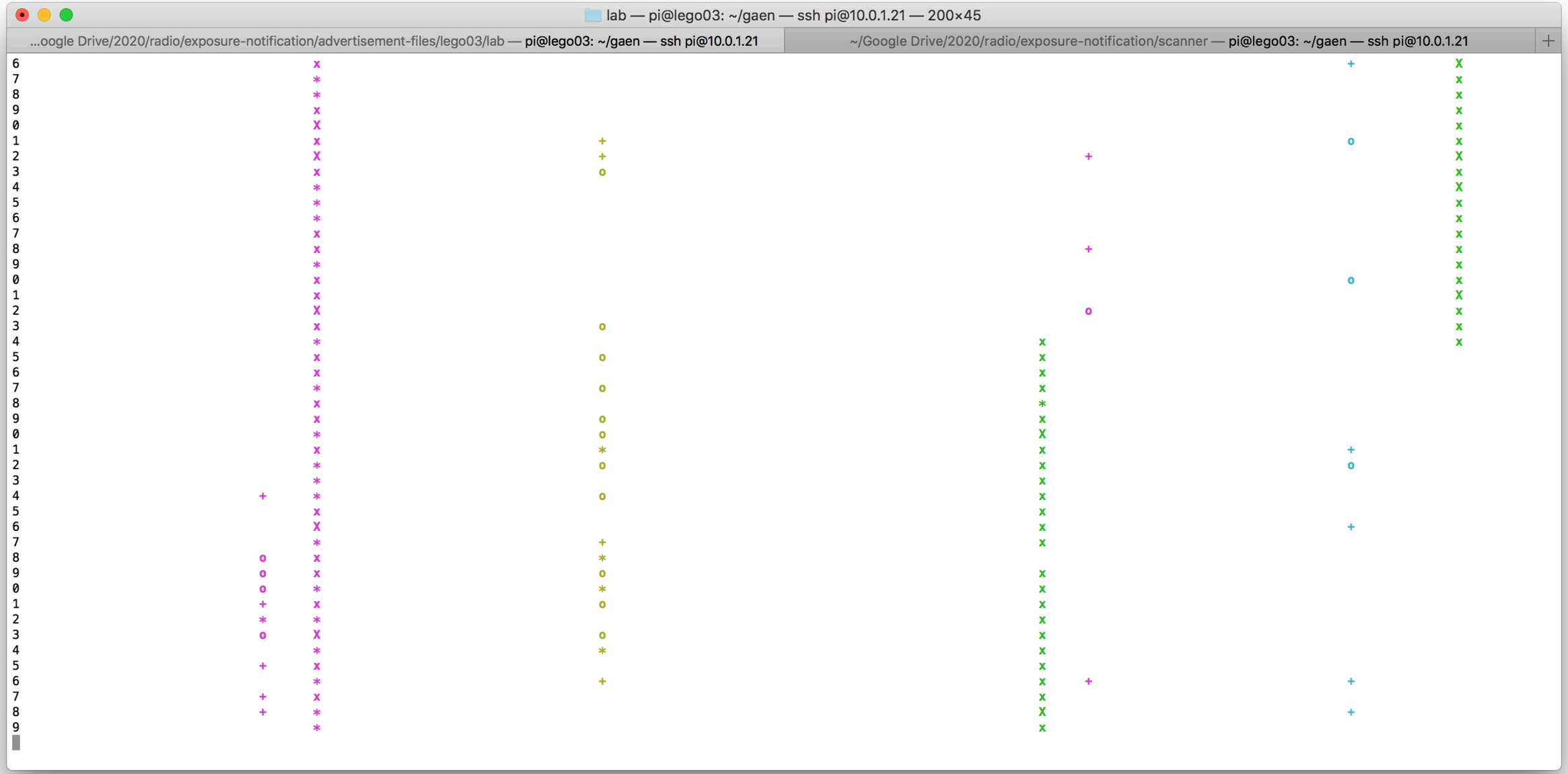
```
(base) macwell:cz tom$ rpigen 7FC206064BA6F5F9D666D16FF116E7E0 2674800 144 …
...
52278574C5AC961A255B78AFC3EA1E81 5165918E 2674809 [2020-11-09,02:30] 7FC2060…
2480BE59291D66698DBE2CA96374C0DB 56899872 2674810 [2020-11-09,02:40] 7FC2060…
076F3AEDFEA4359A6A5326111ABC0EC4 4C324595 2674811 [2020-11-09,02:50] 7FC2060…
1F3C10FC4025FB6166DA0A7190AC033E 9FDA7FD3 2674812 [2020-11-09,03:00] 7FC2060…
ABF3B6D6C75C7A9A98BE8760FE2A7B85 BF9D4341 2674813 [2020-11-09,03:10] 7FC2060…
03F82E7A6A3951E0EA27200F2C8B31EB 5B418588 2674814 [2020-11-09,03:20] 7FC2060…
764AEDB26481CECF7FB506AD04E71B8E FC8F9D2D 2674815 [2020-11-09,03:30] 7FC2060…
...
```

