Cyber Time to Cyber Crime -

TETRA:BURST as a wake-up call for all Critical National Infrastructure

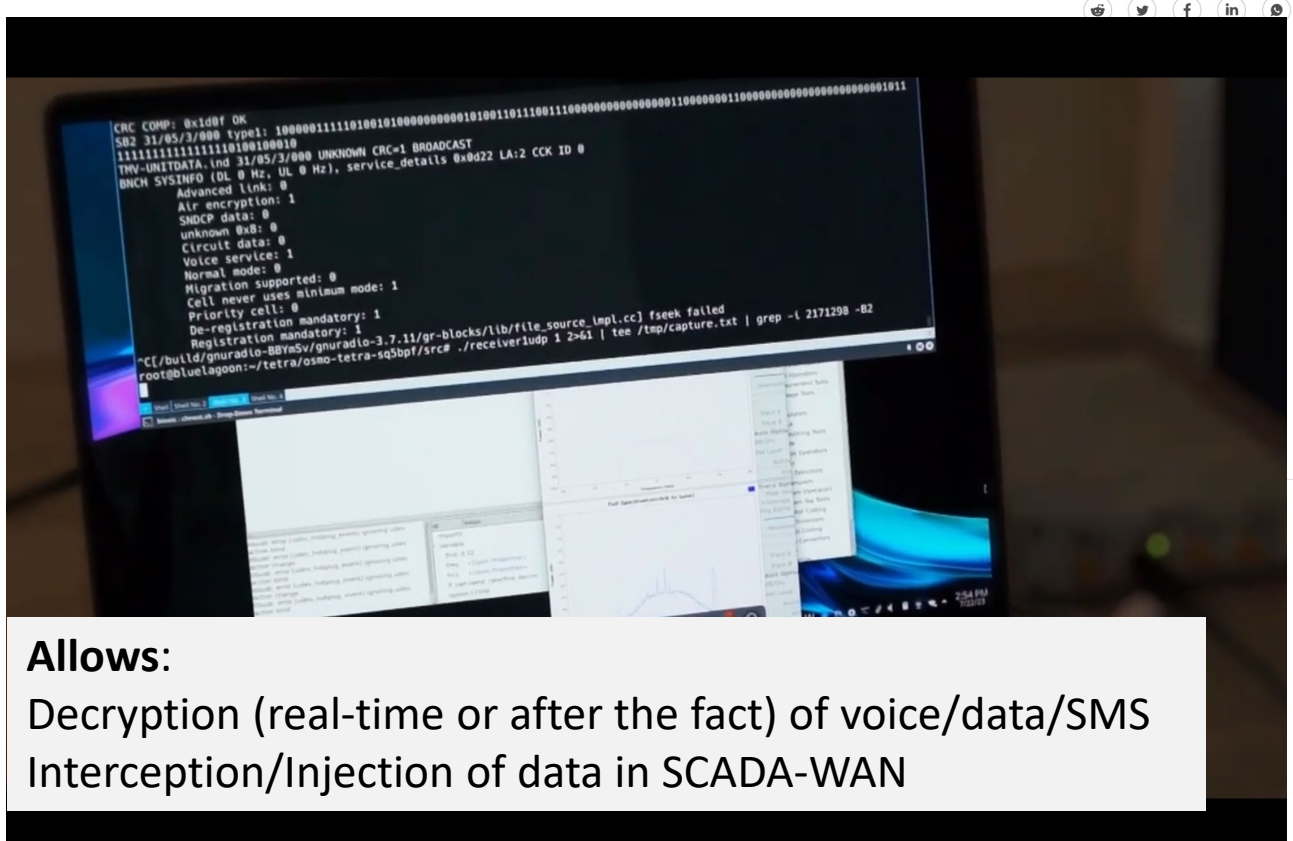
Christian Farrow

May 15th 2025

chronos TECHNOLOGY

Resilient Time – Time as an attack vector

- 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

09:49 Fri 3 Nov

theregister.com

SIGN IN / UP

The Register®

RESEARCH

60

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

Learn more

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.

Secure, proven TETRA - Sepura

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

Sepura

TETRA Overview - Hytera EU

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

Hytera EU

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 complet become the largest in the world, with
The Critical Communications Associat

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 ambulan
communication in emergency situatio

Transportation:
Rail transport, airlines, and other trans
secure communication.

Critical Infrastructure:
Energy and mining sectors utilize TET

Corporate Networks:
Large enterprises deploy TETRA for i
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:

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 complet become the largest in the world, with
The Critical Communications Associat

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, indu
Middle East	UAE, Qatar, Israel, Turkey	Public safety, military, critical infras
Africa	South Africa, Swaziland	Airports, public safety
Latin America	Mexico, Colombia, Chile	Police, emergency services, rail, for
North America	USA, Canada	Utilities, transport, public safety

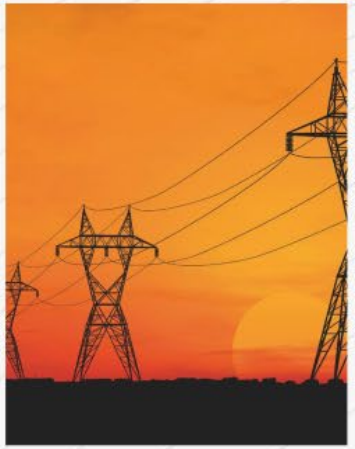
WSTS25, fasten your seat belts & hold on...

