

## Představení Brmlabu

Pavel Růžička <ruza@ruza.eu>



Pracovní skupina CSIRT

14.11.2016







# 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, Písek**  
<http://www.kufr.cz>
- **Pardubice Hackerspace, Pardubice** <http://hackerspacepardubice.cz>



# Soc(ial) room











# HW lab



# Spolupráce na řešení





# Brmdoor (systém řízení přístupu na RFID)



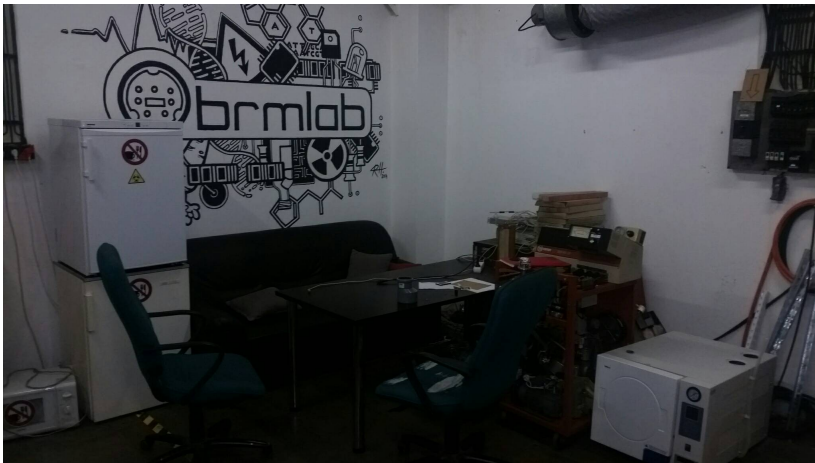


# Biolab





# Biolab



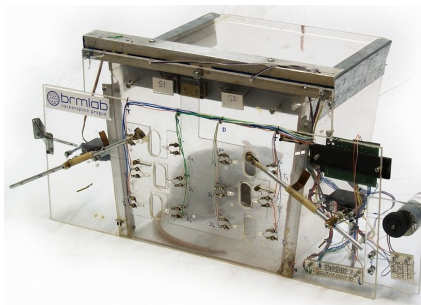
# Biolab



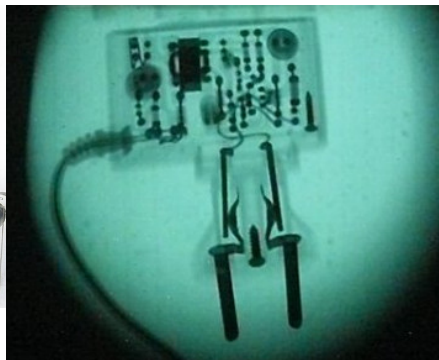
pěstování kultur, mikroskopie,  
sekvencování DNA,  
elektrofyzologie, biofeedback



# Biolab

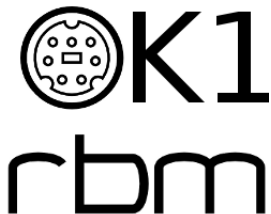


behaviorální výzkum



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 především **výzkum a vzdělávání v oblasti radiových komunikací** obecně a v brmlabu je toto v různých podobách dlouhodobě populárním a aktivním tématem.