rolling proximity identifiers

RADAR-like Traces



RSSI [dBm]	< -97	-97..-88	-87..-78	-77..-68	-67..-58	-57..-48	-47..-38	> -38
Symbol	.	+	o	*	x	X	W	@



RSSI [dBm]	< -97	-97..-88	-87..-78	-77..-68	-67..-58	-57..-48	-47..-38	> -38
Symbol	.	+	o	*	x	X	W	@

RSSI Model

- Let RSSI denote the value provided by the Read RSSI Command via BLE HCI.
- Basing on the formula derived above, we can write:

$$RSSI(d) = RSSI(d_0) - 10n\log\frac{d}{d_0} + X$$

  - d_0 denotes the calibration distance,
  - n is a model parametrisation constant (n = 2 in the free space), referred to as the *attenuation factor*
  - X is a random variable covering fluctuations

Privacy Unfriendly Tracing

```
B7FD84CABD33BBA2A8C63E6F3543C0F5 2 2674944 [2020-11-10,01:00] 144 1 -12
184654C1FEFCC438F1AA3E96EE583570 2 2675088 [2020-11-11,01:00] 144 1 -11
569D45C1496DA0621DB59C2EAC1C4DA8 2 2675520 [2020-11-14,01:00] 144 1 -8
36625AFD45BEE8B9284DAC70F1A34E67 2 2676096 [2020-11-18,01:00] 144 1 -4
```

TEK export batch

```
B874ABD699E626F9157B042BDB318EB8 28BE9DCD 2675003 [2020-11-10,10:50] B7FD84CABD33BBA2A8C63E6F3543C0F5
7D7A86C9C9AF7E6A11A535A84791715E 6AB69909 2675012 [2020-11-10,12:20] B7FD84CABD33BBA2A8C63E6F3543C0F5
D2DD38C040C28F97FAE8CD00D46902C3 0F34D0E5 2675031 [2020-11-10,15:30] B7FD84CABD33BBA2A8C63E6F3543C0F5
9BC7A4973870B4E318133D699F50B9BE F31393AE 2675032 [2020-11-10,15:40] B7FD84CABD33BBA2A8C63E6F3543C0F5
73256A76764EE1153BF51173FFC17132 C8E01768 2675035 [2020-11-10,16:10] B7FD84CABD33BBA2A8C63E6F3543C0F5
C51037B69F3B8F8DB5DB6429AA06A241 8CBDCDBB 2675140 [2020-11-11,09:40] 184654C1FEFCC438F1AA3E96EE583570
F736701ABB9EAD8EE4F10A4E2D56CBC0 CE5D6D7E 2675159 [2020-11-11,12:50] 184654C1FEFCC438F1AA3E96EE583570
9FE961D758776D10417C371DE1ABD953 84C1E820 2675160 [2020-11-11,13:00] 184654C1FEFCC438F1AA3E96EE583570
6F71F3D60849D692567F32B7818BF1EB B2F5DB50 2675606 [2020-11-14,15:20] 569D45C1496DA0621DB59C2EAC1C4DA8
241E8453D776B64D050AC14974E7F121 9E4DEE2E 2676148 [2020-11-18,09:40] 36625AFD45BEE8B9284DAC70F1A34E67
```

