



Cyber Time to Cyber Crime - TETRA:BURST as a wake-up call for all Critical National Infrastructure

Christian Farrow

May 15th 2025



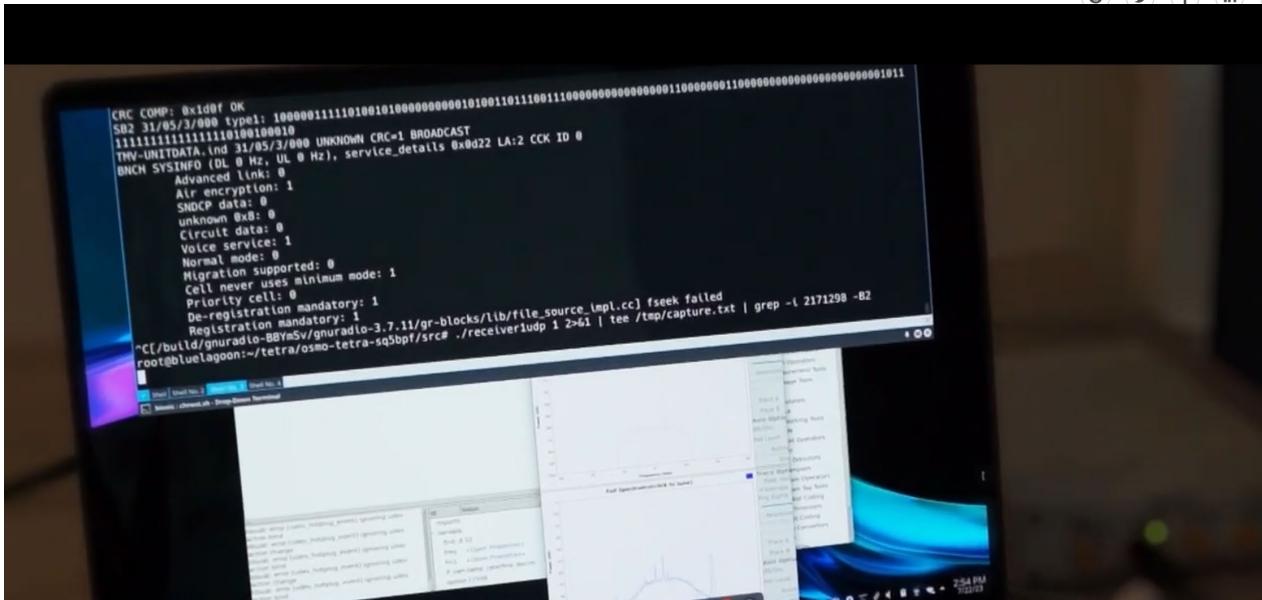
Resilient Time – Time as an attack vector

09:49 Fri 3 Nov

theresister.com



- TETRA:BURST attack
 - based on spoofing "un-authenticated time packets" on the network



Allows:

Decryption (real-time or after the fact) of voice/data/SMS
Interception/Injection of data in SCADA-WAN

TETRA radio comms used by emergency heroes easily cracked, say experts

If it looks like a backdoor, walks like a backdoor, maybe it's ... export control

 Thomas Claburn

Mon 24 Jul 2023 // 23:20 UTC

UPDATED Midnight Blue, a security firm based in the Netherlands, has found five vulnerabilities that affect Terrestrial Trunked Radio (TETRA), used in Europe, the United Kingdom, and many other countries by government agencies, law enforcement, and emergency services organizations.

The flaws, dubbed **TETRA:BURST**, are said to affect all TETRA radio networks. They potentially allow an attacker to decrypt communications in real-time or after the fact, to inject messages, to deanonymize users, or to set the session key to zero for uplink interception.

Two of the flaws are characterized as critical. The first ([CVE-2022-24401](#)) is an oracle decryption attack that can be used to reveal text, voice, or data communication. It is made possible by the Air Interface Encryption (AIE) keystream generator's reliance on network time, which is broadcast publicly and without encryption.

The second ([CVE-2022-24402](#)) is an engineering weakness – the [TEA1 \[PDF\]](#) encryption algorithm, according to the researchers, "has a backdoor that reduces

All references and all credit due to:

<https://www.tetraburst.com/>

Midnight Blue (NL)

<https://www.midnightblue.nl/>

What is TETRA?

AI Overview

TETRA (Terrestrial Trunked Radio) is a globally adopted digital radio standard, particularly for mission-critical communications, used in a wide range of sectors including public safety, transport, energy, and mining. It's [deployed in over 130 countries](#) and serves millions of users daily. TETRA is known for its reliability, scalability, and security, making it a favored technology for professional users who need dependable communication. 

Here's a more detailed look at its global presence:

Key Sectors and Applications:

Public Safety:

Police, fire departments, and ambulance services extensively use TETRA for communication in emergency situations. 

Transportation:

Rail transport, airlines, and other transport networks rely on TETRA for reliable and secure communication. 

Critical Infrastructure:

Energy and mining sectors utilize TETRA to ensure safe and efficient operations. 

Corporate Networks:

Large enterprises deploy TETRA for internal communication, especially where reliability and security are paramount. 