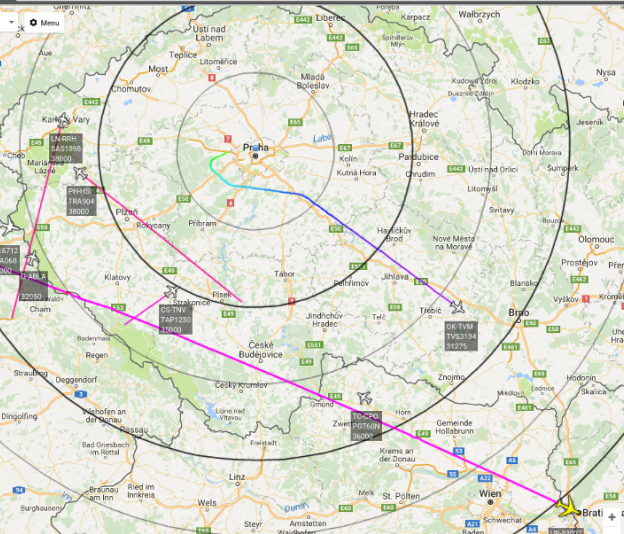
<http://ok1rbm.cz>

# Radiolab



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

https://nat.brmlab.cz:4243/desktop.html



UR-82027 508015  
 Antonov Airlines  
 Ukraine  
 Antonov An-124 100  
 Altitude: 33000 ft Vertical Speed: 64 ft/m Speed: 461.9 kts Heading: 114.3° Distance: 153.64 nmi Squawk: 1233 Engines: Four jet Species: Landplane

Wake Turbulence: Heavy

Route:  
 Route not known



www.airport-data.com :: www.airlines.net :: www.airframes.org :: Database Editor  
 Show on map :: Disable auto-select

Tracking 8 aircraft (out of 9)

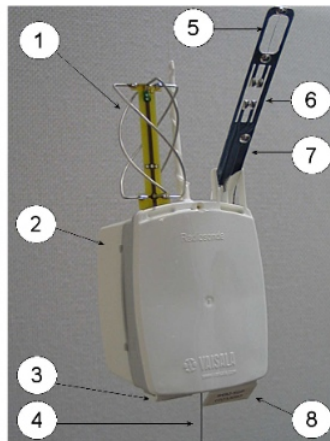
MLAT	Silhouette	Flag	Reg.	Callsign	Route	Altitude	Speed	Ch
No			B-16712	EVA068	EGLL-RCTP	33000 ft	524.7 kts	Ch
No			LN-RRH	SA51398	LIRF-ESSA	38000 ft	493.5 kts	Ch
No			TRA904	DTMB-EHAM	38000 ft	413.3 kts	Ch	
No			OK TVM	TVS3134		31275 ft	483.4 kts	Ch
No			PGT60N	TC-CPO	PGT60N	36000 ft	399.4 kts	Ch
No			D-ABLA			32050 ft	491.0 kts	Ch
No			CS-TNV	TAP1230	LPFF-UUDD	35000 ft	507.8 kts	Ch
Yes			UR-82027	A082560		33000 ft	461.9 kts	Ch

