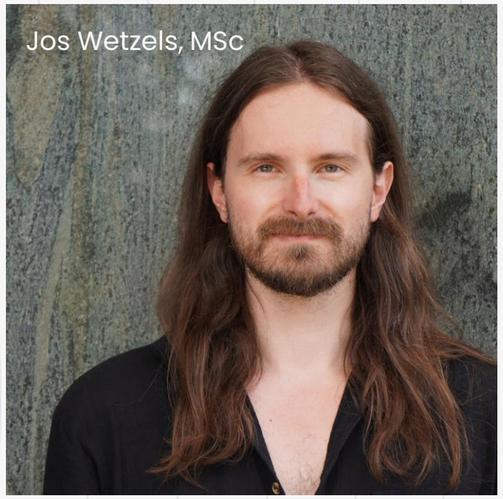
MIDNIGHT
BLUE

December 2023

ALL COPS ARE BROADCASTING

TETRA unlocked after decades in the shadows

By Midnight Blue



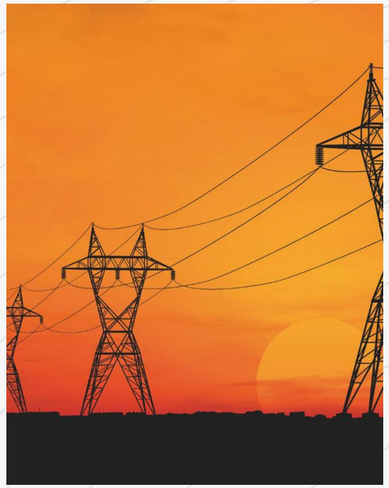
Midnight Blue

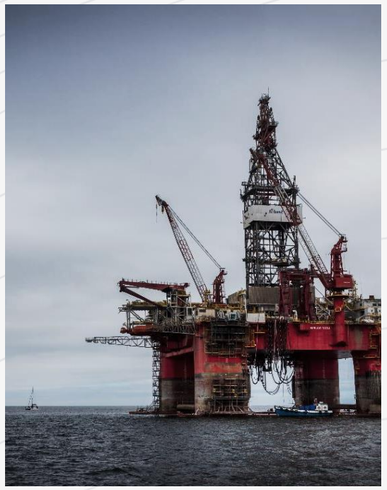
New content

- Deanonymization attack (+demo)
- Details on how cryptographic backdoor spread through Europe + implications for critical infra
- Vendor misinformation
- New TETRA developments!

What is TETRA?

- Globally used radio technology
  - Competes with P25, DMR, TETRAPOL
- Standardized in 1995 by ETSI
  - Known for GSM, 3G/4G/5G, GMR, etc.
- Used for voice & data communications incl. machine-to-machine
- Relies on secret, proprietary cryptography

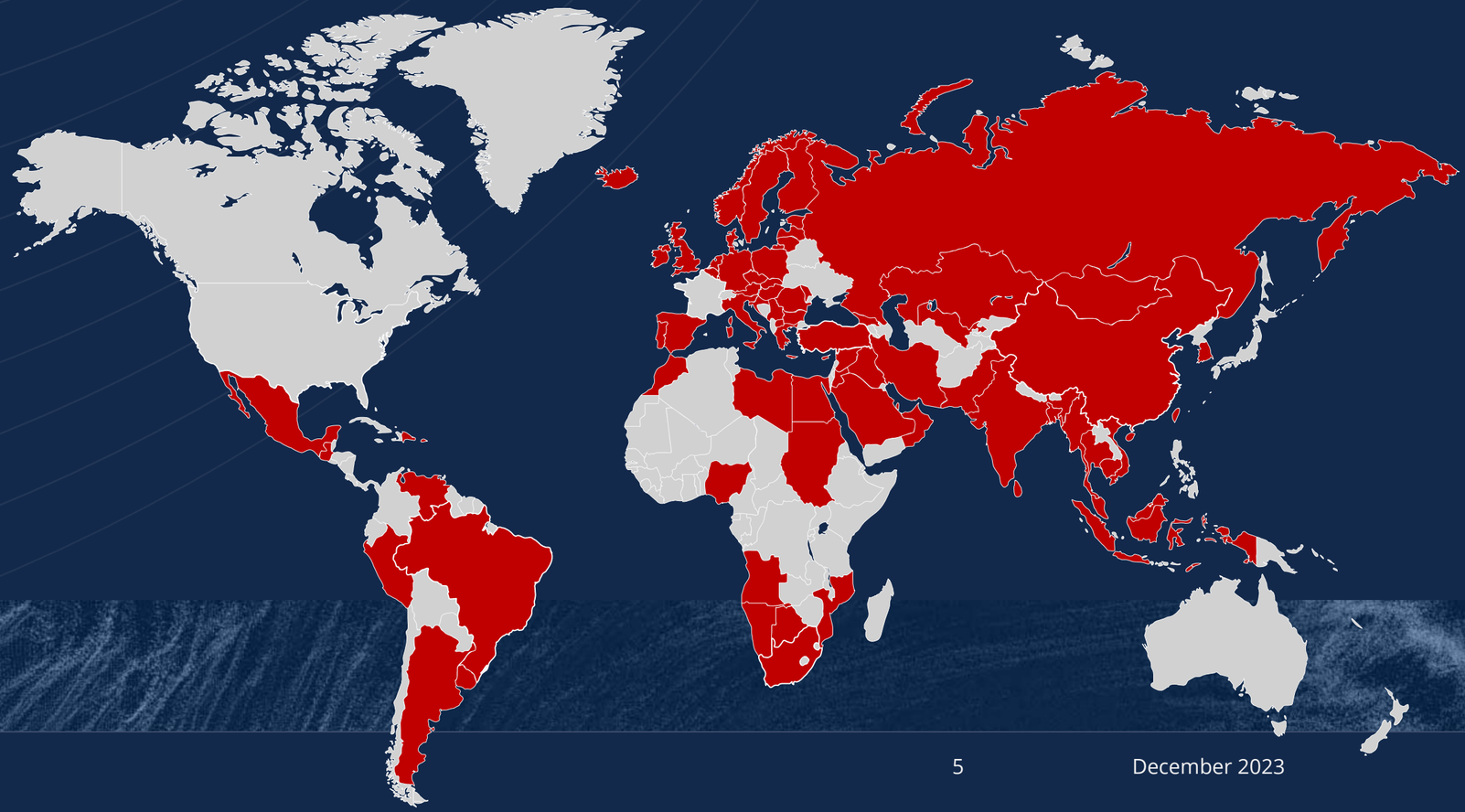




Use by police

Vast majority of global police forces use TETRA radio technology.

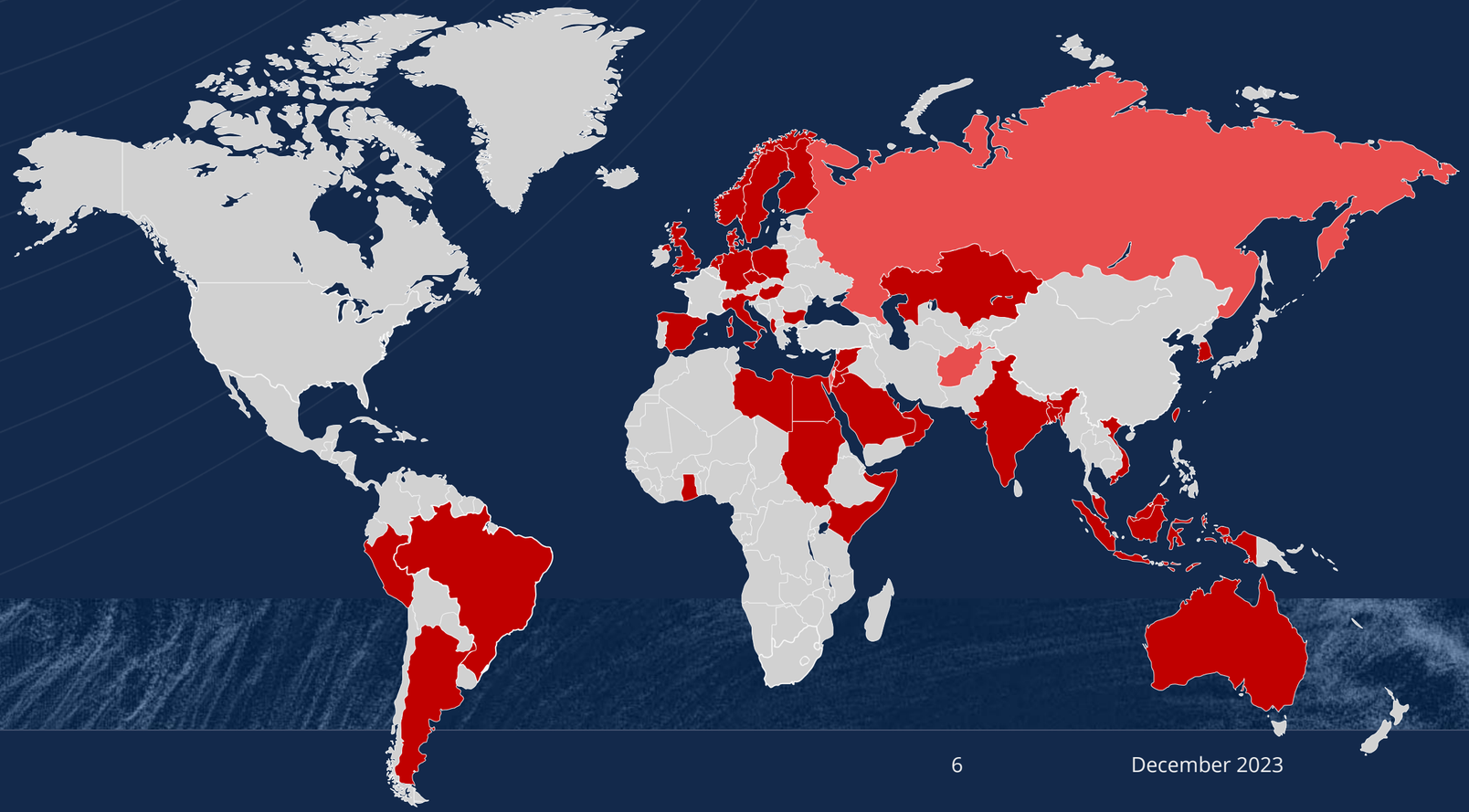
- C2000 (NL)
- ASTRID (BE)
- BOSNET (DE)
- AIRWAVE (UK)
- Nødnett (NO)
- Rakel (SE)
- SINE (DK)
- VIRVE (FI)
- SIRESP (PT)
- …



Based on OSINT

Military & Intelligence

Many countries have one or more military or intelligence units using TETRA radio technology as primary, fallback, or interfacing comms.

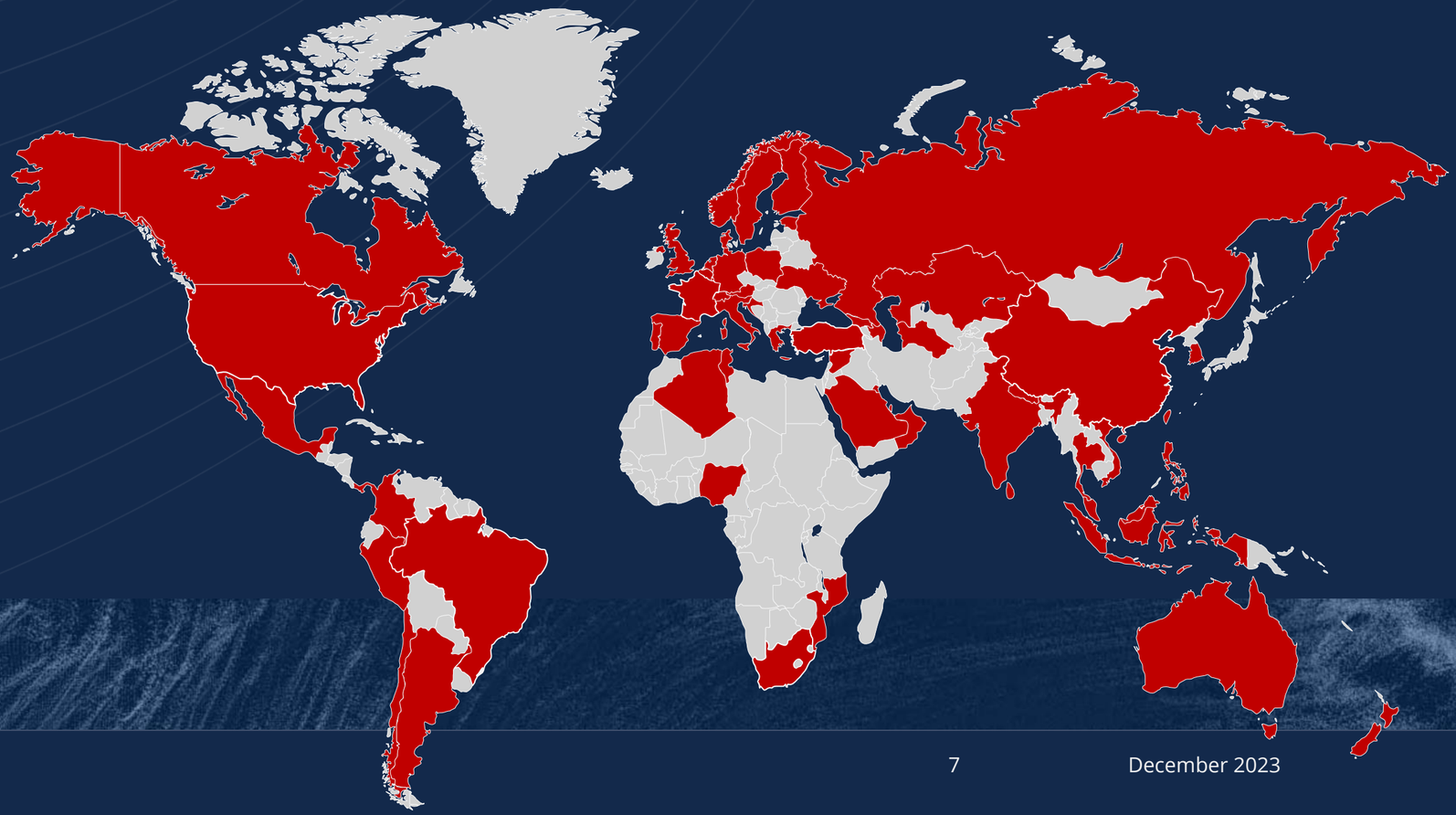


Based on OSINT

Critical Infrastructure

Many parties such as airports, harbors, and train stations use TETRA for voice communications.