Specialized Applications:

TETRA is also found in security services, military, and even in major sporting events for resilient and secure communication. 

Learn more 

Secure, proven TETRA - Sepura

TETRA, or Terrestrial Trunked Radio, is the technology of choice worldwide for mission an...



TETRA Overview - Hytera EU

You will find Hytera's TETRA radios used all over the world, from the Netherlands Police...



Critical communications for all professional users

Germany's network, nearing completion, will become the largest in the world, with more tha...



 The Critical Communications Association 

Show all

What is TETRA?

AI Overview

TETRA (Terrestrial Trunked Radio) is a globally adopted digital radio standard, particularly for mission-critical communications, used in a wide range of sectors including public safety, transport, energy, and mining. It's [deployed in over 130 countries](#) and serves millions of users daily. TETRA is known for its reliability, scalability, and security, making it a favored technology for professional users who need dependable communication.

Here's a more detailed look at its global presence:

Key Sectors and Applications:

Public Safety:

Police, fire departments, and ambulance services extensively use TETRA for communication in emergency situations.

Transportation:

Rail transport, airlines, and other transport networks rely on TETRA for reliable and secure communication.

Critical Infrastructure:

Energy and mining sectors utilize TETRA to ensure safe and efficient operations.

Corporate Networks:

Large enterprises deploy TETRA for internal communication, especially where reliability and security are paramount.

Specialized Applications:

TETRA is also found in security services, military, and even in major sporting events for resilient and secure communication.

Regional Deployment:

Europe:

Europe was the first region to adopt TETRA, and the technology remains widely used there.

North America:

The North American market opened up to TETRA in 2012, with networks already in place in the USA and Canada.

Asia-Pacific:

This region is experiencing rapid growth in TETRA deployments, with many systems in place in China, and the Asian Tiger economies.

Other Regions:

TETRA is also used in countries across Africa, the Middle East, and South America.

Examples of TETRA Use:

Hytera:

Their TETRA radios are used in diverse locations, including the Netherlands Police Network, Shenzhen metro, and the Kazakhstan Ministry of Railways.

Germany:

Germany's network is one of the largest in the world, with over 500,000 users.

London Underground:

The London Underground, one of the oldest metro systems, transitioned to TETRA for system-wide communication.

Copenhagen Metro:

Copenhagen Metro was one of the early adopters of TETRA.

Major Sporting Events:

TETRA is deployed at major events like the Olympic Games and the FIFA World Cup.

Secure, proven TETRA - Sepura
TETRA, or Terrestrial Trunked Radio
technology of choice worldwide for m

 Sepura :

TETRA Overview - Hytera EU

You will find Hytera's TETRA radios u
over the world, from the Netherlands

 Hytera EU :

Critical communications for all
professional users

Germany's network, nearing comple
become the largest in the world, with

 The Critical Communications Association

Show all

What is TETRA?

AI Overview

TETRA (Terrestrial Trunked Radio) is a globally adopted digital radio standard, particularly for mission-critical communications, used in a wide range of sectors including public safety, transport, energy, and mining. It's [deployed in over 130 countries](#) and serves millions of users daily. TETRA is known for its reliability, scalability, and security, making it a favored technology for professional users who need dependable communication.

Here's a more detailed look at its global presence:

Key Sectors and Applications:

Public Safety:

Police, fire departments, and ambulance communication in emergency situations

Transportation:

Rail transport, airlines, and other transport secure communication.

Critical Infrastructure:

Energy and mining sectors utilize TETRA

Corporate Networks:

Large enterprises deploy TETRA for resilience and security are paramount.

Specialized Applications:

TETRA is also found in security services, military, and even in major sporting events for resilient and secure communication.

Regional Deployment:

Europe:

Europe was the first region to adopt TETRA, and the technology remains widely used there.

North America:

The North American market opened up to TETRA in 2012, with networks already in place in the USA and Canada.

Asia-Pacific:

This region is experiencing rapid growth in TETRA deployments, with many systems in place in China, and the Asian Tiger economies.

Other Regions:

TETRA is also used in countries across Africa, the Middle East, and South America.

Examples of TETRA Use:

Region	Notable Countries/Markets	Key Sectors/Applications
Europe	UK, Germany, Sweden, Spain, Romania	Public safety, transport, utilities
Asia-Pacific	China, South Korea, Taiwan, India	Railways, metro, public safety, industry
Middle East	UAE, Qatar, Israel, Turkey	Public safety, military, critical infrastructure
Africa	South Africa, Swaziland	Airports, public safety
Latin America	Mexico, Colombia, Chile	Police, emergency services, rail, forestry
North America	USA, Canada	Utilities, transport, public safety

Major Sporting Events:

TETRA is deployed at major events like the Olympic Games and the FIFA World Cup.

Secure, proven TETRA - Sepura
TETRA, or Terrestrial Trunked Radio, technology of choice worldwide for mission-critical communications.

 Sepura :

TETRA Overview - Hytera EU

You will find Hytera's TETRA radios used over the world, from the Netherlands to the USA.

 Hytera EU :

Critical communications for all professional users

Germany's network, nearing completion, will become the largest in the world, with

 The Critical Communications Association

WSTS25, fasten your seat belts & hold on...

