Představení Brmlabu

Pavel Růžička <ruza@ruza.eu>

Pracovní skupina CSIRT

14.11.2016

Kdo jsem

Pavel Růžička

- `https://ruza.eu/linkedin`
  - Administrátor a IT security konzultant
- `https://ruza.eu/brmlab`
  - předseda spolku a zakládající člen

brmlab, obecné info

- Spolek financovaný z členských příspěvků
  - Předseda spolku - statutární orgán
  - Rada spolku - administrativa, PR, atd
  - Revizní komise - kontrolní orgán
  - Grantová komise - interní granty
  - členská základna a valná hromada
- Počet členů cca 50
- VŠ studenti, lidé z IT praxe, OSVČ, začínající podnikatelé
- první hackerspace v ČR (od r.2010)

brmlab hackerspace prague

Hackerspaces ve světě

`http://hackerspaces.org`

> *Hackerspace je komunitně založený fyzický prostor, kde lidé sdílejí zájem o technologie, setkávají se a pracují na svých projektech, a učí se navzájem.*

- 2106 registrovaných ve wiki celkem
- 1309 aktivních
- 351 plánovaných

`https://wiki.hackerspaces.org/List_of_Hacker_Spaces`

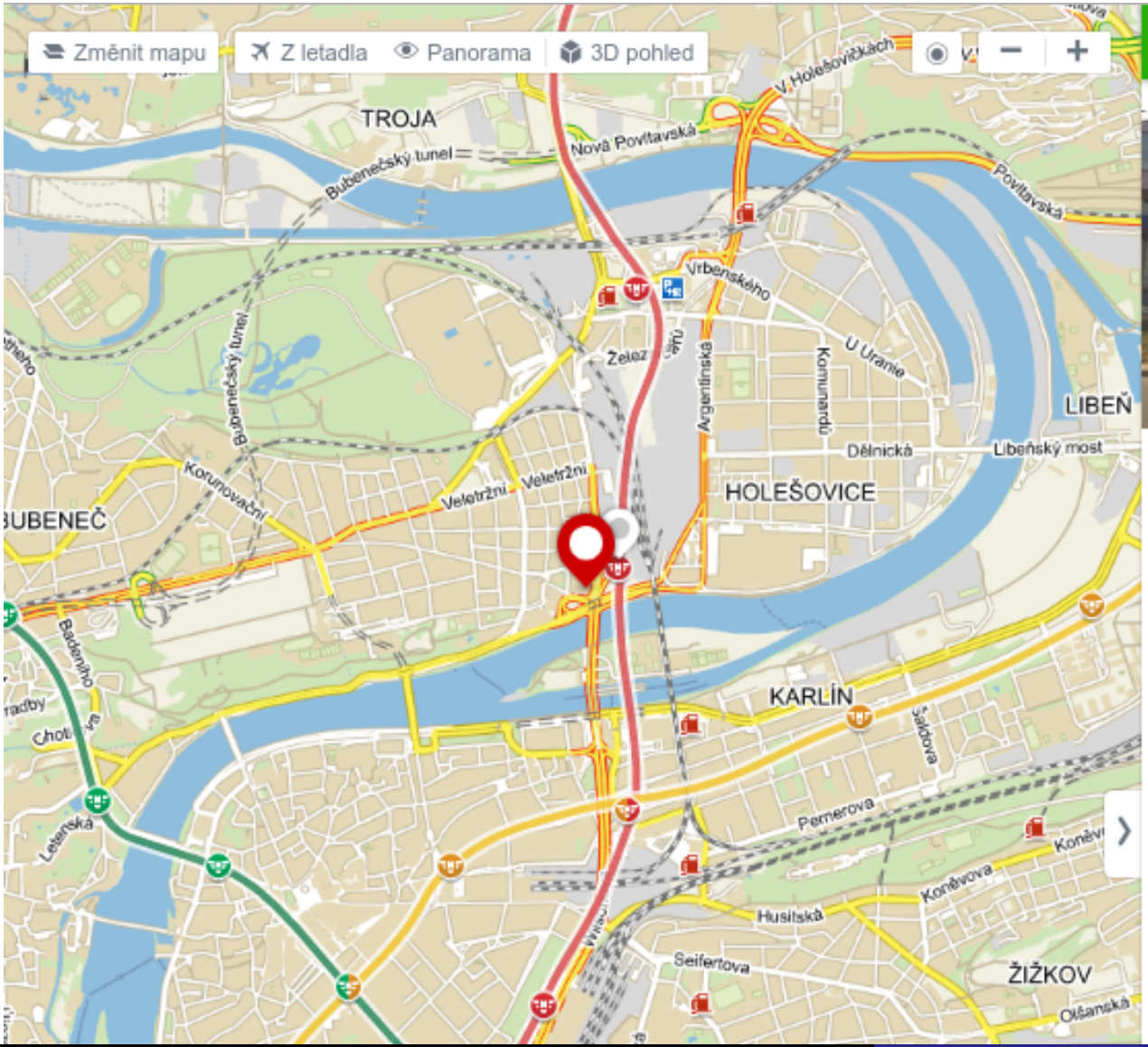
brmlab hackerspace prague

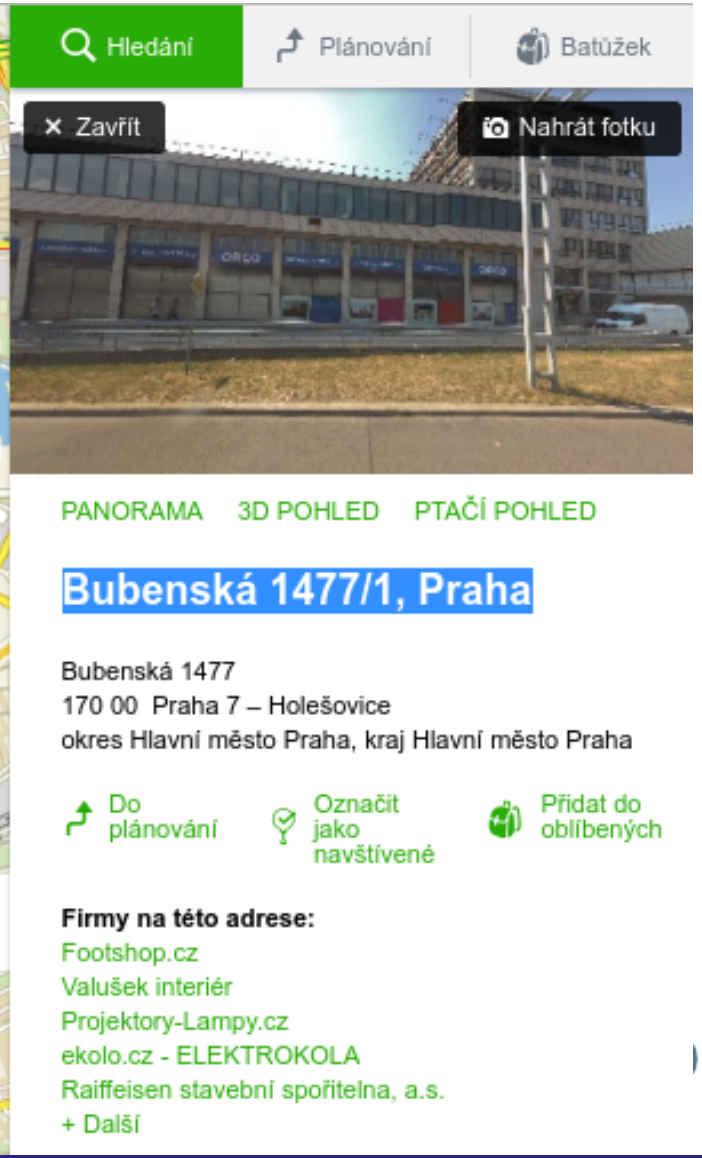
Hackerspace v České republice

- Brmlab, Prague `https://brmlab.cz`
- Cryptoanarchy institute, Prague `http://www.paralelnipolis.cz`
- MacGyver, Prague `http://macgyver.siliconhill.cz`
- Base48, Brno `http://base48.cz`
- Labka, Ostrava `https://labka.cz`
- PiSeC, Pisek `http://www.kufr.cz`
- Pardubice Hackerspace, Pardubice `http://hackerspacepardubice.cz`

brmlab hackerspace prague

brmlab, Bubenská 1477/1, Praha (=M= Vltavská)