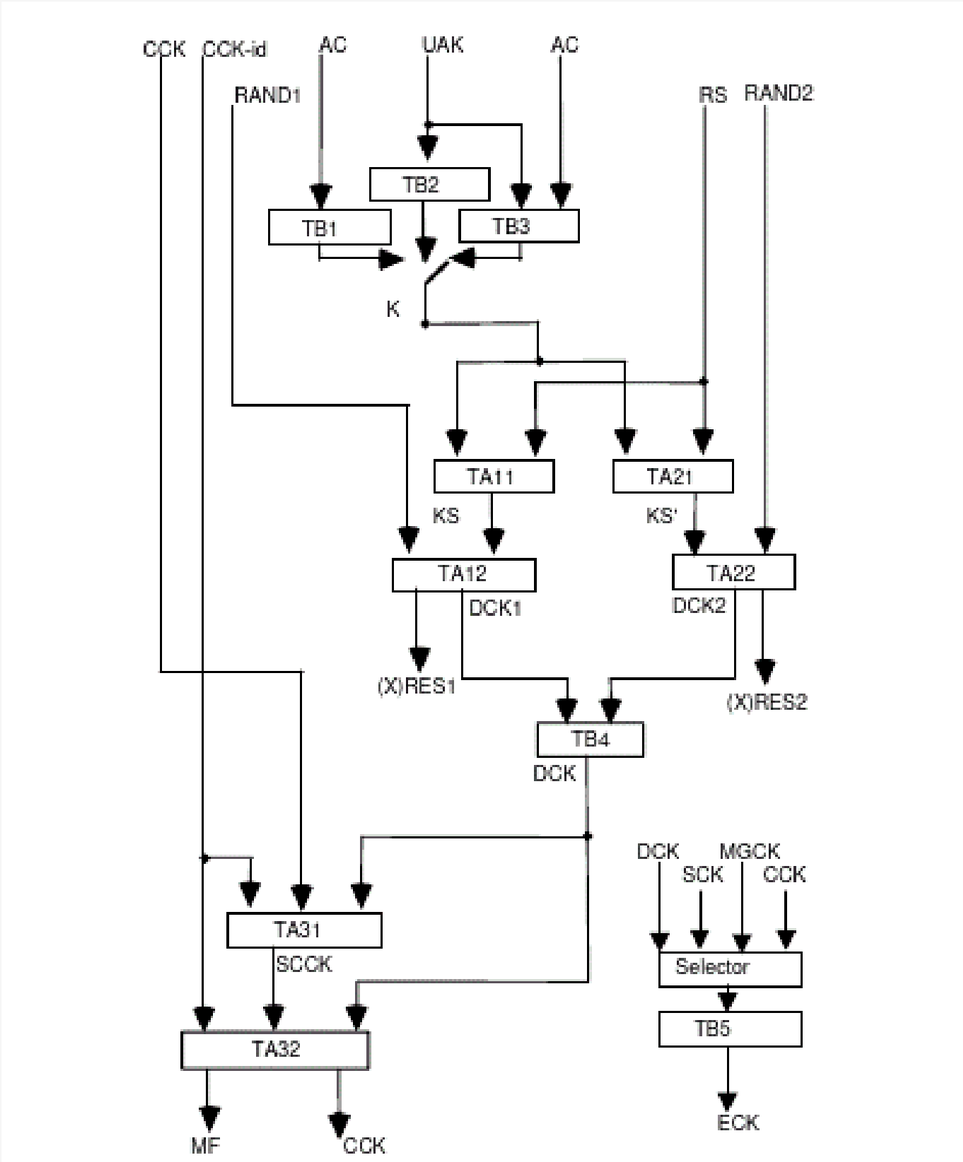
In addition TETRA is used for SCADA WAN, such as substation & pipeline control, or railway signalling.



Based on OSINT

Open standard?

- Public standard, secret crypto
  - NDAs, only available for ‘bona fide’ parties
- Manufacturers must protect algorithms
  - Hardware, or, implementations
  - Software with extraction countermeasures



ıre B.1: Overview of air interface authentication and key management (sheet 1

Lots of ‘bona fide’ vendors

Significant amount of geographically dispersed players

Top-tier adversaries likely have specs (e.g. via in-country manufacturers or theft)

Historical M&As

Teltronic, Simoco → Sepura, Nokia → Airbus, Rohde & Schwarz, PowerTrunk → Hytera, Selex ES → Leonardo, Chelton → Cobham, Artevea → dissolved.

TETRA security

- **TAA1 suite**
  - Authentication, key management / distribution (OTAR)
  - Identity encryption
  - Remote disable

- **TEA (TETRA Encryption Algorithm) suite**
  - Voice and data encryption (Air Interface Encryption (AIE))
    - **TEA1: Readily exportable**
    - **TEA2: European public safety**
    - **TEA3: Extra-European public safety**
    - **TEA4: Readily exportable (hardly used)**
  - Not to be confused with Tiny Encryption Algorithm!

Optional: end-to-end

- **Only used by some countries, usually for special cases only**
- **Not inside TETRA standard**
  - Some guidelines / integrations are provided
- **Proprietary solution on top of AIE**
  - Expensive
- **Again, very opaque…**
  - High-level specification but no detail

Project RE:TETRA

Kerckhoffs' principle

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

-Auguste Kerckhoffs, 1883

Violators don't fare well

- A5/1, A5/2 (GSM), COMP128 (GSM)
- GMR-1, GMR-2 (SATPHONES)
- GEA-1, GEA-2 (GPRS)
- DSAA, DSC (DECT)
- MIFARE (RFID)
- HITAG (RFID)
- MEGAMOS (RFID)
- DST (RFID)
- Legic (RFID)
- CSS (DVD)
- CryptoAG / Hagelin

- Orange = backdoored

~~Kerckhoffs' principle~~ ETSI's principle

"Well [obscurity is] also a way of maintaining security."*

-Brian Murgatroyd, Chairman ETSI TC TETRA, 2023

* Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA
https://zetter.substack.com/p/interview-with-the-etsi-standards

Project motivation

- Proprietary cryptography has repeatedly suffered from practically exploitable flaws which remain unaddressed until disclosed

- GOAL: open up TETRA for public review after 20+ years
  - Enables informed risk analysis
  - Resolve issues
  - Level playing field

- Funded by NLnet
  - NPO funding open IT projects

Research program

Procurement

- Pick the right radio

Analysis

- Identify cipher location

Cipher Extraction

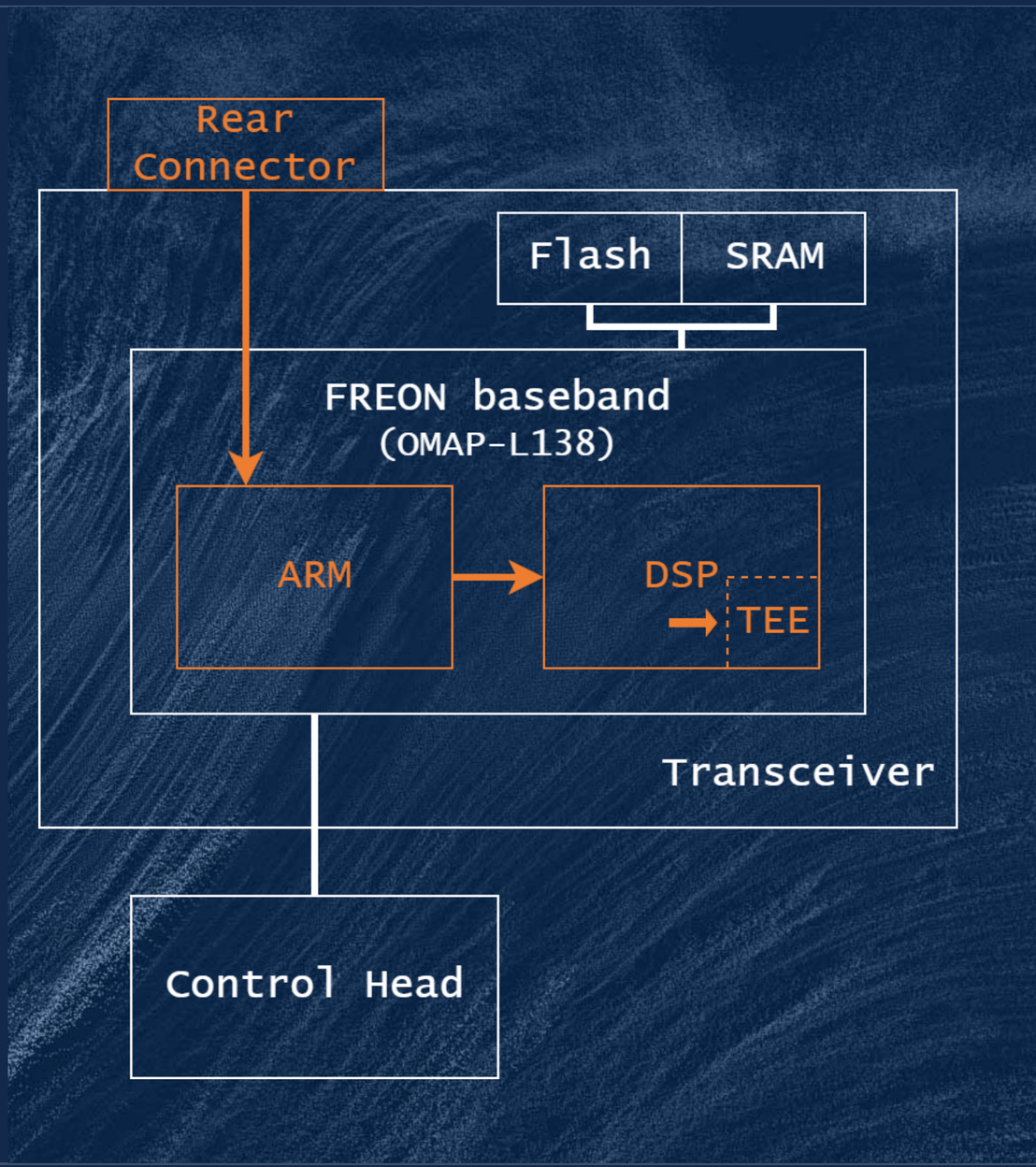
- Extract ciphers from radio

Attack R&D

- Cryptanalysis

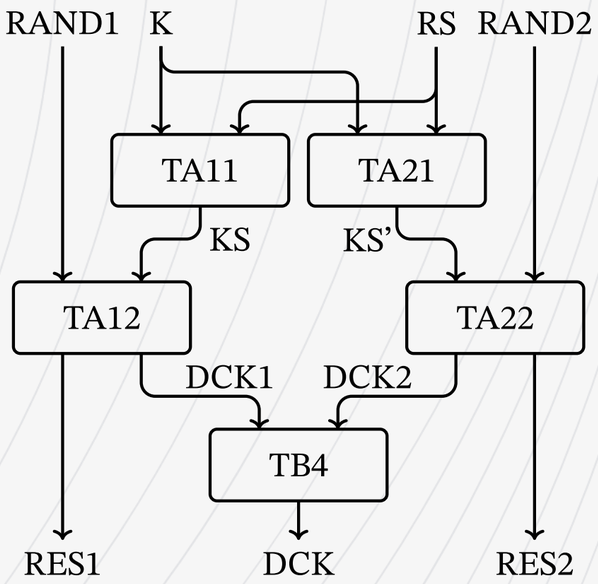
Pwning MTM5400

1. Format string → code exec on AP
2. Pivot to DSP via shared memory
3. Cache timing side-channel on TEE
4. **Secret algos!**
   … and key extraction …
5. **More details in our CCCamp talk**
   … we only have 50 minutes here ☹