- The next 10 slides are a (super-speedy) high-level view of the TETRA:burst attack based on screenshots of Midnight Blue's YouTube videos...

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**



Open standard?

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

All Cops Are Broadcasting

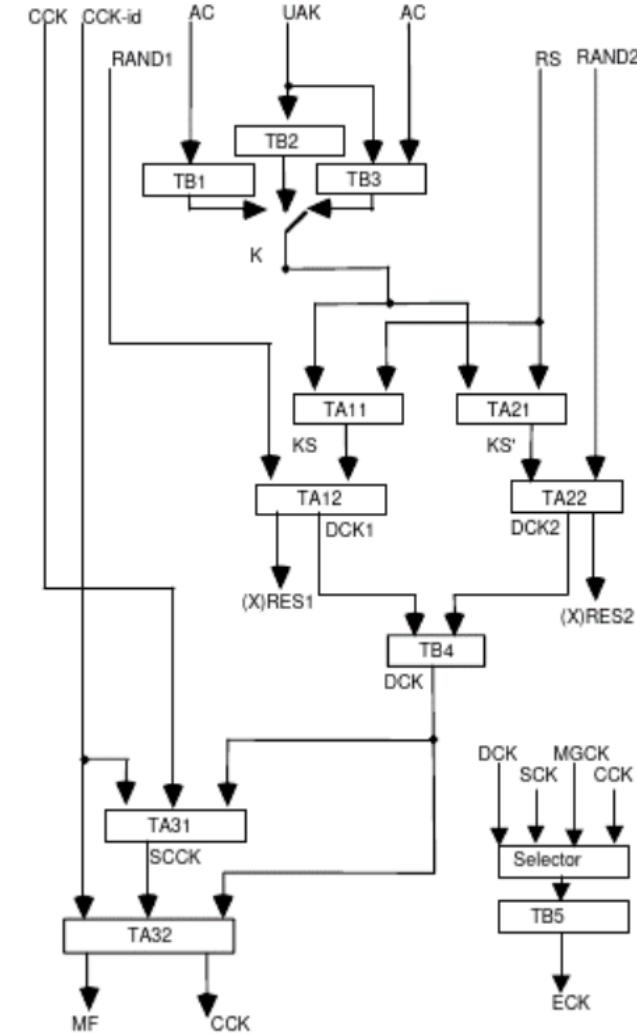


Figure B.1: Overview of air interface authentication and key management (sheet 1)



Kerckhoffs' principle

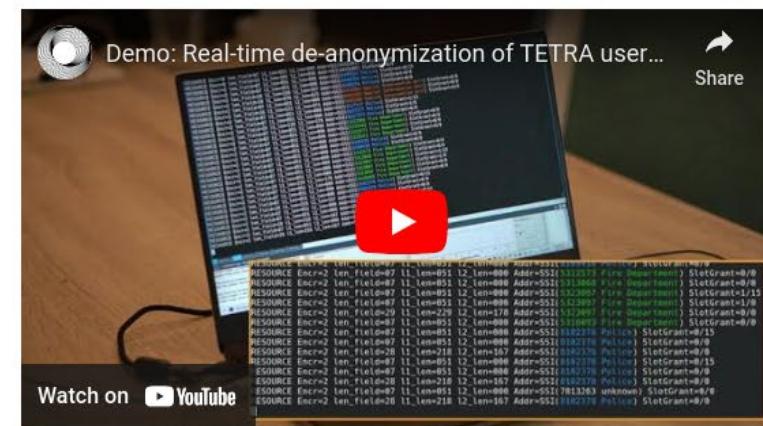
“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

-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

We have recorded several demonstration videos. In the first, we demonstrate the decryption oracle attack (CVE-2022-24401) in our lab setup using an instrumented base station as an attacker platform. In the second video, we demonstrate the TEA1 backdoor (CVE-2022-24402) on a real network. Third, we demonstrate the TEA1 attack running on a 1998 consumer grade laptop, as a response to claims 32 bits of entropy may have been sufficient in the mid nineties. Lastly, in the fourth video, we demonstrate the real-time de-anonymization attack (CVE-2022-24403).



Motorola MTM5400

- Common model, easily obtained 2nd hand online
- Baseband SoC by TI
 - So, no hardware TETRA crypto
- SoC has software security features
 - Used for protecting TETRA crypto from extraction?

This is a very common model, it's easily obtained secondhand online on eBay, and it has a baseband





Etymology of "Pwning"

Origin and Meaning

- "Pwning" comes from the internet slang term "pwn," which means to dominate, defeat, or humiliate someone, especially in online gaming or hacking contexts 1 4 5.
- The word "pwn" originated as a typographical error of "own," due to the proximity of the "p" and "o" keys on QWERTY keyboards 1 3 6.
- It became popular in the early 2000s within online gaming communities, where "owned" meant to decisively beat someone, and "pwned" quickly caught on as an alternative spelling 1 3 6.

Spread and Usage

- The term spread from gaming to hacker slang, where "pwn" also refers to gaining unauthorized control over a computer or network 1 4 6.