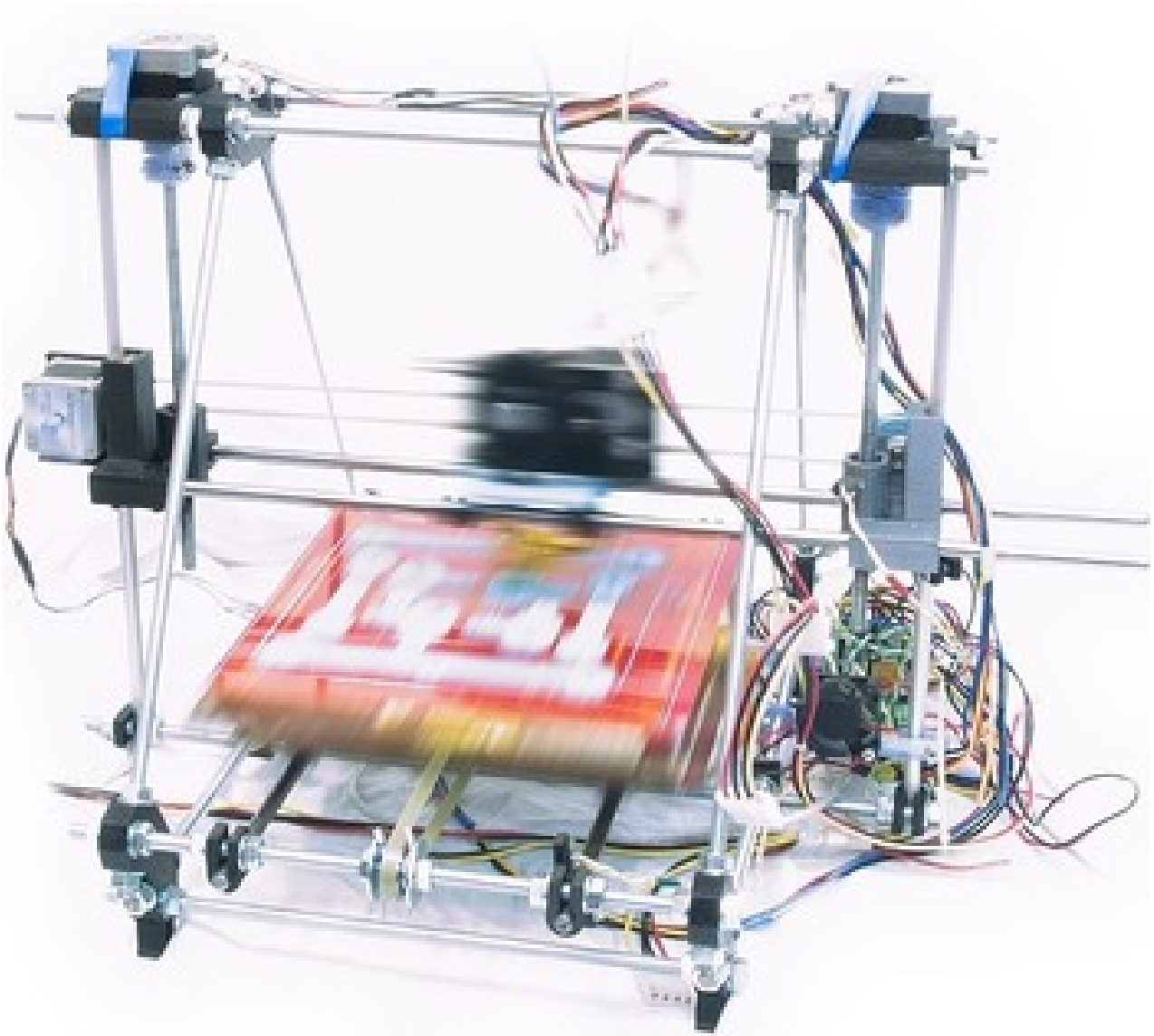




Soc(ial) room

Soc(ial) room

HW lab, 3D tisk

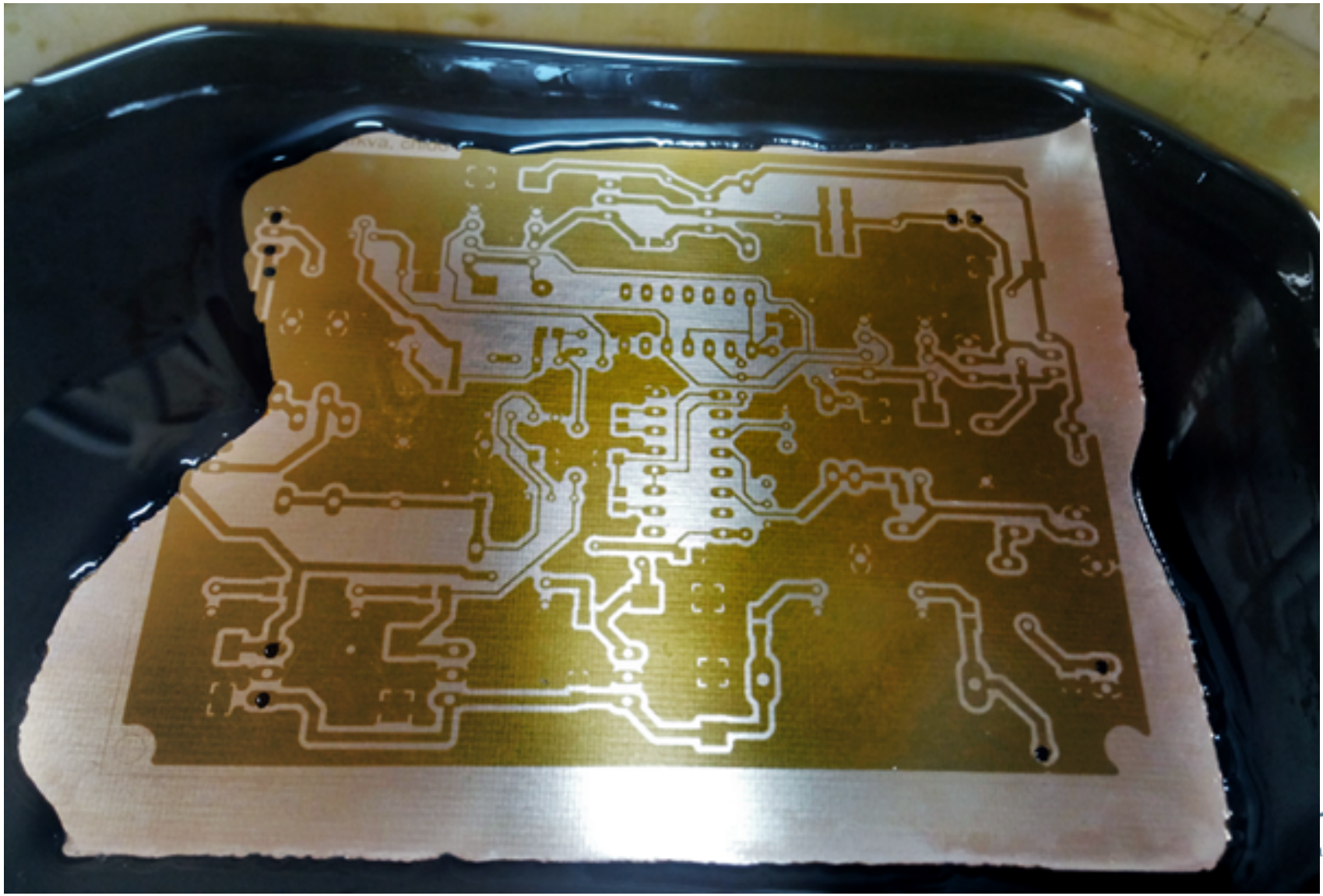


HW lab

HW lab

Spolupráce na řešení

Výroba desek plošných spojů



Brmdoor (systém řízení přístupu na RFID)