coalesced Bluetooth log match

```
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001929 S -89
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001930 S -86
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001931 S -83
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001931 S -88
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001933 S -89
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001933 S -91
4F:2B:2A:5A:EF:2F B874ABD699E626F9157B042BDB318EB874579DCD 1605001933 S -87
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007834 S -91
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007836 S -94
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007841 S -89
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007841 S -84
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007842 S -87
60:12:E7:07:81:94 7D7A86C9C9AF7E6A11A535A84791715E365F9909 1605007843 S -84
```

Bluetooth uncut log (snippet)

1605001929 ~ 2020/11/10 10:52:09 (local)

1605007834 ~ 2020/11/10 12:30:34 (local)

delta increments are in seconds

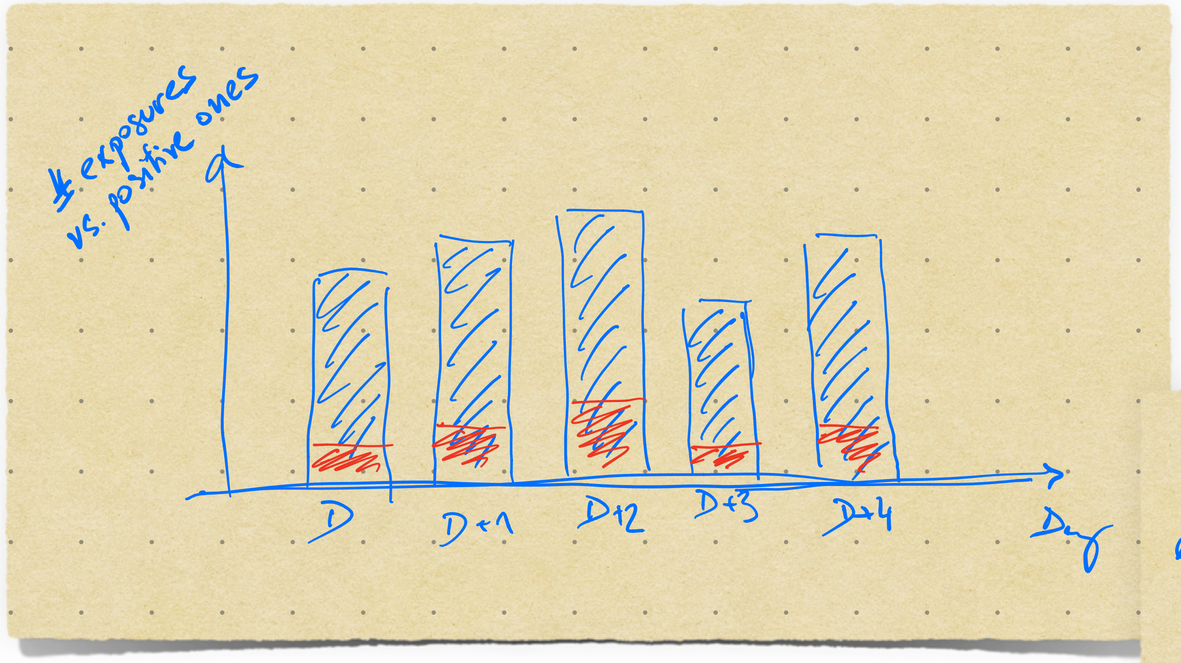
By the way: OTP Security

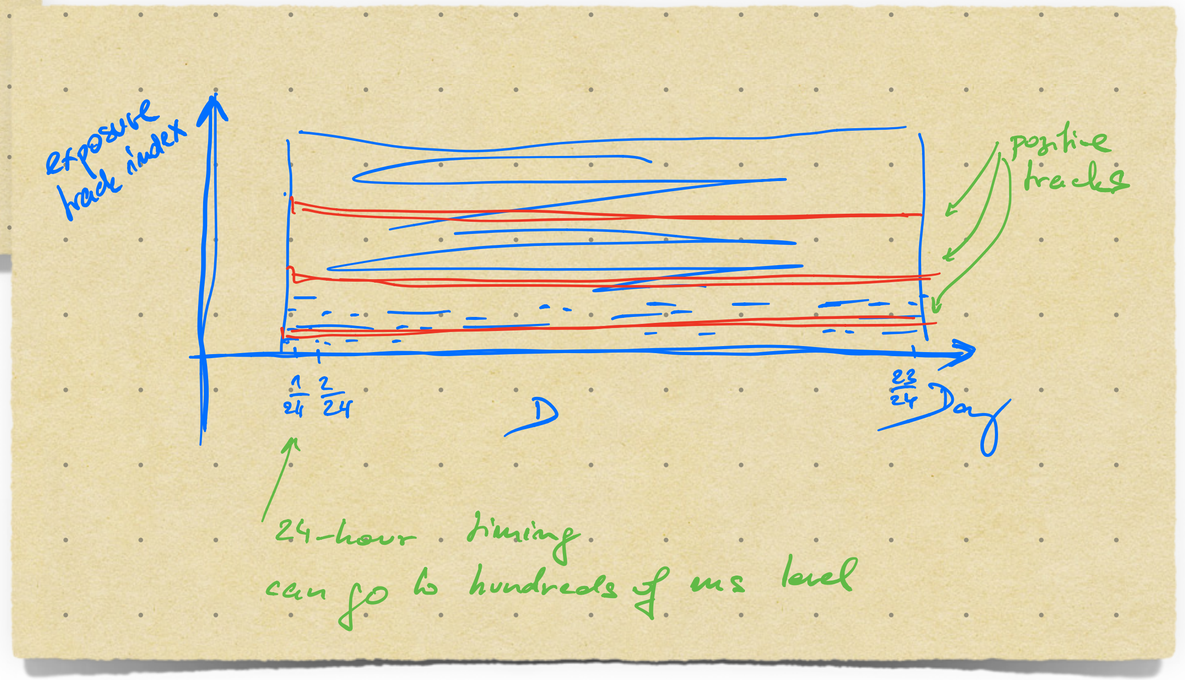
- One-time password required for the exposure keys upload
  - valid OTP allows for easy TEK pullout (tracing) and large-scale false alarms (poisoning)
- OTP of 8 decimal digits observed
  - if there is just one valid OTP ready to use, the success probability of a random guess is expected to be $\mathbf{10^{-8}}$
  - if there would be, however, 10^4 OTP ready to use, this probability then grows to $\mathbf{10^{-4}}$
  - so, this authentication mechanism does not scale securely

GAEN Threats and Vulnerabilities Summary (*probably incomplete*)