Ask follow-up...



ing MTM5400

at string → code exec on AP

to DSP via shared memory

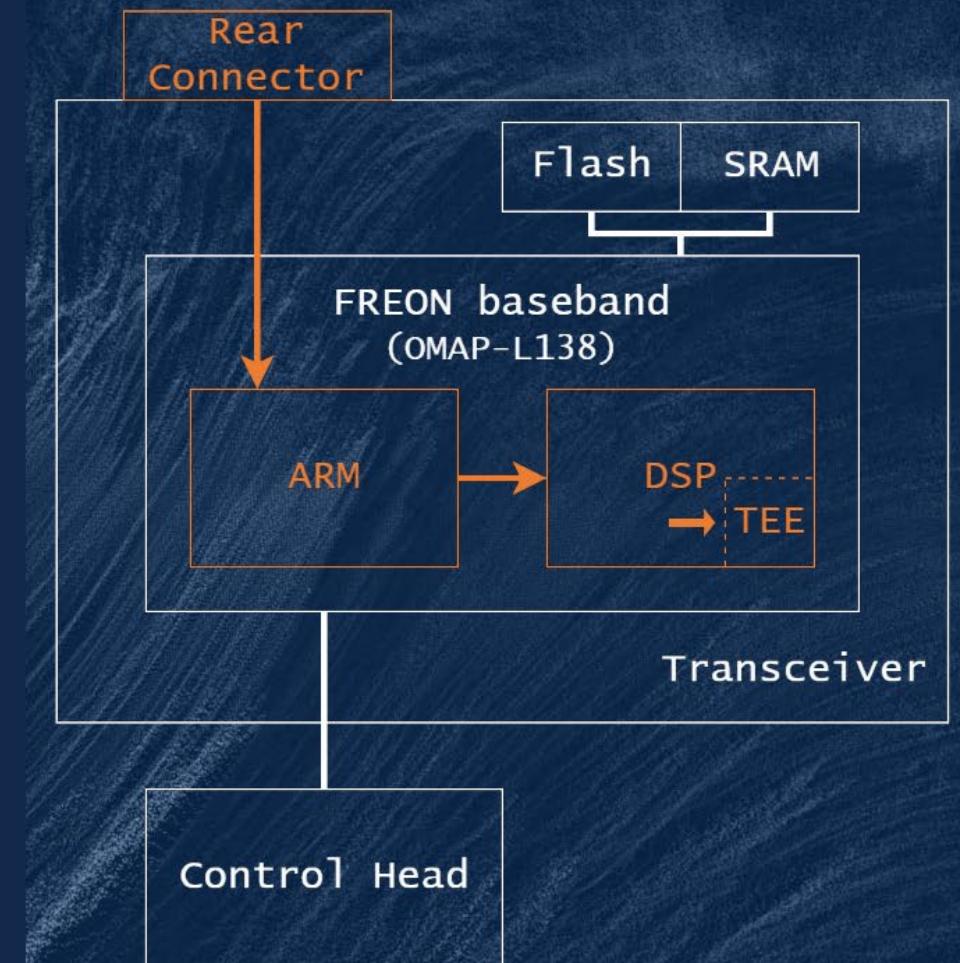
Timing side-channel on TEE

algs!

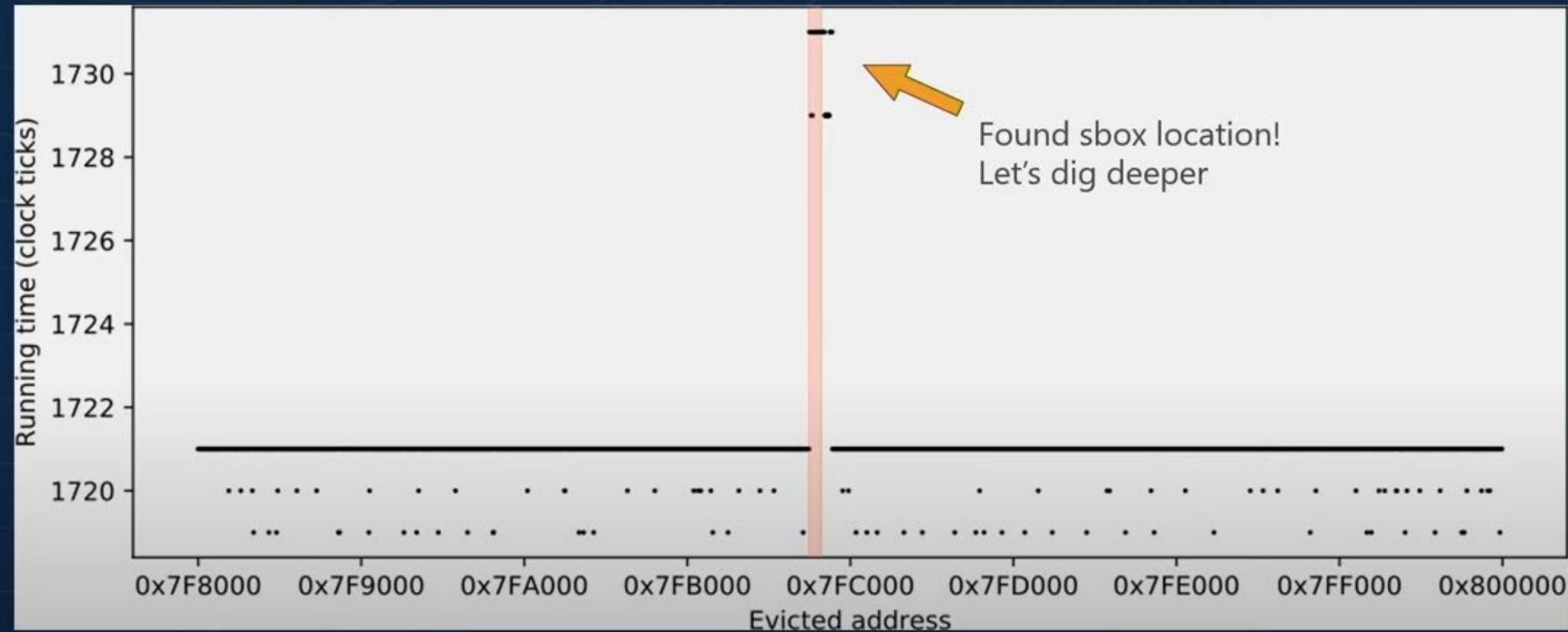
key extraction ...