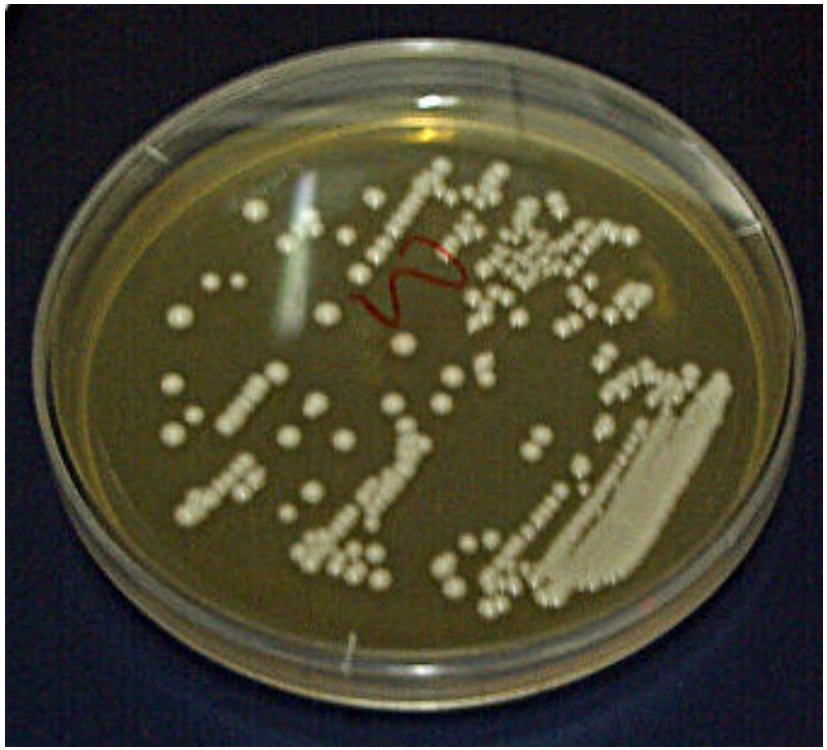
brmlab hackerspace prague

Chemlab

Biolab

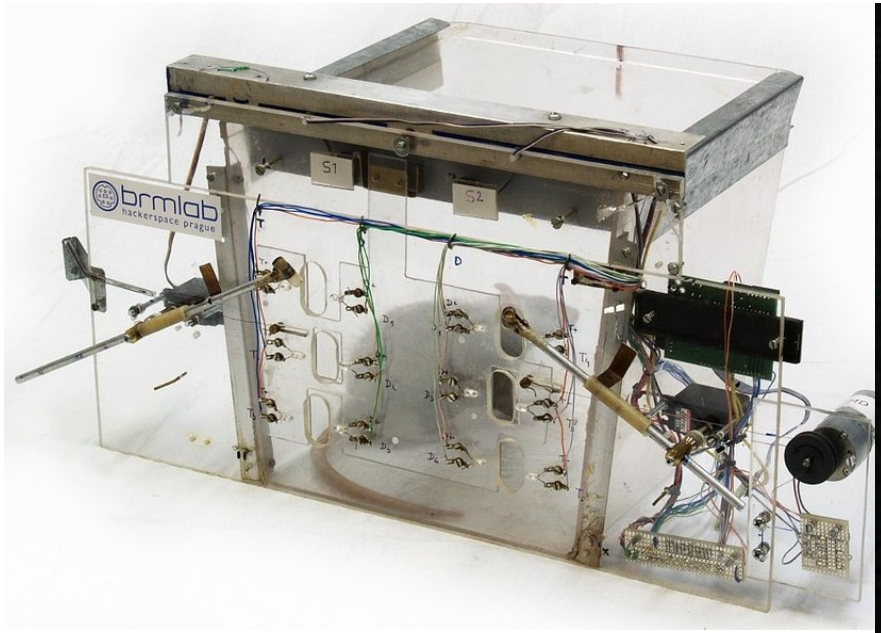
Biolab

Biolab

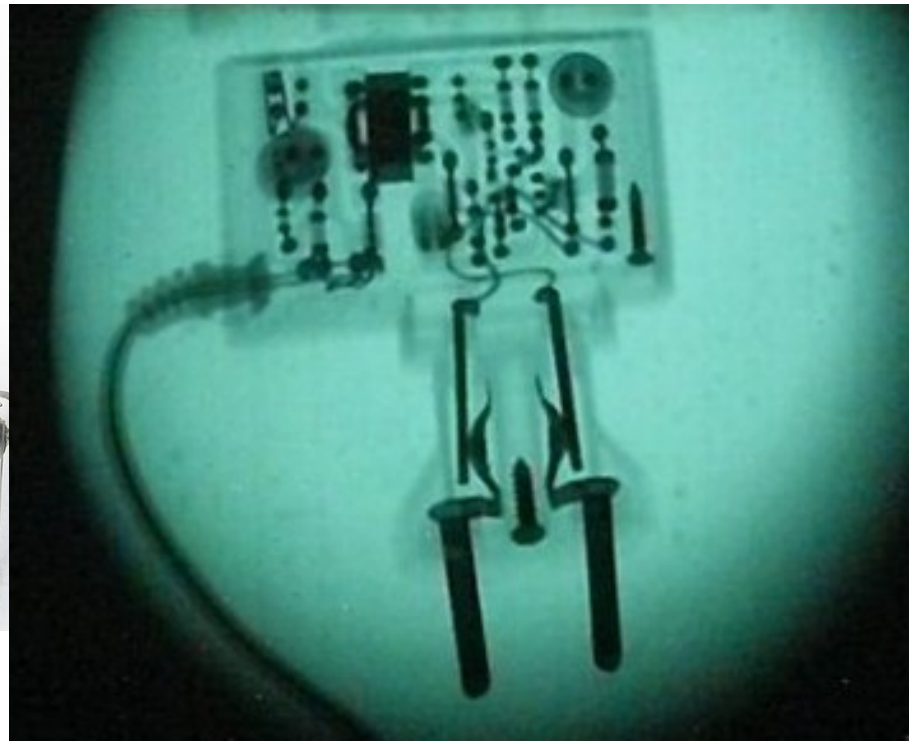


pěstování kultur, mikroskopie, sekvencování DNA, elektrofyziologie, biofeedback

Biolab

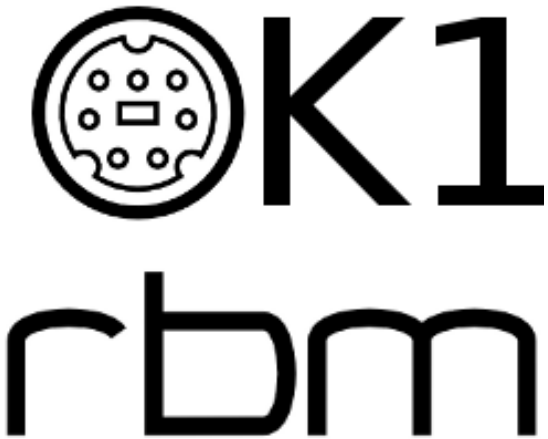


behaviorální výzkum



rentgen

OK1RBM aka Radiolab