The secret TETRA primitives and their security

TAA1 auth and OTAR

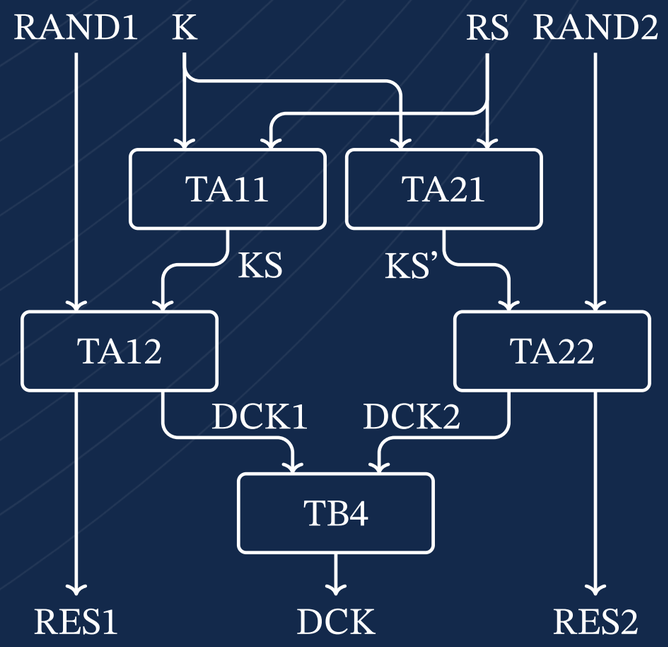


- Protocols in public standard, primitives not. We recovered:
- All TAxx based on HURDLE* cipher
  - 16-round Feistel cipher
  - 64-bit blocks, 128-bit key
- All TBx based on XOR / addition
- Some blocks identical / related
  - TA11 = TA41
  - TA12 = TA22
  - TA11(K, RS) = TA21(K, reversed(RS))

* https://impact.ref.ac.uk/casestudies/CaseStudy.aspx?Id=30193

CVE-2022-24400 DCK pinning attack

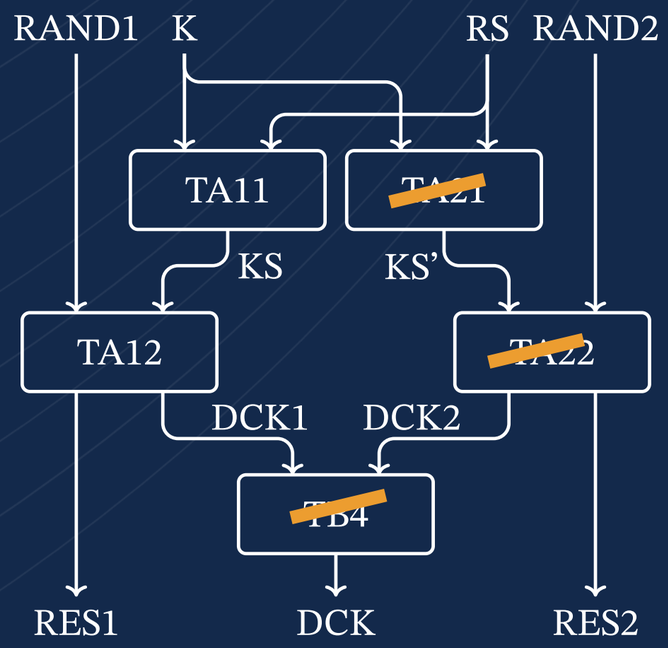
- **Mutual authentication**
  - Shared long-term secret K
  - Random seed RS
  - Challenge-response (RANDx/RESx)
  - Session key DCK




```
DCK = TB4(TA12(TA11(K, RS), RAND1), TA22(TA21(K, RS), RAND2))
```

CVE-2022-24400 DCK pinning attack

- We can simplify the authentication procedure now that we know primitives



TA11(K, reverse(RS))

TA12

XOR

```
DCK = TB4(TA12(TA11(K, RS), RAND1), TA22(TA21(K, RS), RAND2)))
 equals
DCK =     TA12(TA11(K, RS), RAND1) ^ TA12(TA11(K, reversed(RS)), RAND2)
```

CVE-2022-24400 DCK pinning attack

- **Assume we impersonate infrastructure and:**
  - reversed(RS) = RS (“palindrome”)
  - Predict MS challenge RAND2, use it as RAND1 as well
- Then, DCK simplifies to:

```
DCK = TA12(TA11(K, RS), RAND2) ^ TA12(TA11(K, RS), RAND2)
  equals
DCK = XOR(X, X) = 0 ← ALL ZERO KEY
```

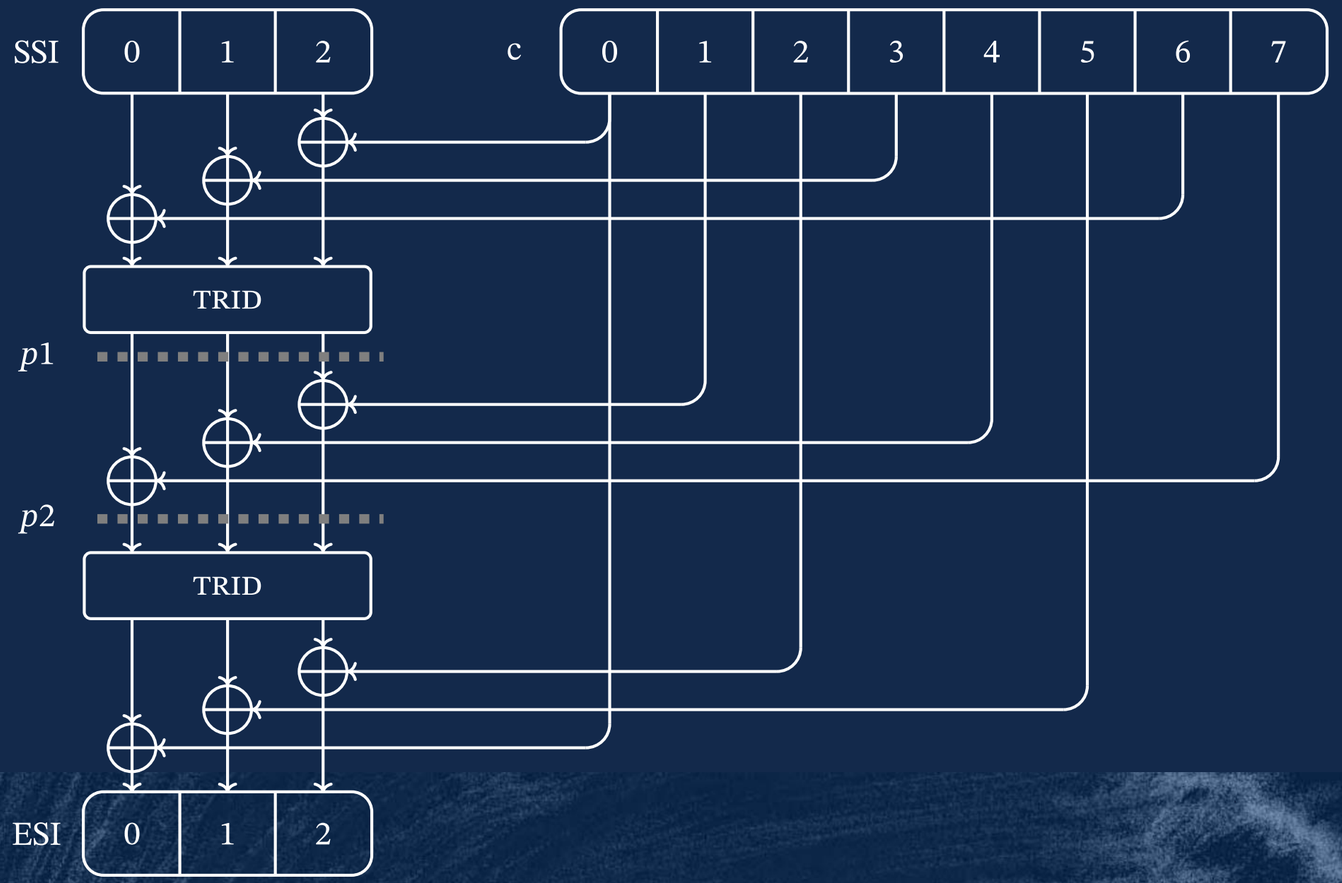
- Authenticated channel with radio,
  intercept uplink, post-auth functionality, etc.

Identity encryption

- **Part of TAA1, called TA61**
- **Encrypts 24-bit TETRA addresses**
  - encrAddr = TA61(addr)
- **Pseudonymity, not anonymity**
  - Encrypted identities change only when network key changes
- ***Implementation disclosed today!***

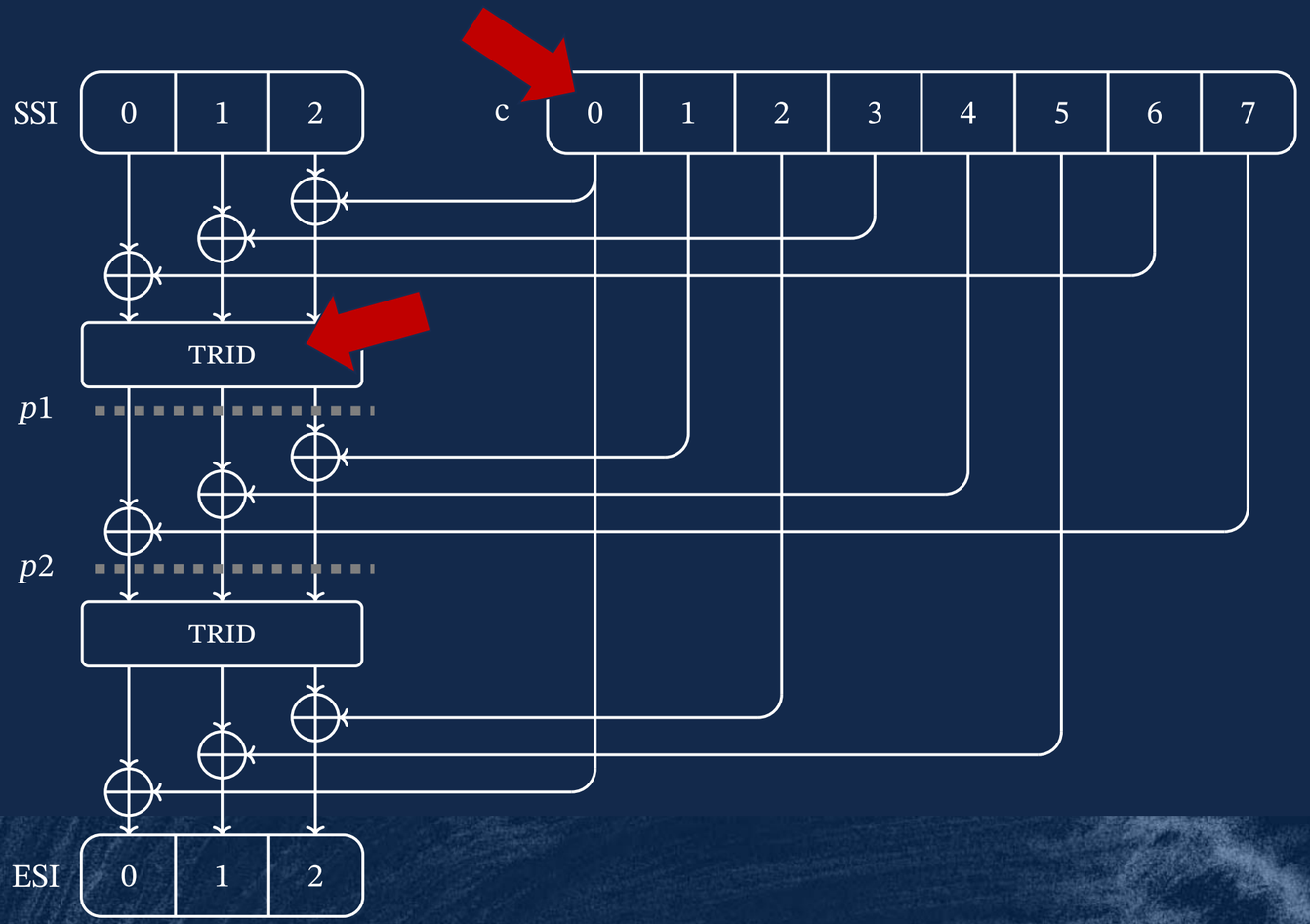
CVE-2022-24403 De-anonymization

- *Intermediate secret* c is derived from CCK using HURDLE
  - Full details ~~in December~~ next slide
- TA61 is vulnerable to *meet-in-the-middle* attack
  - Recovers value of c
  - Complexity: 2^{48} with 3 identity pairs
  - 1 min on laptop
  - Then, instant deanonymization