details at DEF CON

only have 40 minutes here 😊



Privilege / Security	Secure	Non-secure
Supervisor	Secure Kernel and Secure Boot Loader	DSP/BIOS or other OS kernels
User	Licensed Algorithms (e.g. WMV, WMA, etc...)	Non-secure Applications or other OS kernels

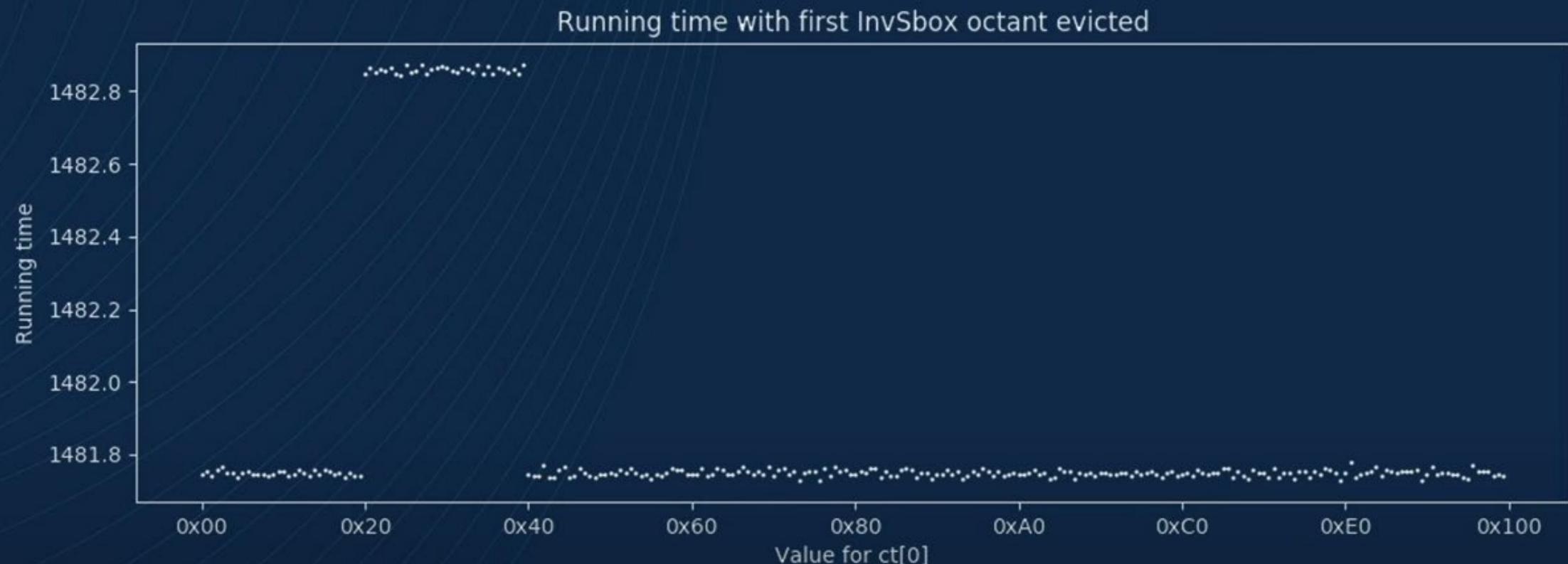


So we get something like this.



sales@midnightblue.nl // midnightblue.nl // All Right Reserved
21:33 / 1:10:12





- If penalty observed: $ct[0] \oplus rk_{16}[0] < 0x20$
So when we plot that, we get something like
- Above example: $0x20 \leq rk_{16}[0] < 0x40$
this, which is quite interesting.