Od **listopadu 2014** je brmlab oficiálně registrovaným **radioamatérským klubem**

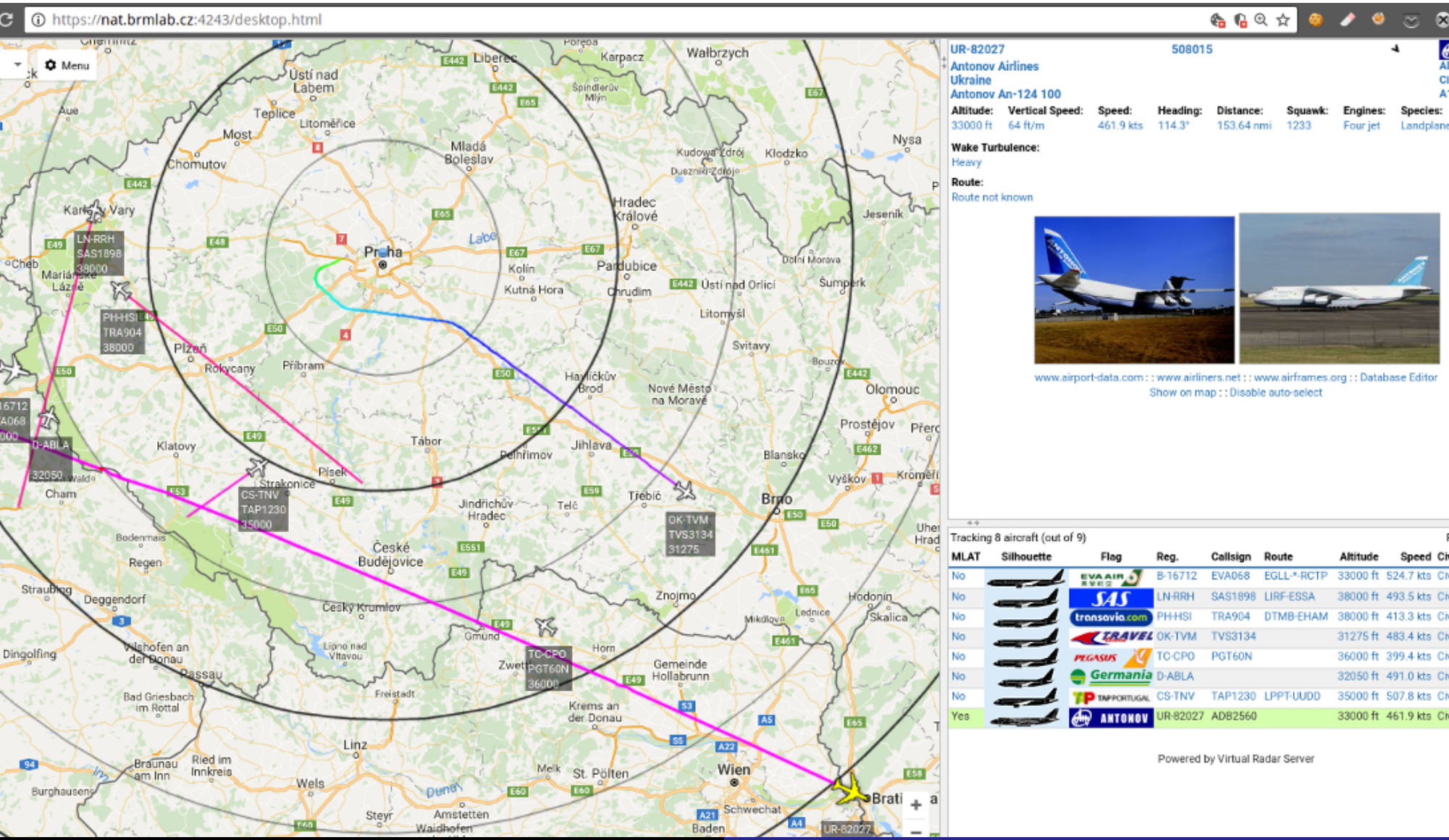
Činnostem spočívajícím v aktivním vysílání na radioamatérských pásmech se věnuje spíše okrajově, hlavní náplní je predevším **výzkum a vzdělávání v oblasti radiových komunikací** obecně a v brmlabu je toto v různých podobách dlouhodobě populárním a aktivním tématem.