CVE-2022-24403 De-anonymization

- **Intermediate secret from HURDLE “hash”**
  - Expand 80-bit CCK (add/XOR) to 128-bit key
  - Compress CCK (XOR) to 64-bit plaintext
  - .. Can anyone find pre-images?
  - .. Would be candidate CCK values!
- **The TRID function**
  - Matrix multiplication on the 3 state bytes
  - Output bytes substituted by HURDLE sbox
  - Invertible
- **Full details on git**
  - https://github.com/MidnightBlueLabs/TETRA_crypto



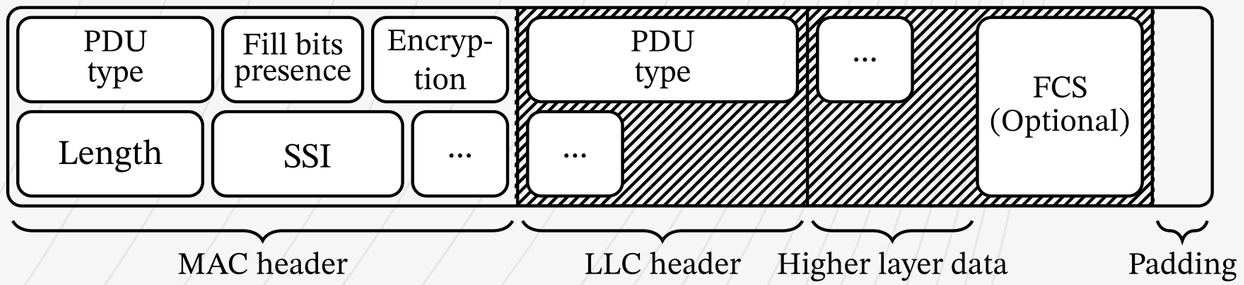
De-anonymization Scenario

- **Contextualize**
  - Correlate identities with observed units
  - Identity ranges allocated to user groups
- **Build live tracking map**
  - Counter-intelligence (unmask covert surveillance units)
  - Early warning (of e.g. police intervention)
- **Convenient**
  - Raspberry Pi + RTL-SDR dongle can be spread for geographic coverage
  - Fully passive, so stealthy!

Demo: CVE-2022-24403

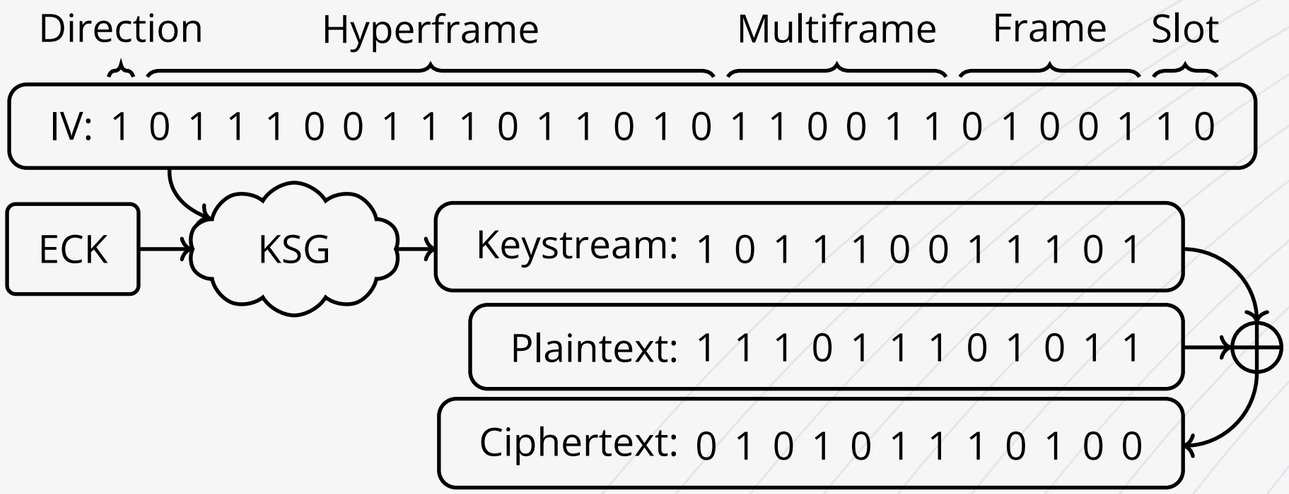
De-anonymization

Air Interface Encryption



- Air interface signalling is encrypted
- MAC header is unencrypted*
- LLC header and further payload gets encrypted by TEAx keystream generator (KSG)
- TETRA messages have no cryptographic auth/integrity guarantee
  - CRC16 on lower MAC layer
  - Optional CRC32 on LLC layer

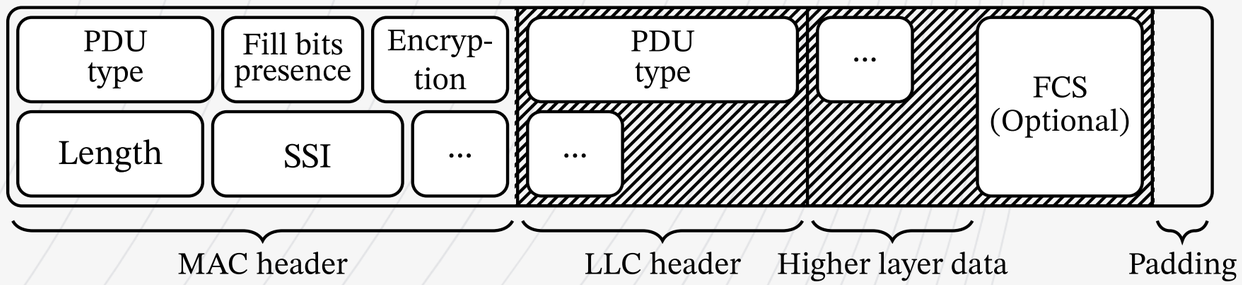
Air Interface Encryption



- **TEAx keystream generators depend on key and on network time**
  - Need to guarantee different keystream is used each time
- **Network time broadcast in unencrypted, unauthenticated manner**
  - SYNC and SYSINFO frames
- **As mentioned; no further *cryptographic* integrity checks**
  - Any encrypted data is taken at face value

CVE-2022-24401 Keystream recovery attack

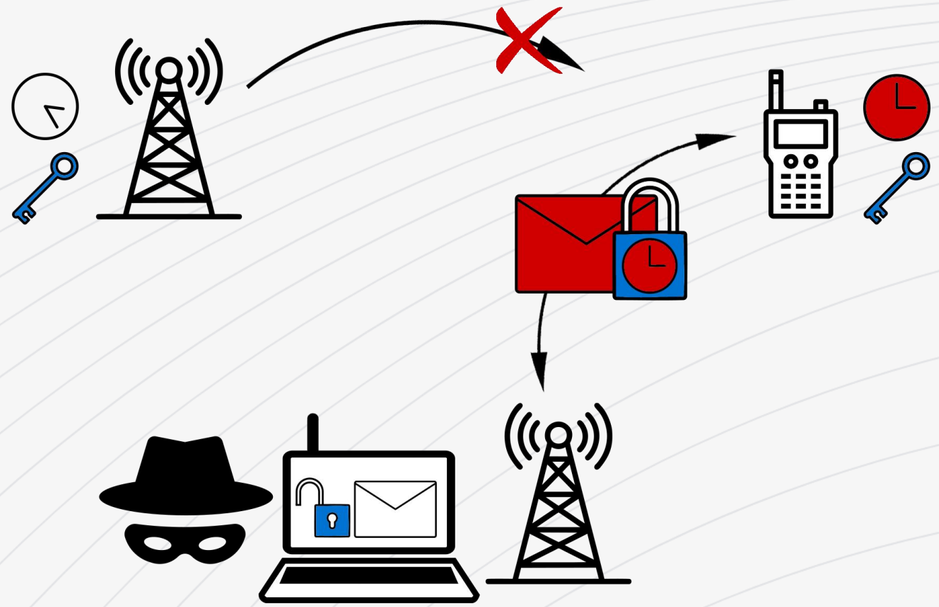
- Attacker can overpower infrastructure and alter MS perception of time
- MS will then use keystream that fits the attacker specified network time
- Works regardless of TEA used, regardless of ‘network authentication’



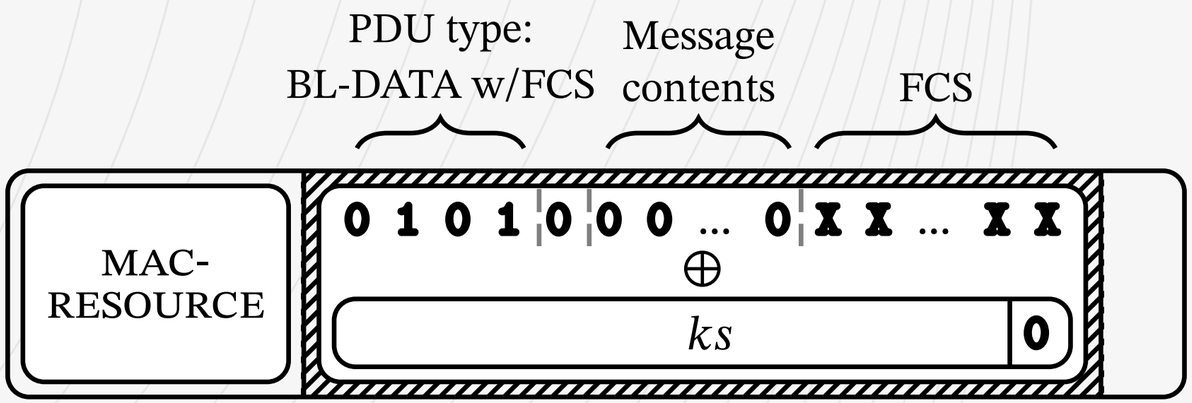
Attack outline

Attack outline:

- Capture interesting encrypted message at time T
- Target MS (any, with same keys)
- Overpower legitimate signal
- Set MS time to time T
- *Somehow recover keystream for that time*
- …
- Profit



Recovering keystream



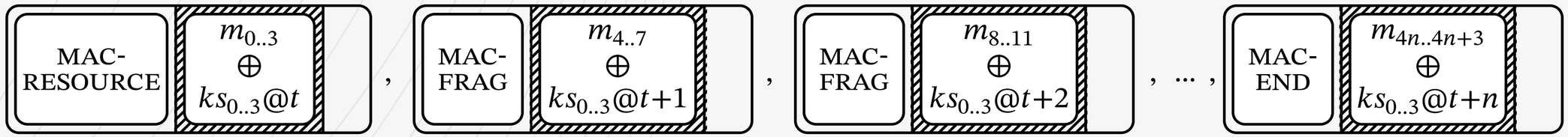
- **Assume we have n bits of keystream for time t. Construct message such that:**
  - It is of length n+1
  - It has an FCS
  - It needs an ACK from the MS
- **Encrypt, guess last ks bit is zero**
- **Send to MS**
- **If MS ACKs: FCS was good**
  - Found keystream bit n+1 = 0
  - If no ACK: keystream bit n+1 = 1
- **Repeat**

Bootstrap

- We need *seed keystream*
- Send 16 messages
  - `00000`, `00010`, …, `11110`
  - Will be decrypted by MS
- Only one will get ACK from MS
  - BL-DATA w/o FCS
  - Other messages are longer or unACKed
- Recovered 4 bits of ks ☺

From 4 to 37 bits

- Recover 4 bits for 10 slots
- Craft aforementioned message with FCS (min 37 bits)
- Use MAC fragmentation to distribute over the 10 slots
- Grow keystream knowledge for any slot of interest by guessing next ks bit