Powered by Virtual Radar Server

# OK1RBM - SSTV

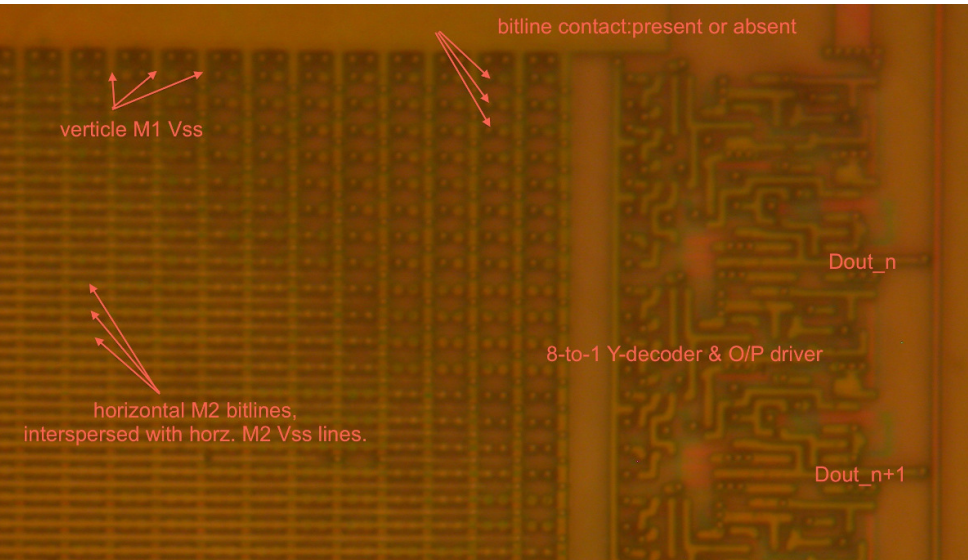


## OK1RBM - Lovení meteo sond





# OK1RBM - Reverzní inženýrství



verticle M1 Vss

bitline contact:present or absent

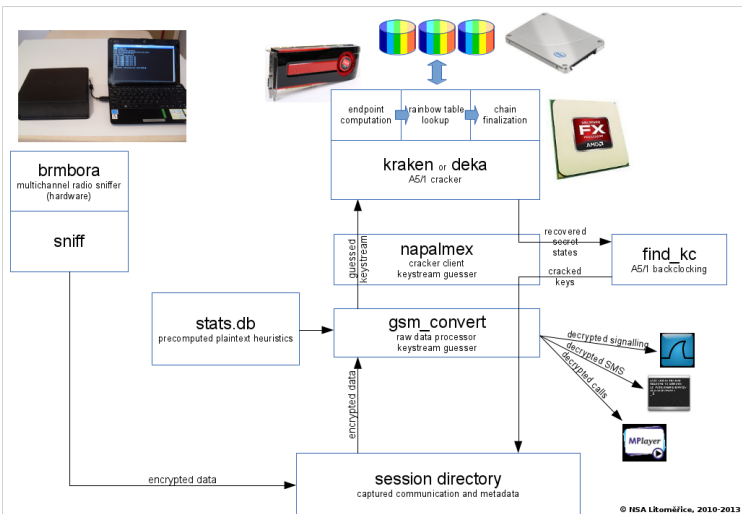
Dout\_n

8-to-1 Y-decoder & O/P driver

Dout\_n+1

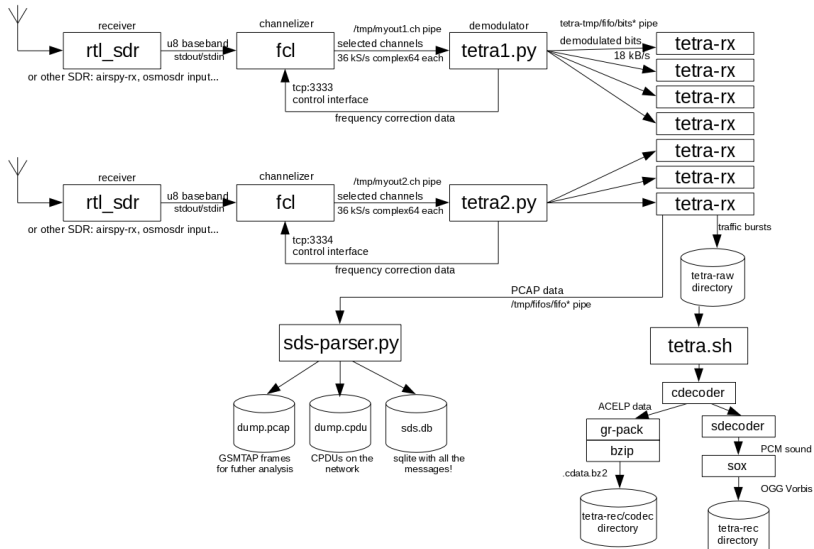
horizontal M2 bitlines,  
interspersed with horz. M2 Vss lines.

# Bezpečnost GSM sítí



© NSA Litoměřice, 2010-2013

# Bezpečnost Městských Radiových sítí TETRA



# Systémy řízení přístupu

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

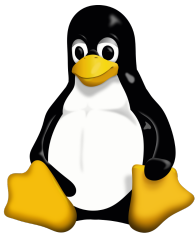
# Přednášková činnost, konference

- 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



## Společenská témata

- **2600 meetingy** - celosvětově organizovaná setkání “u piva o bezpečnosti“
- V návaznosti na zjištění v rámci brmlabího projektu zkoumajícího Městské Rádiové Síť (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



# Komerční spin-offy, General bytes s.r.o.

## BTC ATM