PoC II gtfo

- **Wrote .ksreuse module**
 - Implements sudden changes of network time and a way to recover keystream
- **Our MTM5400 rebooted..**
 - Run into some synchronization issues, resolved by aligning time changes to 4 multiframe
 - Can be resolved, but would be beyond PoC
- **Some more tinkering...**
 - .. and the MTM gladly accepts any jumps in network time



TETRA_burst Public

[Watch 44](#)[Fork 7](#)[Star 61](#)[main](#)[1 Branch](#)[0 Tags](#)[Go to file](#)[Add file](#)[Code](#)

 carlicious placeholder for release of tooling

79056d0 · last year 

 LICENSE

placeholder for release of tooling

last year

 README.md

placeholder for release of tooling

last year

 tetraburst.svg

placeholder for release of tooling

last year

 README

 Apache-2.0 license



<https://tetraburst.com>

This repository will contain all resources and tools developed during the TETRA:BURST research trajectory that we deem of potential public interest. Stay tuned.

About

No description, website, or topics provided.

 Readme

 Apache-2.0 license

 Activity

 61 stars

 44 watching

 7 forks

[Report repository](#)

Releases

No releases published

Packages

No packages published

Time as an attack vector?

- Previous talks have focused on "de-synchronisation" attacks

 **Dana A. Goward, FRIN** · Following
President, Resilient Navigation & Timing Foundation; Propri...
21h •   

#GPS #GNSS #Galileo #PNT #cyber #jamming #spoofing #IT #infrastructure
#telecom



GPS = CYBER!

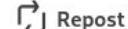
The growing threat to GPS is a cyber issue - Stephen Dye on LinkedIn

Dana A. Goward, FRIN on LinkedIn • 7 min read

What's New: Another voice pointing out that PNT (and therefore GPS) is a critical IT component an...

  Ivan Petrunin and 60 others

4 comments • 15 reposts

 Like  Comment  Repost  Send

 **Tomasz Widomski** reposted this    

 **Andrzej Gab** • 2nd
Senior manager / expert | CCIE (Sec) | CISSP | CCSP | Mari...
20h •  

+ Follow

This article is also inspired by a man - **Tomasz Widomski** who has just graduated Cybersecurity Management MBA postgraduate studies at **Wojskowa Akademia Techniczna w Warszawie** (Military University of Technology in Warsaw, Poland) and shared his work with me recently.

Tomasz's work titled: "Analysis of the phenomenon of desynchronization as a new cyber weapon destabilizing national infrastructures" excellently expands the theme of time and time synchronization in the context of cybersecurity.

In short, why time and its synchronization are important - it is because there exist attacks on time domain. More follows in the article

Tomasz Brol, Grzegorz Kaczmarek 😎



#maritime #shipping #offshore #cyber #cybersecurity #security #vessels
#digitalization #transport #cyberstorm #badcyberweather #time
#time_synchronization #e-Czas #sextant



IS IT YOUR TIME?

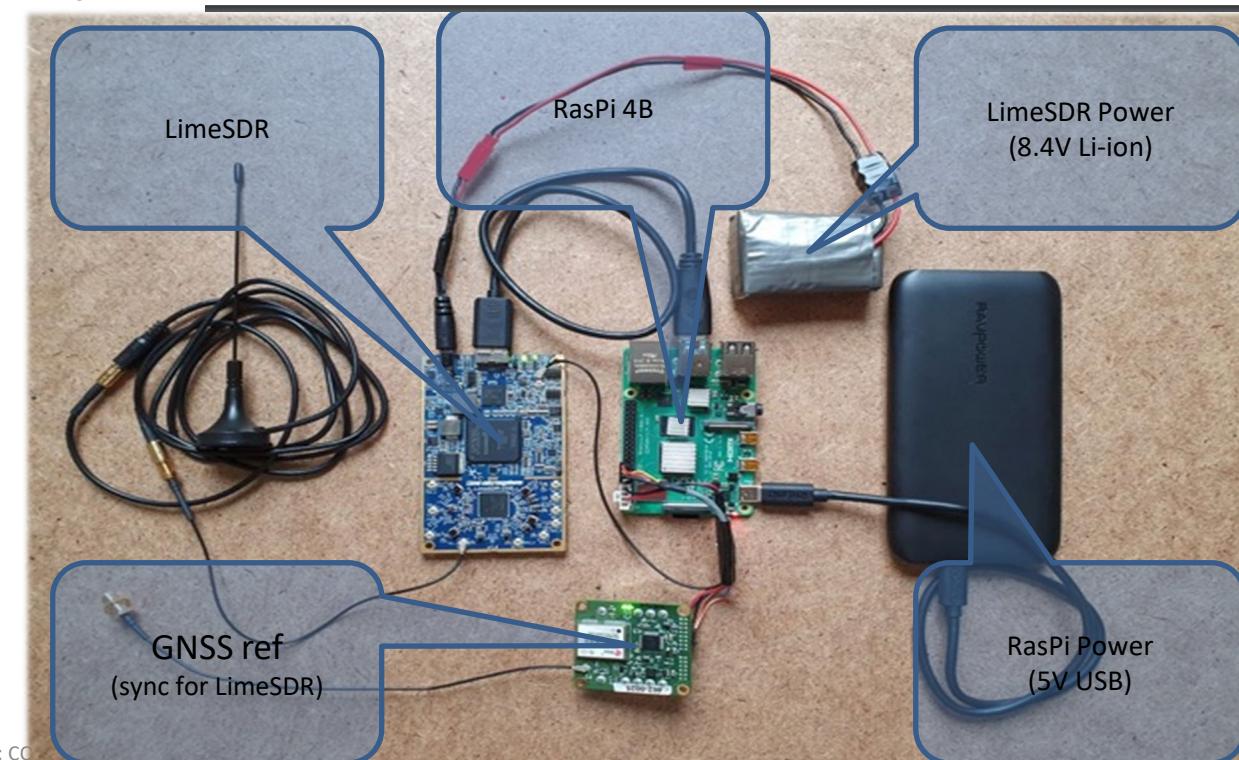
Is it your time?