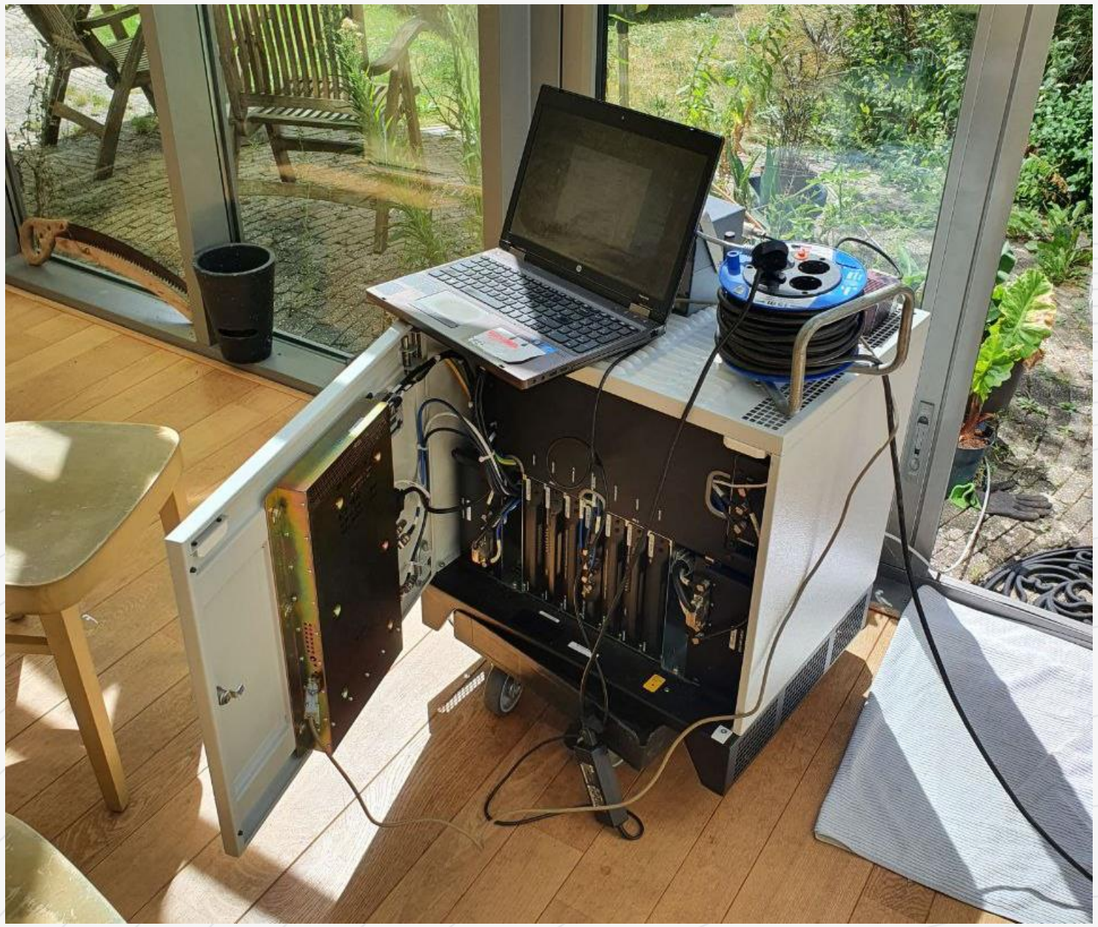


Intermezzo: ETSI

- **“Theoretical attack”**
- **Okay, so, can we have a base station to prove practicality?**
  - Haha lol no
  - More stakeholders responded like this
- **What do we do now?**
  - Implement TETRA infra stack for SDR?
  - Sounds like a lot of work…

There's your PoC

- Bought old Motorola MBTS
- Found some vulns in it
- Wrote module framework for it
- Turned it into attack platform

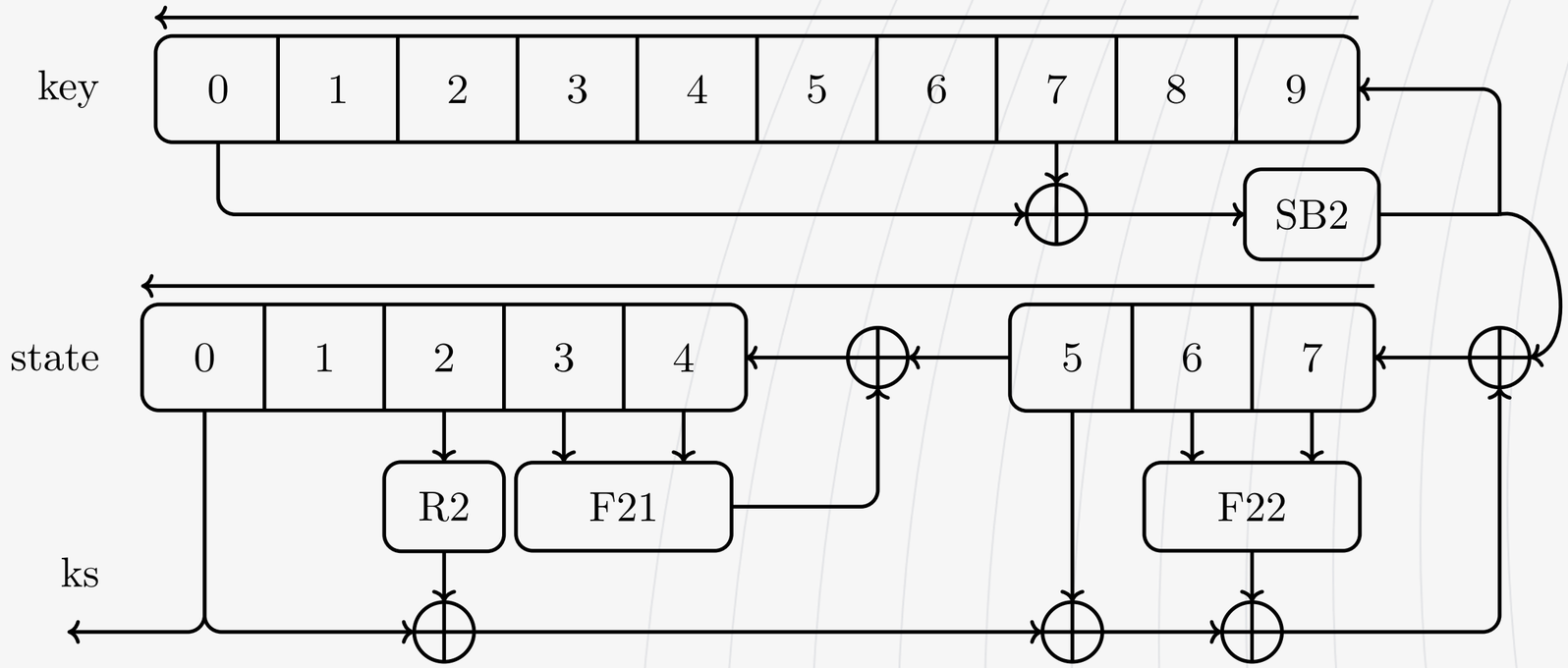


Demo: CVE-2022-24401

Keystream recovery attack

TEA Keystream generators

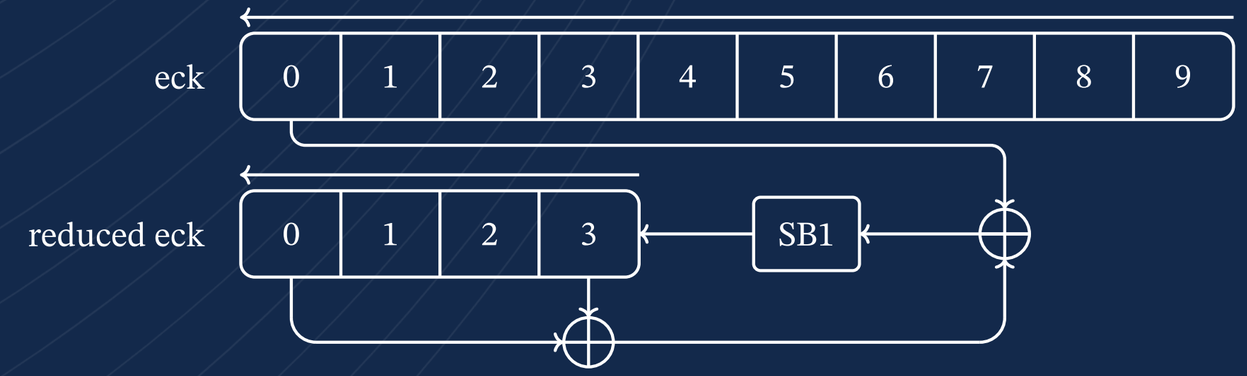
- Used for air interface encryption
- All KSGs have similar structure
- TEA2 seems robust*
  - We are not cryptographers
  - Public scrutiny needed!

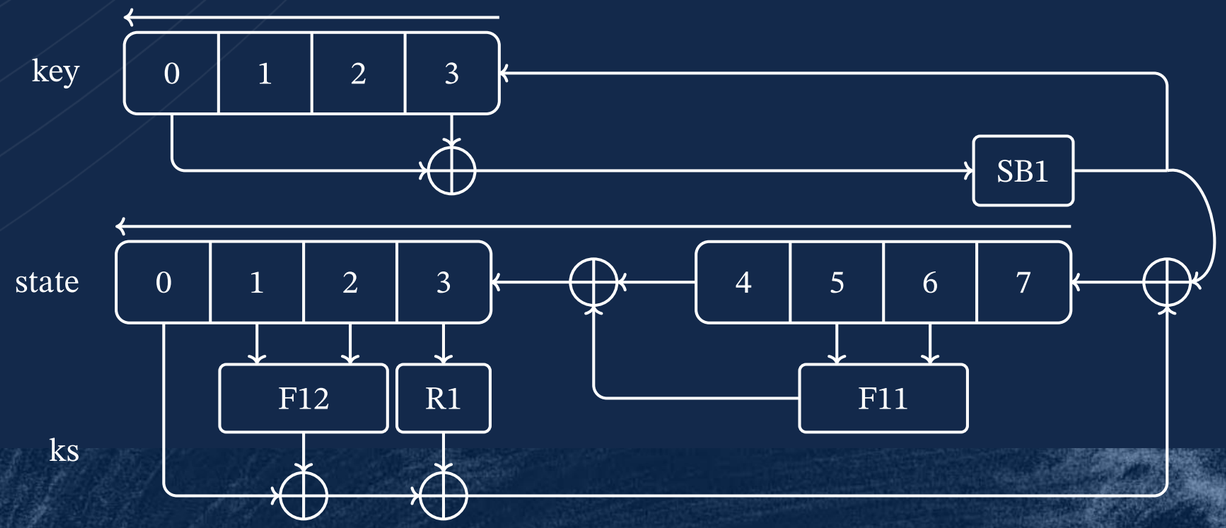


Pictured: TEA2

CVE-2022-24402 TEA1 backdoor

- **Target audience**
  - Private security, “less friendly” police / mil
  - .. But also, power, water, oil & gas
- **Advertised with 80-bit key**
  - Readily exportable but no hard indication on actual security (56-bit? 40-bit? 32-bit?)
- **Has “key initialization” function**
  - Reduces 80-bit key into 32-bit register
- **Trivial passive brute force (<1min)**
  - Intercept comms
  - Inject data (SCADA WAN!)





NVIDIA GTX 1080

State-of-the-art… consumer hardware… in 2016…

"**BM**: The researchers found that they were able to decrypt messages from this, using a **very high-powered graphics card** in about a minute."[1]

"**BM**: I suppose all I can say is that **25 years ago the length of this algorithm was probably sufficient to withstand brute-force attacks**.
KZ: You're saying 25 years ago 32 bit would have been secure?
BM: I think so. I can only assume."[1]

"**BM**: I would say it's vulnerable if you happen to be an expert and have some **pretty reasonable equipment**."[1]

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA
https://zetter.substack.com/p/interview-with-the-etsi-standards

- Let’s not assume

- Let’s not assume
- Let’s not use reasonable equipment

Toshiba Satellite 4010CDS

- Let’s not assume
- Let’s not use reasonable equipment
- Let’s go back to 1998!
  - 266 MHz Pentium II
  - 4.1 billion byte hard disk
  - 32MB SDRAM

Demo: Party like the ‘90s

Hold on ….

Surely the TEA1 backdoor doesn't impact Europe right?

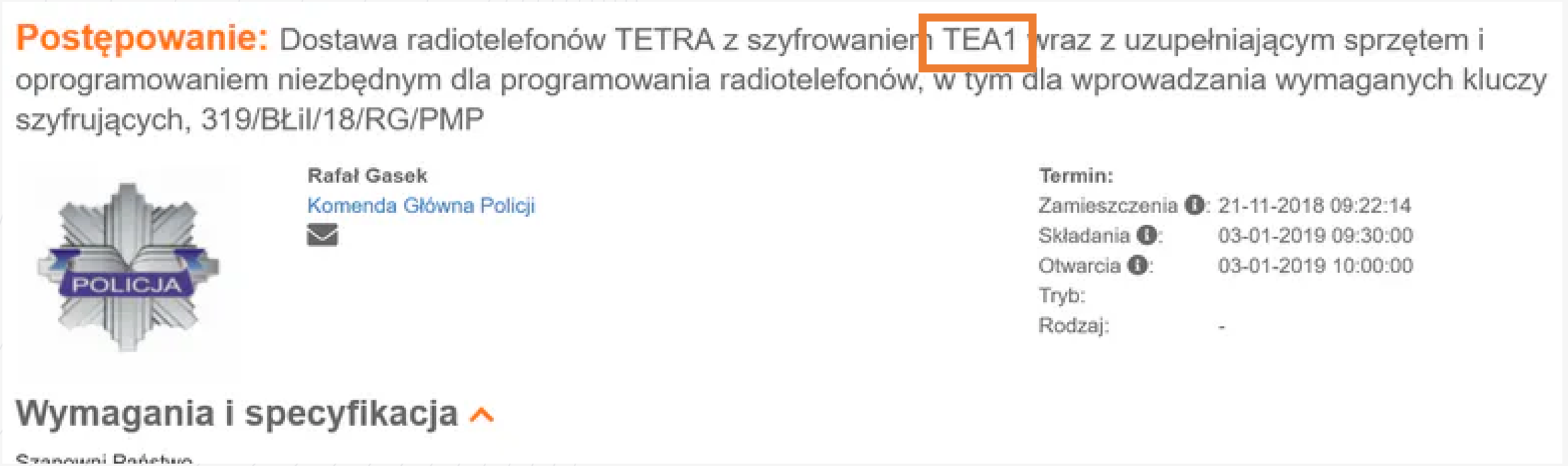
Nobody would shoot themselves in the foot like that?!