`http://ok1rbm.cz`

brmlab hackerspace prague

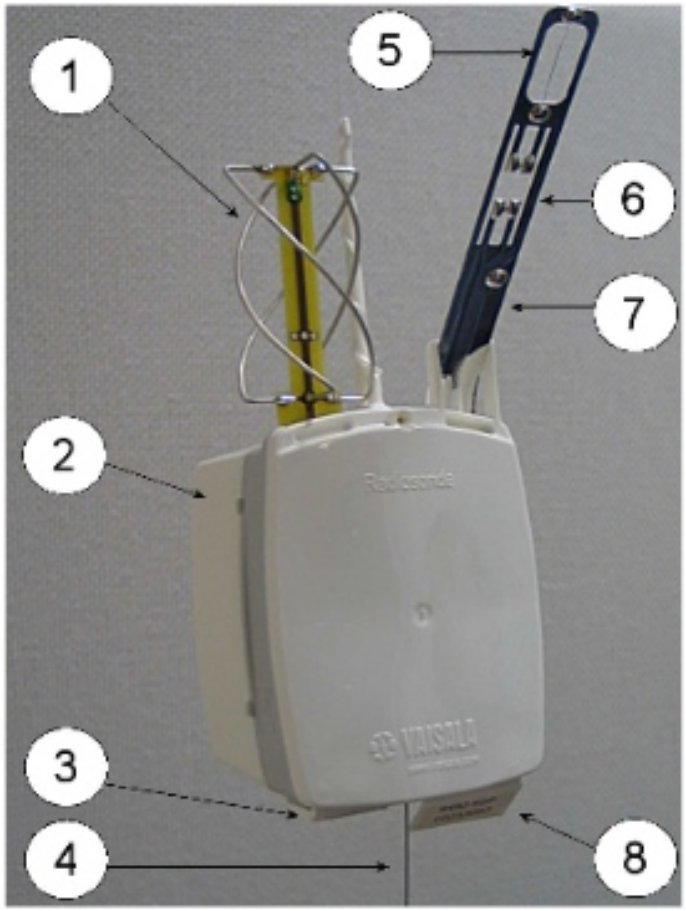
Radiolab

OK1RBM - ADSB (https://nat.brmlab.cz:4243/desktop.html)