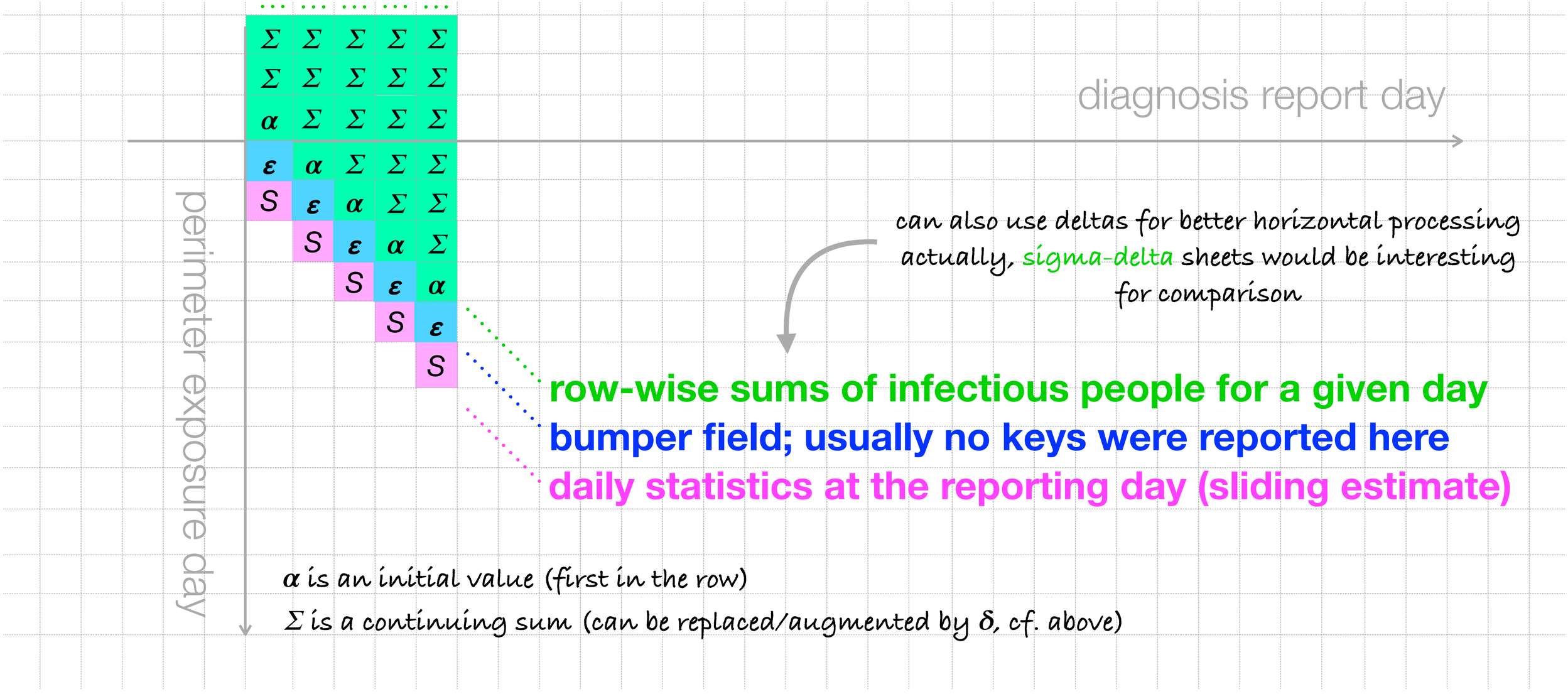
- **Massive false alarm - pretending fictional super spreading events by a relay attack or OTP brute-forcing**
- **Jamming - hiding real super spreading events**
- **Privacy breach**
  - RADAR like tracking and recognition of kinetic activity in a given perimeter
  - RIP rollback (time-shift regeneration) and TEK pullout attacks in general
  - individual trace and activity reconstruction after TEK public exposure
  - social patterns - Who Acquires Infection From Whom (WAIFW), etc.

Observing Localised Exposure Risk Factors (workbench ideas)





Office Exposure Field and Its Anonymous Updates



Thank you for your attention

Přednášející:	**Tomáš Rosa**
Společnost:	**Raiffeisen BANK, CBCC**
E-mail:	**easy to guess**

CYBER SECURITY CONFERENCE 2022

CYBER SECURITY CONFERENCE 2022

PANELOVÁ DISKUZE

TRENDY V INFORMAČNÍ BEZPEČNOSTI

Revision History

- 2022/06/07 ~ public release at Security 2022