Cyber Security for Time

- Not just threats from the network...
GNSS RF signal inherently vulnerable
- Jamming (DoS) - Spoofing (MITM)
- Space-based attacks,
Space Weather



Zero to Operational in 10 minutes With No GPS Expertise
Step By Step Instructions from a Script Kiddie on How to Download and Run a Spoofing App



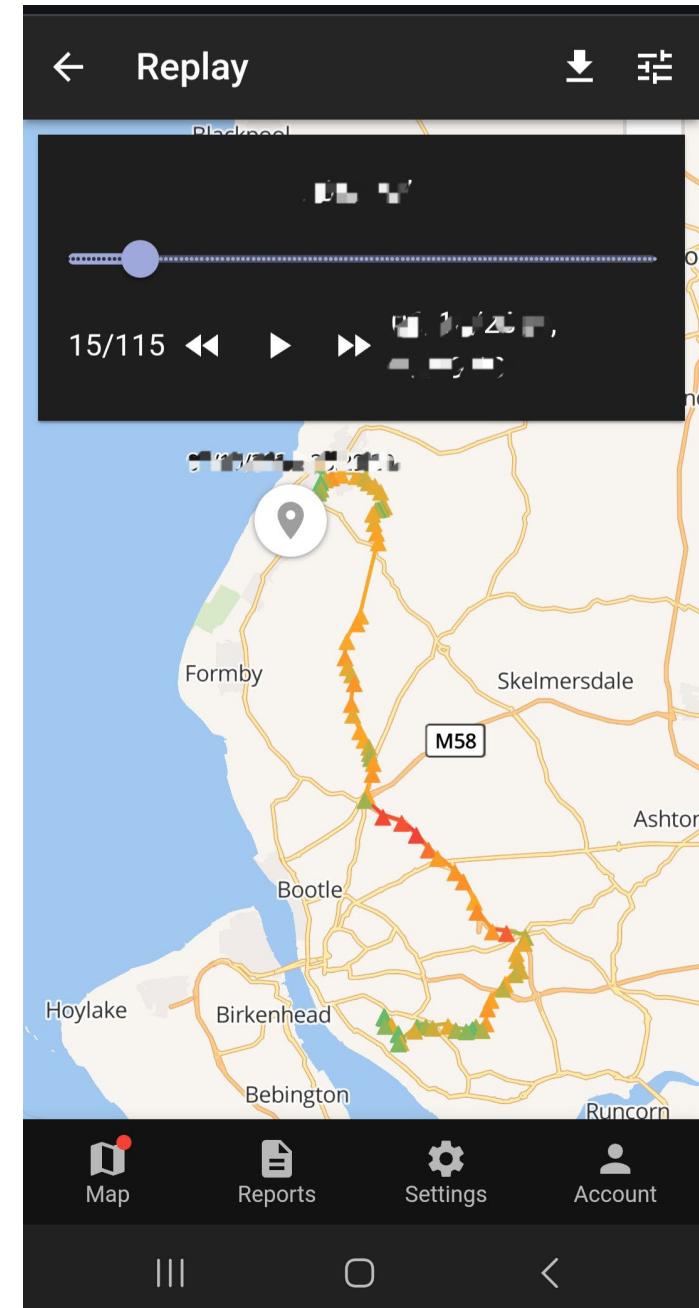
Time as an attack tool

- Cache timing attacks
- Race conditions - glitches
- Re-synchronisation attacks
(keys/random data valid at t_0
time-of-use, time-of-check)

- Kerchoff's Principle
- time broadcast in the clear
- crypto mechanism can be reduced in strength
(c.f. *bidding down*)
- reverse engineering of software/firmware yields keys

Designed Secure

- Zero Trust
 - Authenticate everywhere, make no assumptions
- Secure by Design
 - No secret algorithms, no backdoors, no excuses
 - Design to make reverse engineering difficult
 - Resilience by default:
 - Backup/diverse sync sources, holdover
 - **Hardware security: ARM CHERI/MORELLO**
(prototype SOCs available since 2022)



A woman with blonde hair, wearing a black fedora hat and a dark jacket, is looking down at a smartphone she is holding in her hands. The background is blurred, showing city lights and a traffic light, suggesting an urban night setting.

The Arm Morello research program led by Arm to create a more secure hardware architecture for processors of the future. Its unique architectural extensions are based on Arm's work with the University of Cambridge since 2015 on the CHERI (Capability Hardware Enhanced RISC Instructions) protection model.