"**BM:** And I would expect that anybody … who need a lot of protection would not just be using TEA1. Within Europe… I would suggest that anyone who needed high security would be using TEA2. …. The problems generally are that TEA2 is only licensed for use within Europe by public safety authorities."[1]

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA https://zetter.substack.com/p/interview-with-the-etsi-standards

EU TEA1 Example #1: Poland

- EU Member since 2004
- Municipal Police were sold TEA1 as of 2019/2020
  - Warsaw, Krakow, Łódź, Główna, …



Postępowanie: Dostawa radiotelefonów TETRA z szyfrowaniem TEA1 wraz z uzupełniającym sprzętem i oprogramowaniem niezbędnym dla programowania radiotelefonów, w tym dla wprowadzania wymaganych kluczy szyfrujących, 319/BŁiI/18/RG/PMP

POLICJA

Rafał Gasek
Komenda Główna Policji

Termin:
Zamieszczenia: 21-11-2018 09:22:14
Składania: 03-01-2019 09:30:00
Otwarcia: 03-01-2019 10:00:00
Tryb:
Rodzaj: -

Wymagania i specyfikacja

Szanowni Państwo

[1] https://www.o2.pl/informacje/niepokojace-informacje-luka-w-systemie-tetra-niech-ktos-cos-zrobi-6923376203832288a

EU TEA1 Example #2: Bulgaria

- EU Member since 2007
- Ministry of Defense procured TEA1 infra as of 2019/2020

		КЖЦ – заменена с MTS 4/2BR
4.	MTS 4/4BR	MTS 4 -Базова станция, 380-400Mhz, 4BR 1контролен и 15физикални канала, TEA1, възможна работа с 220v / -48v В състав: Тетра сайт конролер TSC 1бр. Базово радио BR 2бр.,Захранващ блок PSU 1бр., Вентилатори 3бр., Система за честотно разпределение (автоматична)
5.	MTS 4/ 2BR	MTS 4 -Базова станция, 380-400Mhz, 2BR 1контролен и 7физикални канала, TEA1, възможна работа с 220v / -48v В състав: Тетра сайт конролер TSC 1бр. Базово радио BR 2бр.,Захранващ блок PSU 1бр., Вентилатори 3бр., Система за честотно разпределение(автоматична)

EU TEA1 Example #3: Slovenia

- **EU Member since 2004**
  - Had a TETRA (lack of) encryption scandal[1]
- **Aviation Police procured helicopter(s) outfitted with TEA1 radios in 2018**

Slovenačka policija kupuje novi višenamenski transportni helikopter

Vazduhoplov bi trebao biti opremljen s dva VHF radija frekventnog opsega koji se kreće od 118 do 135,992 MHz, razmakom između kanala od 8,33 kHz i bar 10 W predajne snage, zatim taktičkim radiom TEA1-encrypted TETRA koji je kompatibilan s slovenačkim policijskim sistemom i ETSI standardima (frequency

[1] https://www.rtl-sdr.com/security-researcher-jailed-for-researching-tetra/

EU TEA1 Example #4: Montenegro

- **Candidate EU Member since 2010**
  - Serious problems with (international) organized crime & drug cartels
- **Police procured TEA1 radios as of 2018**

Crna Gora
OPŠTINA BAR

Napomena:
- ponuda je zasnovana na našem "TETRA GOVERNMENT" paketu
- u cijenu je uračunat transport
- u cijenu je uračunata enkripcija "over the air"
- u cijenu je uračunato programiranje radio stanice i dodjeljivanje ključeva
- u cijenu je uračunato puštanje opreme u rad i uključenje u TETRA mrežu Crne Gore;
- u cijenu je uračunata obuka
- radio stanice koriste TEA1 sistem enkripcije
- u cijenu je uračunata garancija u trajanju od jedne gosine (12 mjeseci) od trenutka uključenja u TETRA mrežu Crne Gore

[1] https://www.o2.pl/informacje/niepokojace-informacje-luka-w-systemie-tetra-niech-ktos-cos-zrobi-6923376203832288a

EU TEA1 Example #5: Moldova

- **Candidate EU Member since 2022**
  - Geopolitically sensitive…
- **Moldovan Police & Carabinieri procured TEA1 radios between 2017 and 2020**
  - Including with U.N. aid

MTP3500 TETRA Portable
- High capacity batte
- Frequency band: at
- TEA1;

Criptare interfaţă radio
Algoritm de criptare TEA1
Clase de securitate 1, 2, 3
Cod de intrare PIN/PUK

We kindly request you to submit your quotation for the **Supply and Delivery of TETRA terminals and accessories to the General Police Inspectorate**, as detailed in Annex 1 of this RFQ. When preparing

Denumirea autorităţii contractante: Departamentul Trupelor de Carabinieri

TEA1 Example #6: U.S. local allies

- **Various police & military of U.S. local allies were handed TEA1 radios (not TEA3)**
  - Iraq's AFRN (2011 – U.S. DoD)
  - Lebanon's LISF (2012 – U.S. DoS)
  - CJTF-HOA (2017 – U.S. DoD)
  - AFOC Kabul (2020 – UNOPS)

MTH800 Portable Subscriber 380-430MHz

Antenna UHF whip

Standard Travel Charger - UK

TEA1 Arabic

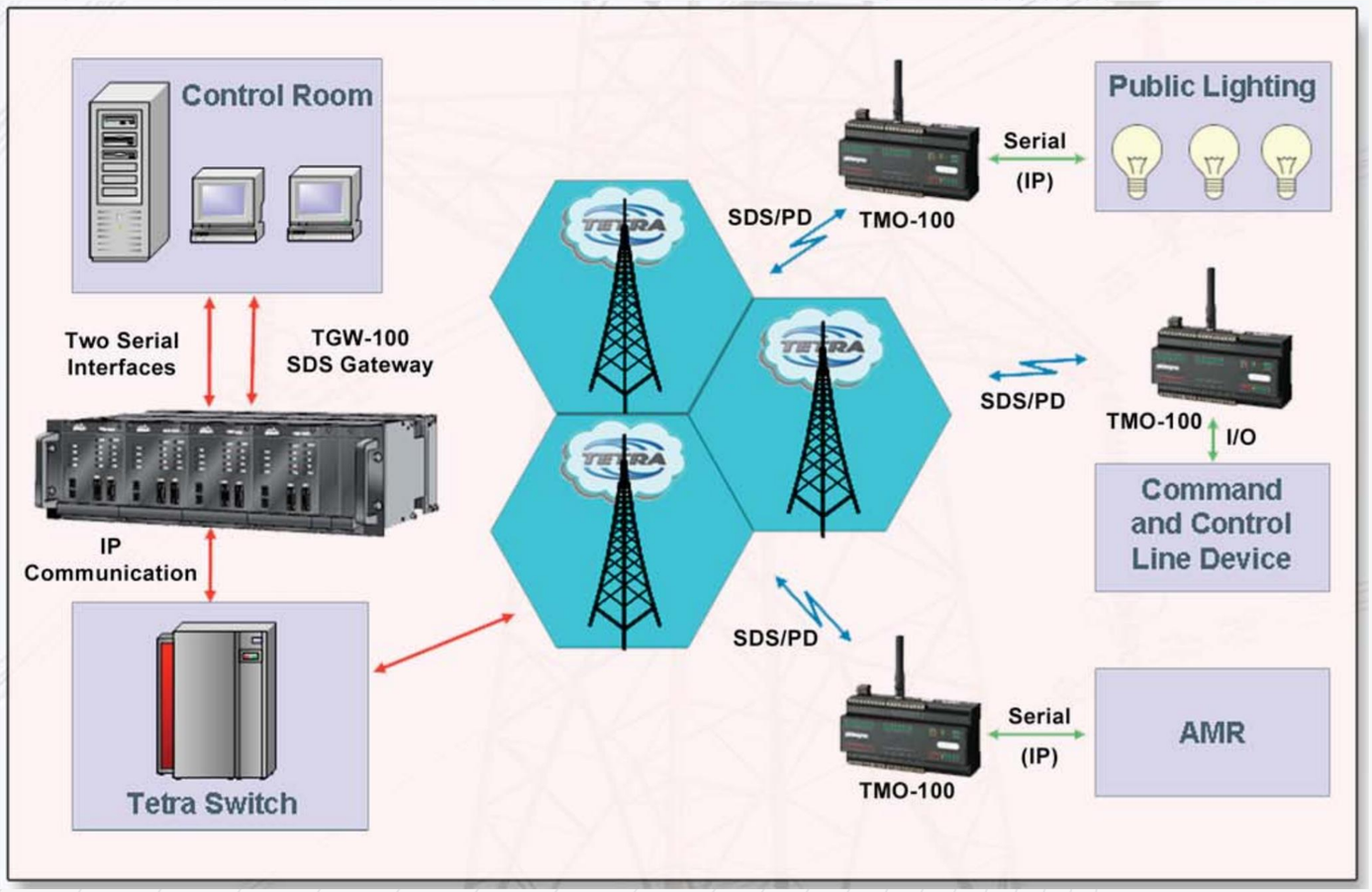
- Enabled with GPS, TEA1 encryption
- Accessories required to include individ

QA05097AA MTP3550 UHF TEA1 ROM GNSS 35

The system must be provided with initial implementation:

- TEA1 Encrytion
- Derived Cipher Key (DCK)

TETRA in Critical Infrastructure



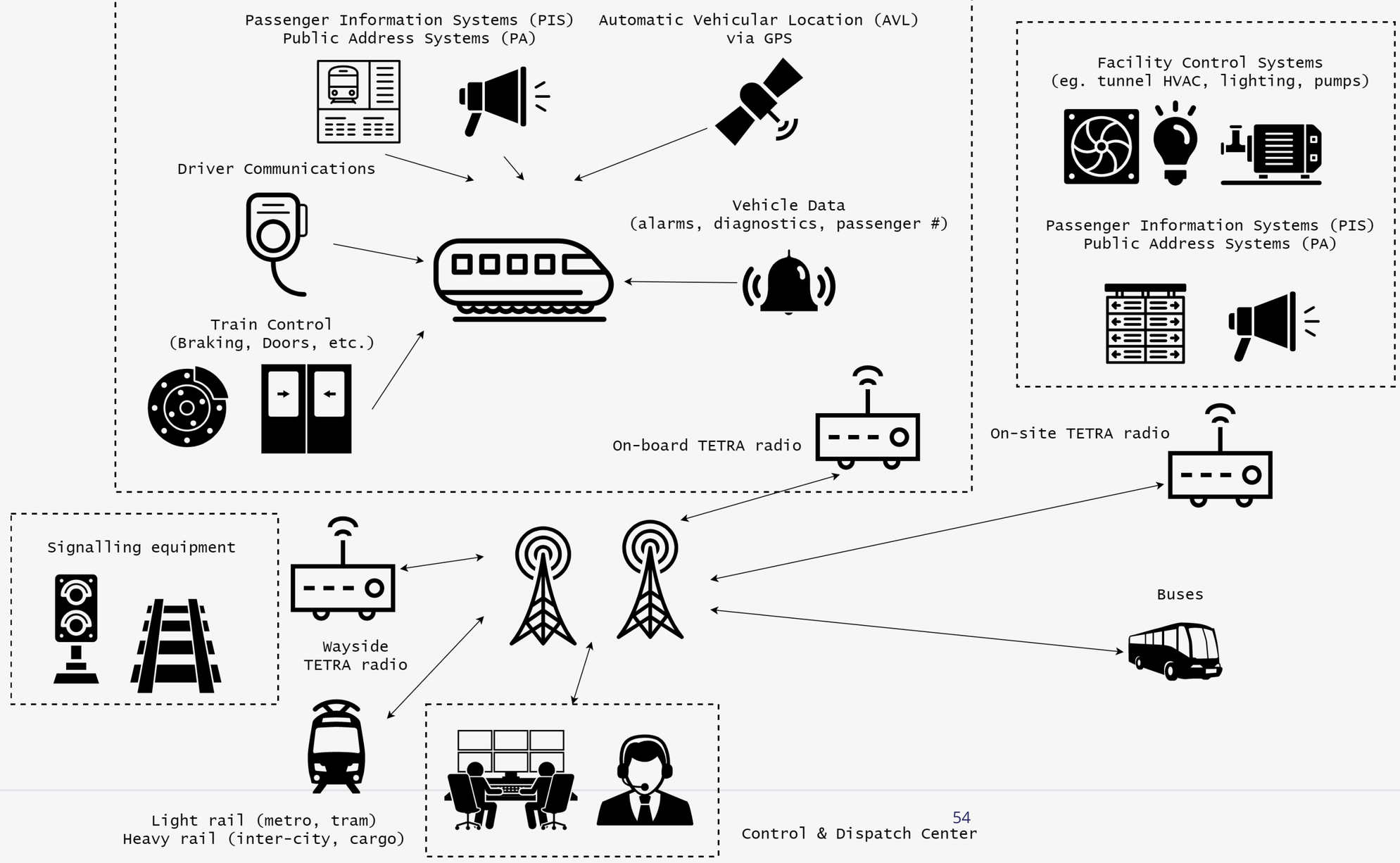
- **Networking architectures**
  - Radio-to-Radio, Gateway, direct IP via switch
- **Communication modes**
  - **Short Data Service (SDS):** Like SMS
  - **Packet Data (PD)**: IP subnet over TETRA
- **Data carriers (via SDS/PD)**
  - Serial, Serial-over-IP, Pure IP
- **Carry usual suspects**
  - IEC-101/104, DNP3, Modbus, ...