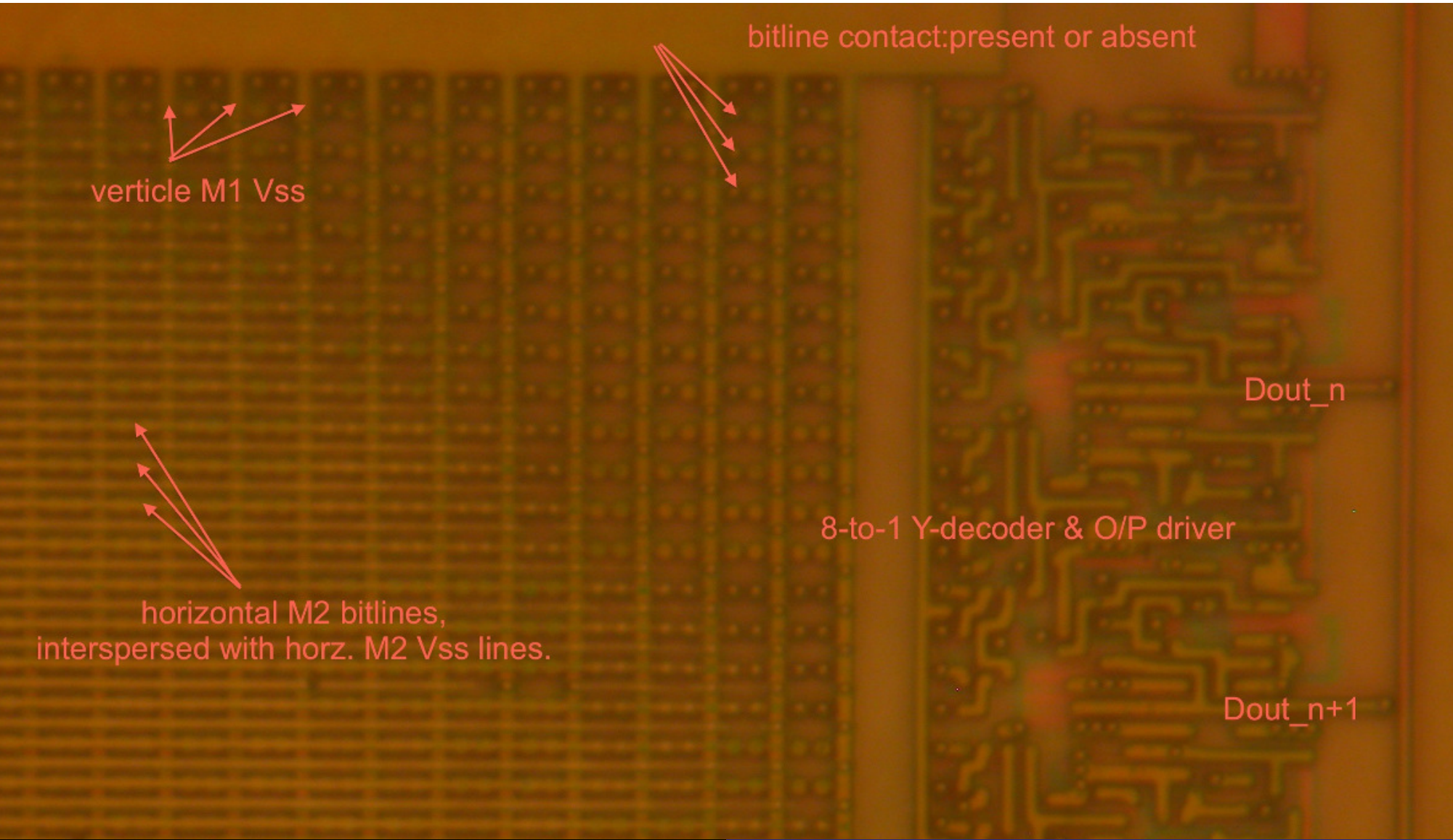


OK1RBM - SSTV

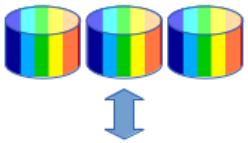
OK1RBM - Lovení meteo sond



OK1RBM - Reverzní inženýrství



Bezpečnost GSM sítí



endpoint computation → rainbow table lookup → chain finalization

kraken or deka
A5/1 cracker

brmbora
multichannel radio sniffer (hardware)