Mitigations: ARM CHERI

<https://newsroom.arm.com/blog/morello>

The Morello program aims to assess the viability of the Morello Board, a prototype hardware system on chip (SoC) employing unique extensions to the conventional Arm hardware instruction set that significantly improve device security. The Morello Board serves as a real-world test platform for the deployment of more secure hardware architecture in processors of the future.

NIST IR 8425A (Initial Public Draft)

 Obsoleted on September 10, 2024
[8425A](#)

Recommended Cybersecurity Requirements for Consumer-Grade Router Products



Chances are you home have a wide internet-connected as computers, tablets, smartphones, printers and various Internet of Things (IoT) devices. Do

Routers cybersecurity best practices - ITSAP.80.019

D.med software

From: [Canadian Security](#)

October 2022 |

Alternate form of [cyber security best practices - ITSAP.80.019 \(Part 1\)](#)

The aim of this overview about the regulation of the cyber security of consumer-grade router products is to:

- IEC 80001-1: and security and use of devices or software – I risk management



National Cyber Security Center of Excellence

PAGE 40 OF 5

[GUIDANCE](#)

Cyber Security Standard IEC 606

D.med Software
Fri 11 Nov

Device Security Guidance

Guidance for organizations to choose, configure and use devices securely



Principles to support the design of connected devices

These devices

produced by the [Security Center](#) with the [Device Innovation](#)

help organizations that [enterprises](#) are protecting their cyber security

The primary

Pages

[Device Security](#)

[Platform Guide](#)

[Getting ready](#)

[Policies and set](#)

[Managing devi](#)

Core principles

Guides for the design of cyber secure systems

Pages

[Secure design principles](#)

[Cyber security design principles](#)

1. Establish the context before designing a system

2. Make compromise difficult

3. Make disruption difficult

4. Make compromise detection easier

5. Reduce the impact of compromise



[Virtualisation security design principles](#)





- <https://www.gov.uk/government/publications/secure-by-design-problem-book/secure-by-design-problem-book>

Guidance

Secure by Design Problem Book

Published 24 April 2025

Contents

[Introduction](#)

[Problem 1: how do we up-skill UK defence in 'Secure by Design'?](#)

[Problem 2: how does 'Secure by Design' account for unevenly distributed information and knowledge?](#)

[Problem 3: how do we incorporate 'Secure by Design' into the very earliest stages of capability acquisition?](#)

[Problem 4: how do we support 'Secure by Design' through life?](#)

Introduction

'Secure by Design' is becoming mandated across UK government for securing crown data and services. The 'Secure by Design' approach adopted by the Ministry of Defence (MOD) ensures security is designed into any project delivering capabilities or services, such that security is considered from the outset and through life.

Successful adoption of 'Secure by Design' requires a step change in design thinking about security. However, the range of military capabilities that need to be supported means its adoption within UK defence also introduces challenges not found in enterprise settings, or other parts of government. These include social and technical interoperability challenges, technical debt associated with legacy platforms, and the difficulties presented by operating capabilities in harsh and contested operating environments worldwide.

Cyber Time: Summary

- TETRA multiple failures in philosophy, implementation
- Zero Trust + Secure by Design
 - Architecture
 - Hardware, Software, Protocol including hardening against reverse engineering



```
Text Processor 14: REM::C::NOTES\TER1.C
// Copyright 2023, Midnight Blue.
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
// http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.

#include <stdio.h>
#include <inttypes.h>
#include <string.h>

#include "teal1.h"

const uint16_t g_awTealLutA[8] = { 0xDA86, 0x85E9, 0x29B5, 0x2BC6, 0x8C6B, 0x974C,
const uint16_t g_awTealLutB[8] = { 0x85D6, 0x791A, 0xE985, 0xC671, 0x2B9C, 0xEC92,
const uint8_t g_abTealSbox[256] = {
  0x9B, 0xF8, 0x3B, 0x72, 0x75, 0x62, 0x88, 0x22, 0xFF, 0xA6, 0x10, 0x4D, 0xA9,
  0x9F, 0x78, 0xF3, 0xB6, 0xA0, 0xCC, 0x17, 0xAB, 0x4A, 0x41, 0x8D, 0x89, 0x25,
  0xCE, 0x47, 0x35, 0x2C, 0x6D, 0xE7, 0x6A, 0xB8, 0xB7, 0xFA, 0x8B, 0x8B,
  0x23, 0xDE, 0x39, 0x6C, 0x1E, 0x8E, 0xED, 0x30, 0x73, 0xBE, 0xBB, 0x91, 0xCA,
  0x5F, 0xB9, 0xC0, 0x06, 0x34, 0x2A, 0x63, 0x4B, 0x90, 0x28, 0xAC, 0x50, 0xE4,
  0xA4, 0xD2, 0xD4, 0x96, 0xD5, 0xC9, 0x66, 0x45, 0xC5, 0x55, 0xDD, 0xB2, 0xA1,
  0x32, 0x2B, 0x3E, 0xB5, 0x5C, 0x54, 0x67, 0x92, 0x56, 0x4C, 0x20, 0x6B, 0x42,
```



Thank you for your attention

Cyber Time to Cyber Crime

Christian Farrow B.Sc(Hons) MIET MInstP AFRIN

Chris.Farrow@Chronos.uk :: @Chronos_ChrisF :: <https://chronos.uk>