Image source: Piciorgros

Example: Transportation

- **Buses + light rail**
  - U.S.
  - U.K.
  - Germany
  - Spain
  - Greece
  - Australia
  - Argentina
  - Brazil
  - Mexico
  - Poland
  - Taiwan
  - …

- **Heavy rail**
  - EU ETCS = mostly GSM-R
  - but…
    - Finnish rail = TETRA
    - Kazakhstan rail = TETRA
    - Colombia rail = TETRA
    - …



Scenario 1: Passenger deception

Telecommunication sub-systems covered by TETRA

Interaction with Passenger Information System

- Text messages from the control centre to the on-board TETRA radio, which are displayed in the train LCD screens.
  - Train schedules
  - Information about incidents in the metro network

Telecommunication sub-systems covere

Interaction with Public Address System

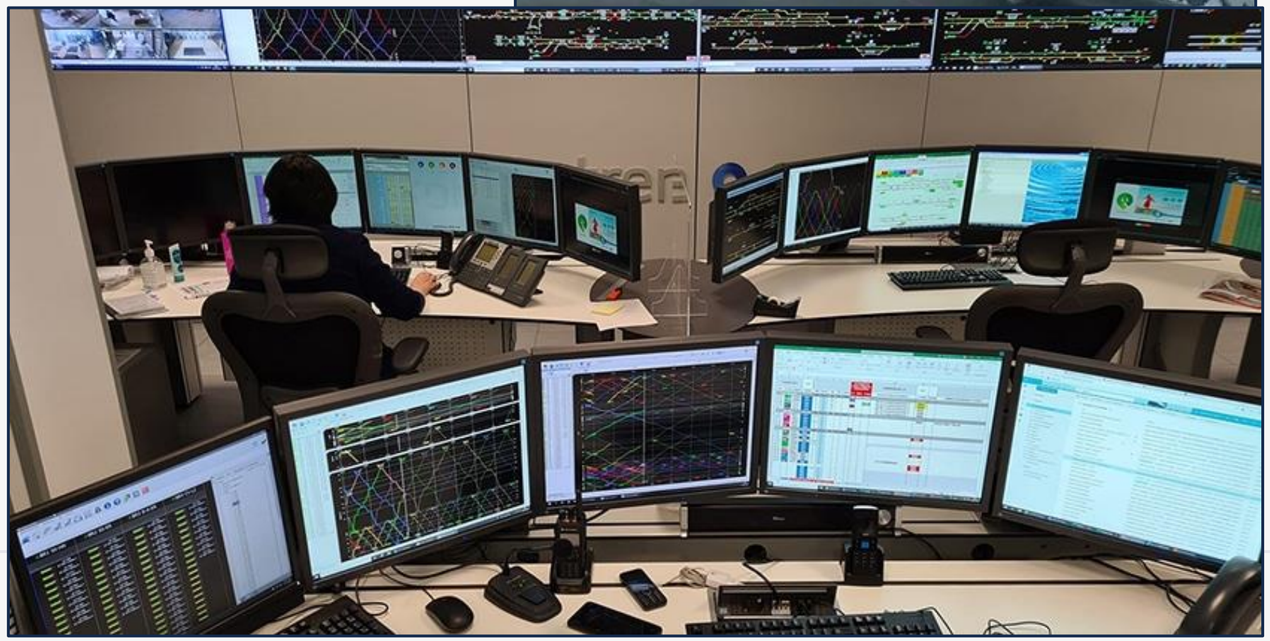
- Communication with Public Address System from driver or control center:
  - Call to the on-board PA Systems of a train
  - Call to the PA System in a platform
  - General call to all trains of line (static group)

'Unprecedented Chaos': Cyberattack Disrupts Iran Rail Network

A notice on electronic boards at stations asked travelers to call a number belonging to the office of Supreme Leader Ayatollah Ali Khamenei

Scenario 2: Dispatcher deception

Gridlock as hackers order hundreds of taxis to same place in Moscow

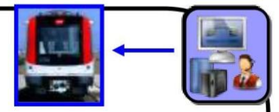


Scenario 3: Emergency braking

SDS-TL protocol for remote controls and alarms

PROTOCOL ID = C0H (ETSI registered)			
TYPE OF MESSAGE	ACK	SS	ST
MESSAGE REFERENCE (counter)			

Examples of remote controls and alarms



REMOTE CONTROLS:

- Train switch on / off
- Train identity (number and type of train)
- Emergency breaking
- Bypass of break / Traction loop
- Disable service break

ALARMS:

- Fire detection
- Emergency alarm activated
- Emergency breaking applied
- S.O.S alarm
- End of line alarm

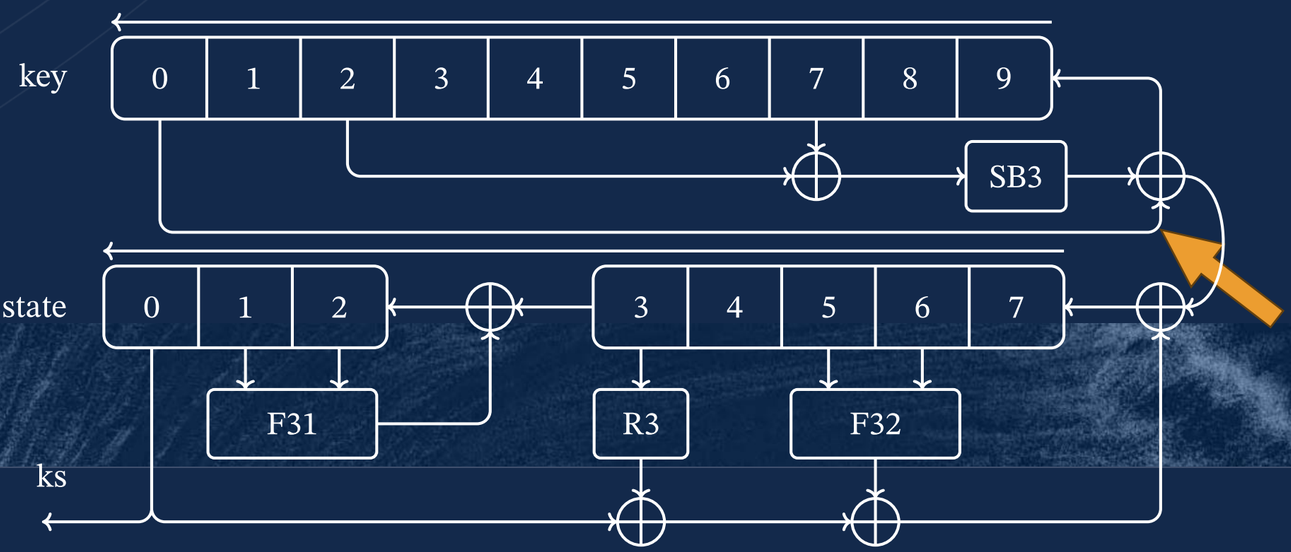
Poland's Railways Halted by a Simple Radio Hack

Polish teen derails tram after hacking train network

TEA3 quirk 🤔

- **Sbox not a permutation**
  - Duplicate entry
    - Flip bit → matches properties of other TEAs
  - Key register feedback structure slightly different, hides the issue
  - Highly unusual, certainly not positive
  - Unlikely to be accidental
    - Interoperability, feedback structure
- **Impact unclear**
  - Could not find practical attack
  - **Public scrutiny needed!**

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	7D	BF	7B	92	AE	7C	F2	10	5A	0F	61	7A	98	76	07	64
10	EE	89	F7	BA	C2	02	0D	E8	56	2E	CA	58	C0	FA	2A	01
20	57	6E	3F	4B	9C	DA	A6	5B	41	26	50	24	3E	F8	0A	86
30	B6	5C	34	E9	06	88	1F	39	33	DF	D9	78	D8	A8	51	B2
40	09	CD	A1	DD	8E	62	69	4D	23	2B	A9	E1	53	94	90	1E
50	B4	3B	F9	4E	36	FE	B5	D1	A2	8D	66	CE	B7	C4	60	ED
60	96	4F	31	79	35	EB	8F	BB	54	14	CB	DE	6B	2D	19	82
70	80	AC	17	05	FF	A4	CF	C6	6F	65	E6	74	C8	93	F4	7E
80	F3	43	9F	71	AB	9A	0B	87	55	70	0C	AD	CC	A5	44	E7
90	46	45	03	30	1A	EA	67	99	DB	4A	42	D7	AA	E4	C2	D5
a0	F0	77	20	C3	3C	16	B9	E2	EF	6C	3D	1B	22	84	2F	81
b0	1D	B1	3A	E5	73	40	D0	18	C7	6A	9E	91	48	27	95	72
c0	68	0E	00	FC	C5	5F	F1	F5	38	11	7F	E3	5E	13	AF	37
d0	E0	8A	49	1C	21	47	D4	DC	B0	EC	83	28	B8	F6	A7	C9
e0	63	59	BD	32	85	08	BE	D3	FD	4C	2C	FB	A0	C1	9D	B3
f0	52	8C	5D	29	6D	04	BC	25	15	8B	12	9B	D6	75	A3	97



Coordinated Vulnerability Disclosure

Timeline

- **01-2021** • Started work on the RETETRA project
- **12-2021** • First contact NCSC-NL
- **01-2022** • First meeting Dutch police
- **01-2022** • First meeting ETSI
- **01-2022** • First meeting intelligence community
- **02-2022** • Detailed preliminary advisory distributed
- **'22/'23**
  - Further advisory info & mitigations distributed to stakeholders
  - Coordinated publication timeline

Mitigations

CVE	Description	Recommended Mitigation	Compensating Controls
CVE-2022-24401 CVE-2022-24404	Keystream recovery attack	• Firmware updates • E2E • (data) TLS / IPsec	• Renew keys frequently • Risk assessment, adjust OPSEC
CVE-2022-24402	TEA1 backdoor	• TEA2 • E2E • (data) TLS / IPsec	• Assume TEA1 == cleartext • Risk assessment, adjust OPSEC
CVE-2022-24403	Deanonymization attack	• Migrate to TAA2	• Risk assessment, adjust OPSEC
CVE-2022-24400	DCK key pinning attack	• Firmware updates • E2E • Migrate to TAA2	• Disable radios with unacceptable FW update rollout timelines

Misinformation!

Misinformation: ETSI & TCCA

- **Official statement (July ‘23)**
  - TEA1 is “not a backdoor”
  - No mention of other vulns whatsoever

> *“The research uncovered some general areas for improvement in the TETRA protocol”* [1]

- **As of December ‘23: continued statements to industry claiming only TEA1 issue is relevant**

1 https://www.etsi.org/newsroom/news/2260-etsi-and-tcca-statement-to-tetra-security-algorithms-research-findings-publication-on-24-july-2023

Misinformation: ETSI & TCCA

- Continue recommending TETRA as “highly secure” wireless link for SCADA (**1.5 years after our disclosures**)

TETRA automation use case: Some train operators use TETRA for train control and safety functionality. Many train, rail, metro and tram transport operators use TETRA for auxiliary control and functionality for their public transport operations. The high security and encryption support of TETRA enables these safety-critical applications.