sniff

guessed keystream

napalmex
cracker client
keystream guesser

recovered secret states

cracked keys

find_kc
A5/1 backclocking

stats.db
precomputed plaintext heuristics

gsm_convert
raw data processor
keystream guesser

decrypted signalling

decrypted SMS

decrypted calls

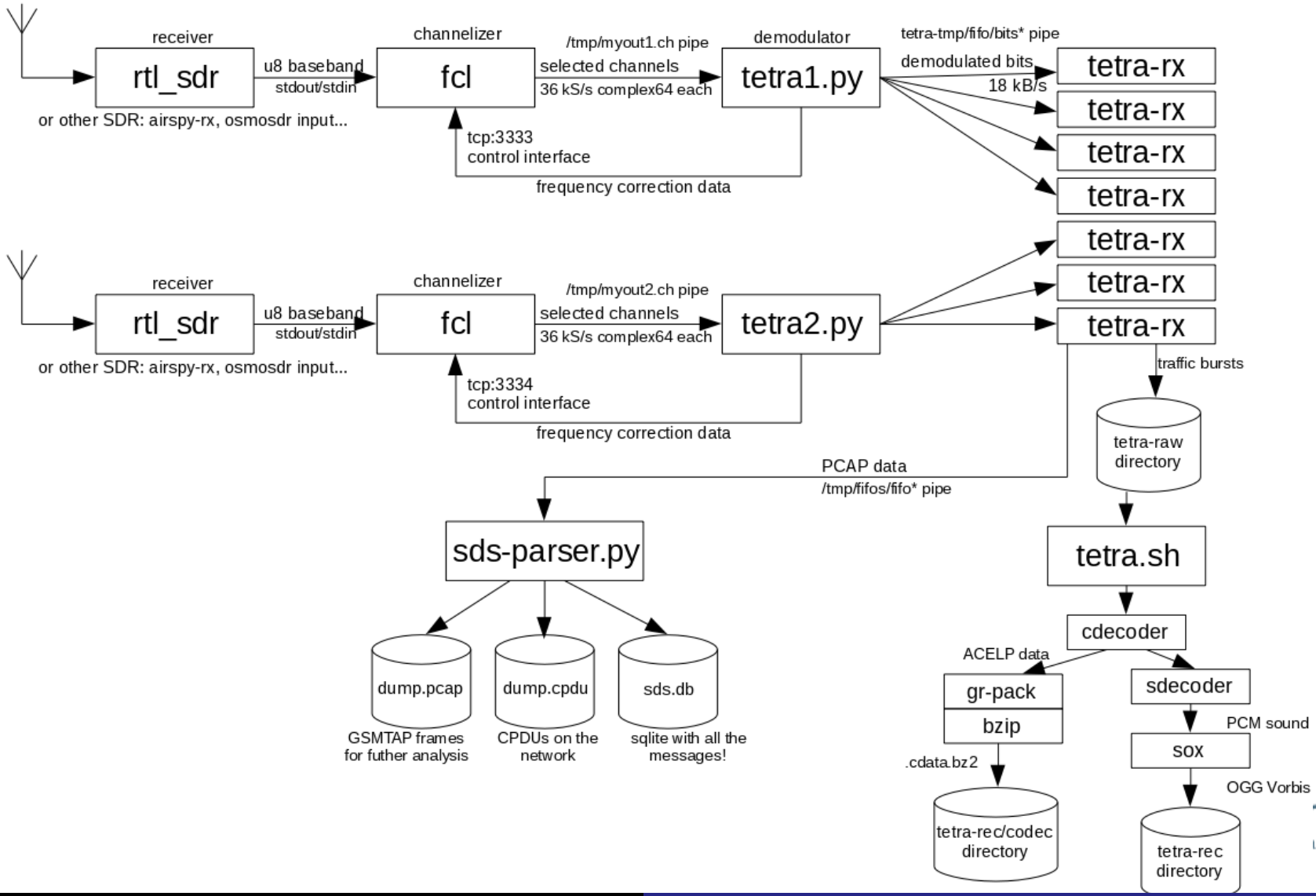
encrypted data

encrypted data

session directory
captured communication and metadata

© NSA Litoměřice, 2010-2013

Bezpečnost Městských Radiových sítí TETRA



Systémy řízení přístupu

- RFID
- NFC
- magnetic cards
- MIFARE cards
- FAB/physical keys, lockpicking
- smartcards
- etc

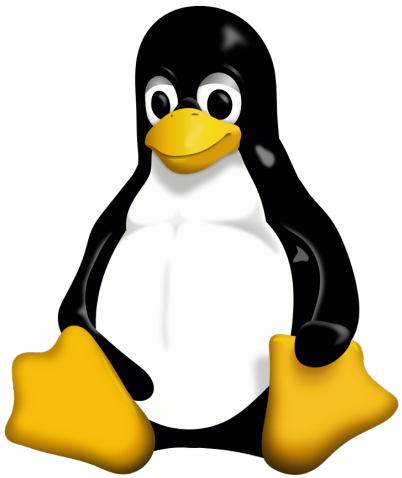
Přednášková činnost, konference

- Installfest - SDR, Efektivní implementace útoku na šifru A5/1
- CTJB - Reverzování NFC karet
- Europen - SDR, Machine learning, distribuované systémy
- Chaos Communication Camp - BTC Trezor, package signing, clipboard insecurity
- brmlab - https://brmlab.cz/video

Vývoj software

- FCL channelizer - výkonější než GnuRadio
- Tetrapol-kit - open source SW přijímač a decoder
- Kukuruku - open source SDR klient
- GnuRadio patche
- rapid prototyping - open source SW & HW, 3D tisk, arduino, apod.

Operační systémy



brmlab hackerspace prague

Společenská témata

- **2600 meetingy** - celosvětově organizovaná setkání “u piva o bezpečnosti“
- V návaznosti na zjištění v rámci brmlabího projektu zkoumajícího Městské Rádiové Sítě (MRS) v září 2016 upozorňuje Pirátská strana medializací na nedostatky v zabezpečení radiokomunikačních sítí **TETRA** v lokalitě Praha
- vyjádření ke **kauze zveřejnění emailů** premiéra serverem White-media
- vyjádření k prohlášení ministra vnitra o nutnosti **identifikace uživatelů** Internetu
- podpora iniciativy **“Přichází cenzor”** sdružení CZ NIC
- podpora “Joint Statement **against Radio Lockdown**” organizace “Free Software Foundation Europe” (omezení možnosti nahrávání alternativních firmware)
- **analýza leaku** Hacking team pro media

BRM-CSIRT

Hackerspace a CSIRTy jsou organizace, zabývající se počítačovou bezpečností a mohou se vzájemně obohatit. Některým tématům se už věnujeme:

- vuln/artifact analysis, response
- technology watch
- education/training

brmlab hackerspace prague

Další info...

BRM-CSIRT: `https://csirt.brmlab.cz`
Projekty: `https://brmlab.cz/project`
Další foto: `http://nat.brmlab.cz/phtagr/explorer/`