TETRA automation use case: TETRA network coverage can be optimised to cover an oil or gas pipeline with low number of base stations and enable pipeline monitoring and control using a secure wireless network in addition to providing secure and reliable voice communications along the length of the pipeline.

https://tcca.info/tetra/tetra-and-the-internet-of-life-saving-things/
https://www.criticalcommunicationsreview.com/ccr/news/110722/tetra-data-capabilities-are-still-under-utilized-in-2023

Misinformation: Vendors & System Integrators

- **Vast majority:** ☑ ☑ ☑
  - No public statement
  - Some don’t even inform customers
- **Others echo ETSI / TCCA downplaying**
  - No surprise: they ***are*** ETSI / TCCA
- **“hypothetical”, “lab conditions”, “no evidence of real world attacks”**
- **This makes our & NCSC’s job a lot more tiresome …**

1 https://insidestory.gr/article/eyalotoi-se-epitheseis-oi-asyrmatoi-tis-ellinikis-astynomias
2 https://hmf-smart-solutions.de/en/statement-on-possible-vulnerabilities-of-the-tetra-air-interface/

Misinformation: Vendors & System Integrators

- **They do risk assessments for their customers**
  - Nice: grading your own exam!
  - For supposedly “hypothetical vulnerabilities”
- **<u>But</u>: they don’t understand things**
  - CVE-2022-24401 is ***not*** a MitM[1]
- **And they give *bad* advice (all in 2023)**
  - Tried to sell TEA1 to <u>multiple</u> critical infra parties telling them it was fine or that it would be ‘patched’
  - Told <u>multiple</u> critical infra parties “network authentication” would protect them against message injection
  - At least 1 case of broken patch that **<u>did nothing</u>**

1 https://hmf-smart-solutions.de/en/statement-on-possible-vulnerabilities-of-the-tetra-air-interface/

Aftermath

Maybe nobody targets TETRA networks?

"**KZ:** But is that in the best interest of the public that are using these algorithms?

BM: Well it's a moot point isn't it, really. That's a difficult thing to say "yes it's to the benefit of the public or not." There's no evidence of any attacks on … TETRA that we know of."[1]

"ETSI and TCCA are not at this time aware of any exploitations on operational networks."[2]

2 out of 5 attacks are passive so… 🤔

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA
https://zetter.substack.com/p/interview-with-the-etsi-standards

[2] ETSI and TCCA Statement to TETRA Security Algorithms Research Findings Publication on 24 July 2023
https://www.etsi.org/newsroom/news/2260-etsi-and-tcca-statement-to-tetra-security-algorithms-research-findings-publication-on-24-july-2023

Right…

Snowden leaks show joint NSA & ASD project to collect Indonesian police TETRA comms during U.N. climate change conf in Bali 2007[1]

Not proof of TETRA:BURST exploitation specifically – but proof of *active TETRA targeting*

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(S//SI//REL) SIGDEV Efforts in Support of the United Nations Framework for Climate Change Conference, Bali, Indonesia

POCs: [redacted]

(U) The United Nations Framework Climate for Change Conference (UNFCCC), held in Bali, Indonesia from 3-14 December, was attended by10,000 conferees, activists, journalists, and high ranking representatives from 190 countries, including the newly elected Australian Prime Minister, Mr. Kevin Rudd, the U.S. Secretary of State, and former U.S. Vice President Al Gore.

(S//SI//REL) Beginning on 29 November, the SIGDEV and Collection Operations Divisions executed a self-initiated network development effort, in coordination with the Defense Signals Directorate (DSD) and site leadership, in support of this target. The goal of the development effort was to gain a solid understanding of the network structure should collection be required in the event of an emergency. This involved identifying systems in use, isolating talk groups and TETRA towers of highest interest, determining network hierarchy, and reporting flow. Site produced a Telecommunications Information Report (TELIR) documenting network structure and activity. *(Please contact* [redacted] *if you would like a copy of the TELIR.)*

(S//SI//REL) Although DSD's initial collection requirements were only for UHF push-to-talk communications collected via remote operations in Canberra, RAINFALL proposed a more in-depth SIGDEV effort. To start, a communications externals (COMEXT) task was generated to rapidly survey 100–3300MHz. Using this data, site analysis identified a previously unknown TETRA trunk mobile network with towers in both Jakarta and Bali. With this information, site analysts began a focused TETRA network development effort, which resulted in the identification of Indonesian security forces (POLRI) communications at both locations. At DSD's request, site dedicated a staff member (a trained Indonesian linguist) to this effort to monitor, scan, and transcribe the TETRA voice communications in order to provide daily summaries of network activity. Intercept ranged from network set-up to situation reports. Highlights include the compromise of the mobile phone number for Bali's Chief of Police and demonstration routes.

[1] https://theintercept.com/document/nsa-telegraph-sigdev-efforts-in-support-of-the-united-nations-framework-for-climate-change-conference-bali-indonesia/

Right…

Op QUITO (TSI): Following a couple OMGs and a significant amount of prep work, the planning phase of Op QUITO, an effects op to support FCO's goals relating to Argentina and the Falkland Islands, is almost complete. The plans are due to go to submission in the next month, and then this will hopefully lead to a long-running, large scale, pioneering effects operation.

Snowden leaks reveal GCHQ TSI '*effects operation*' QUITO against AR around Falklands/Malvinas oil exploration rights tensions in 2009[1]

Involved TETRA collects as part of military/leadership tasking

Not proof of TETRA:BURST exploitation specifically – but proof of *active TETRA targeting*

Argentina

TSI initiated and supported OH tasking against Argentina in efforts to collect high priority military and Leadership comms. Work was coordinated across the OH enterprise to obtain results when opportunity arose using US 903G and US 940C, MHS Ops were a main driver for this collection. Results included a number of TETRA collects and at least seven Argentinian PCM (digital) microwave emitters which were processed and geolocated. Although TSI haven't got desired results on their comms of interest as yet, this was a positive and encouraging team effort against this target in readiness for when next opportunity arises. Efforts between TSI and MHS continue.

[1] https://cryptome.org/2015/04/nsa-gchq-jtrig-intercept-15-0402.pdf

What’s next? New algos!

The new algorithms

- **Algorithm set B**
  - TAA2 authentication suite
  - TEA5-7 air interface encryption ciphers
- **Initially were to be secret but..**
- **Following our disclosures, old & new algos will be public!**

"Transparency is at the root of ETSI, in our governance and technical work. With their decision at the TCCE meeting, our members proved once again that we evolve with technology and market requirements," - Luis Jorge Romero, ETSI Director-General.

https://www.etsi.org/newsroom/press-releases/2293-etsi-releases-tetra-algorithms-to-public-domain-maintaining-the-highest-security-for-its-critical-communication-standard

Yay*

- **Assuming no sleight of hand**
  - Open design criteria
  - No unexplained constants
  - Open reference implementations
  - No rigging of manuals[1]

- **There's a clear front door now**

"The new algorithm TEA7 has an effective key length reduction to 56 bits and will be available in many countries as per the Wassenaar Arrangement."

1 https://www.cryptomuseum.com/intel/nsa/backdoor.htm#manual
2 https://tcca.info/tetra/tetra-documentation/research_disclosures/

56 – A *bit* on the weak side…

- **Assuming set B is as fast as set A**
  - Bitsliced CPU TEA1 cracker as baseline [1]
  - Single AWS c7i.metal-48xl machine would take 170 days [2]
- **AWS cost as low as 5000 euro [3]**
  - *Within a week for ~5/6K seems reasonable*
  - Alternatively: GPU, FPGA, …
  - **Cost will only decrease over time …**
- **Well within capabilities of determined adversary**
  - States (including your bad guy of choice)
  - Organized crime
  - Bored teenagers with wealthy parents

1) Many thanks to Aram
2) Based on extrapolation of a benchmark on 32-core c7i.8xlarge
3) Based on discounted spot pricing, which seems reasonably available

"Insanity is doing the same thing over and over again and expecting different results"

- **Wassenaar since year 2000:**
  - Exceptions for public crypto
  - Exceptions for (mobile) civil use
  - Exceptions for *"connected civil industry application"..*
- **Will critical infra get TEA7?**
  - As was the case for TEA1..
  - **This would be a big mistake**
- **At least now we know before adoption..**

Should we trust TEA6?

What do you think?

Should we trust TEA6?

Let's ask ETSI!

"**KZ: Should we trust ETSI algorithms going forward**?
BM: I've no reason to believe you shouldn't.
KZ: But the public has a reason not to — the fact that they're secret.
BM: I can think of all sorts of algorithms that, over time, they become weak. And lots of them have been public ones as well. Sure, algorithm may not have a life of a quarter of a century that's for sure.... [But] **we have no reason to produce dodgy algorithms, if you like.**"[1]

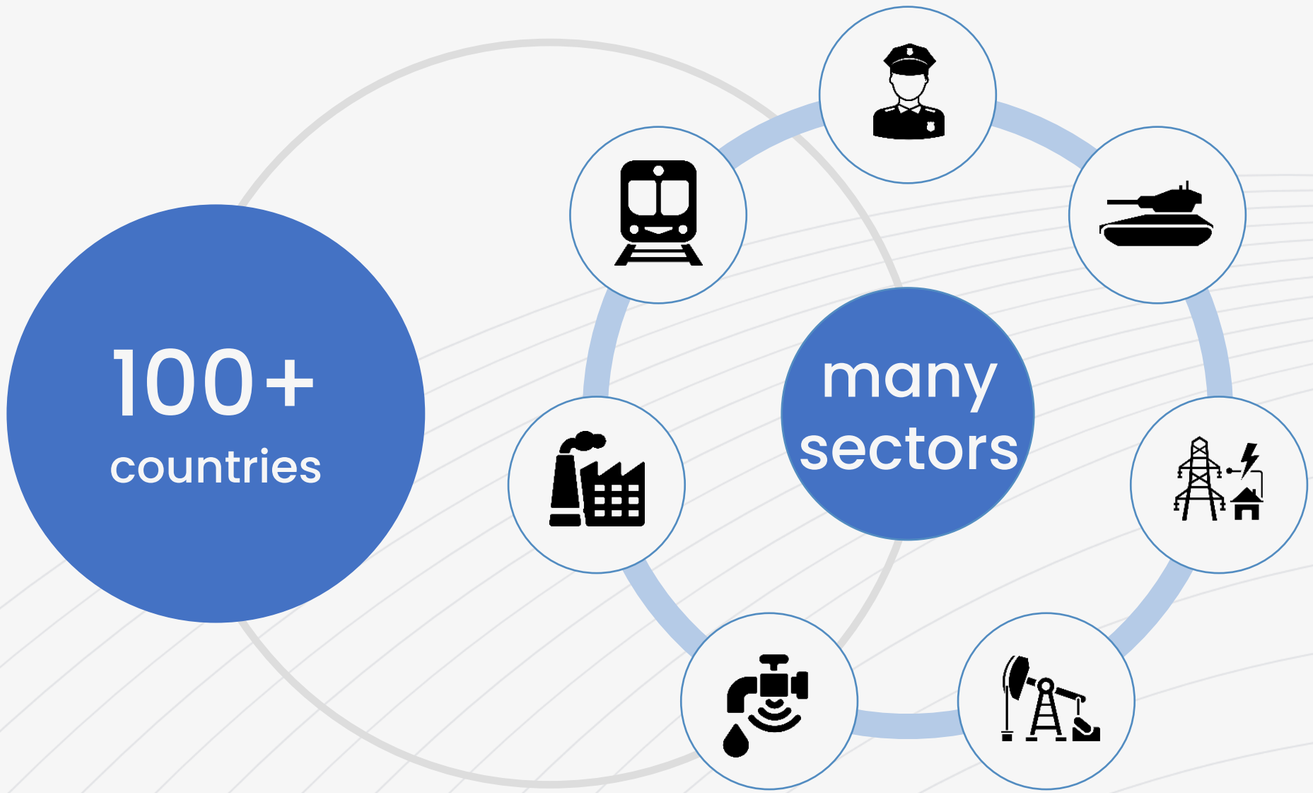
"**BM:** We were just given those algorithms. **And the algorithms were designed with some assistance from some government authorities, let me put it that way**."[1]

"**BM: At the end of the day, it's down to the customer organization to ensure that things are secure enough for them. Now, I agree that's difficult with a private algorithm.** The manufacturer knows the length of the key, but it's not publicly available. **But the reason we have three different algorithms available must be clear to somebody that they're not all as secure as each other.**"[1]

[1] Interview between Kim Zetter and Brian Murgatroyd, Chair of ETSI TC TETRA
https://zetter.substack.com/p/interview-with-the-etsi-standards
NOTE: BM's comments refer to TEA1-4 but there is little reason to doubt their applicability to TEA5-7

Conclusion

- First public, in-depth TETRA security analysis (after 20+ years)
- Secret crypto algorithms reverse-engineered
- Multiple vulns found (incl. backdoor)
- Patches available for some issues, mitigations for others
- Lots of work still to be done for asset owners!



Call to Action

1. If your organization uses TETRA
   - Look into relevant mitigations
   - Don’t blindly trust vendors, **please reach out to us when in doubt**

2. Take a closer look at the crypto
   - TEA set A & B, HURDLE

3. Implement / extend open TETRA stacks
   - Great work by OsmocomTETRA / SQ5BPF
   - .. Still lots to do, talk to NLnet, OsmocomTETRA

4. Stop doing secret crypto please
   - Looking at you, TETRA E2EE…

Questions?

Social

-

Web

- midnightblue.nl
- tetraburst.com

Contact

- c.meijer@midnightblue.nl
- w.bokslag@midnightblue.nl
- j.wetzels@midnightblue.nl