- 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?

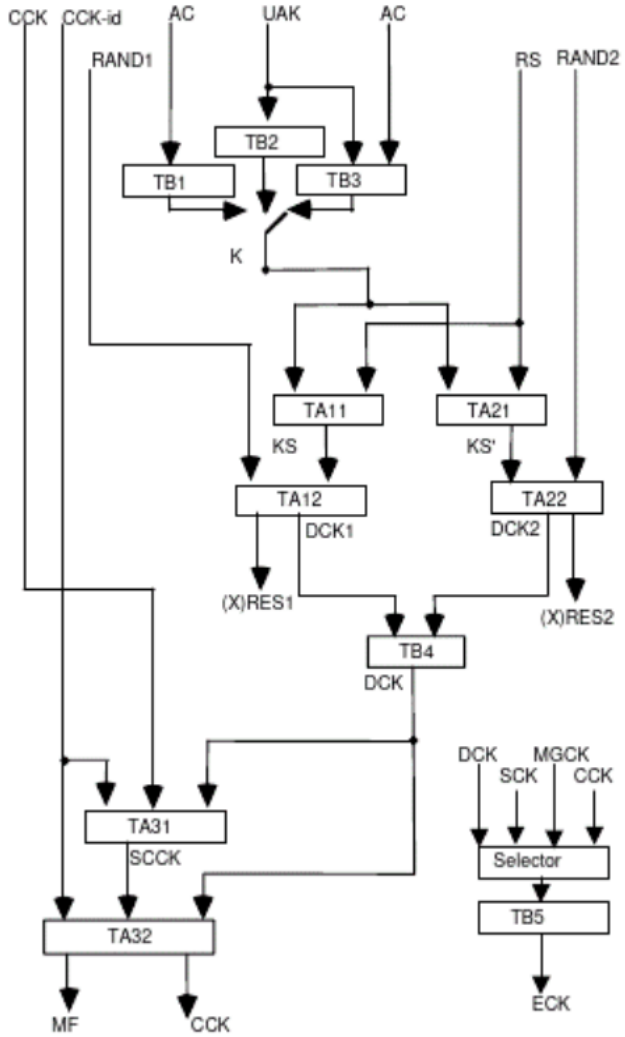
- Globally used radio technology
  - Competes with P25, DMR, TETRAPOL
- Standardized in 1995 by ETSI
  - Known for GSM, 3G/4G/5G, GMR, etc.
- Used for voice & data communications incl. machine-to-machine
- Relies on secret, proprietary cryptography






Open standard?

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



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

Kerckhoffs' principle

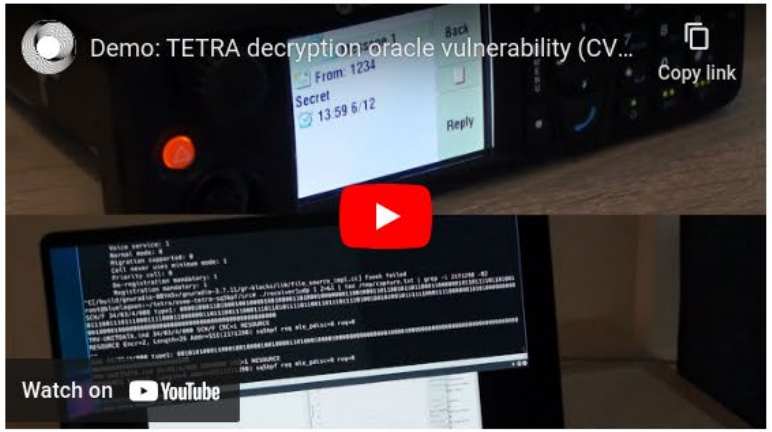
> "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."
>
> -Auguste Kerckhoffs, 1883

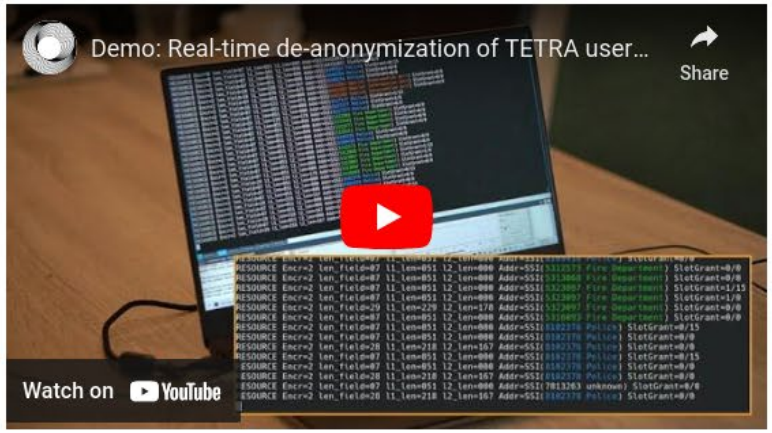
Violators don't fare well

- 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

CVE-2022-24401, CVE-2022-24404, CVE-2022-24402, and CVE-2022-24403 were validated and found practically exploitable in a lab setup with real TETRA radio and base station hardware.

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

6:33 / 1:10:12

16:26 92%

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

Ask follow-up...

ing MTM5400

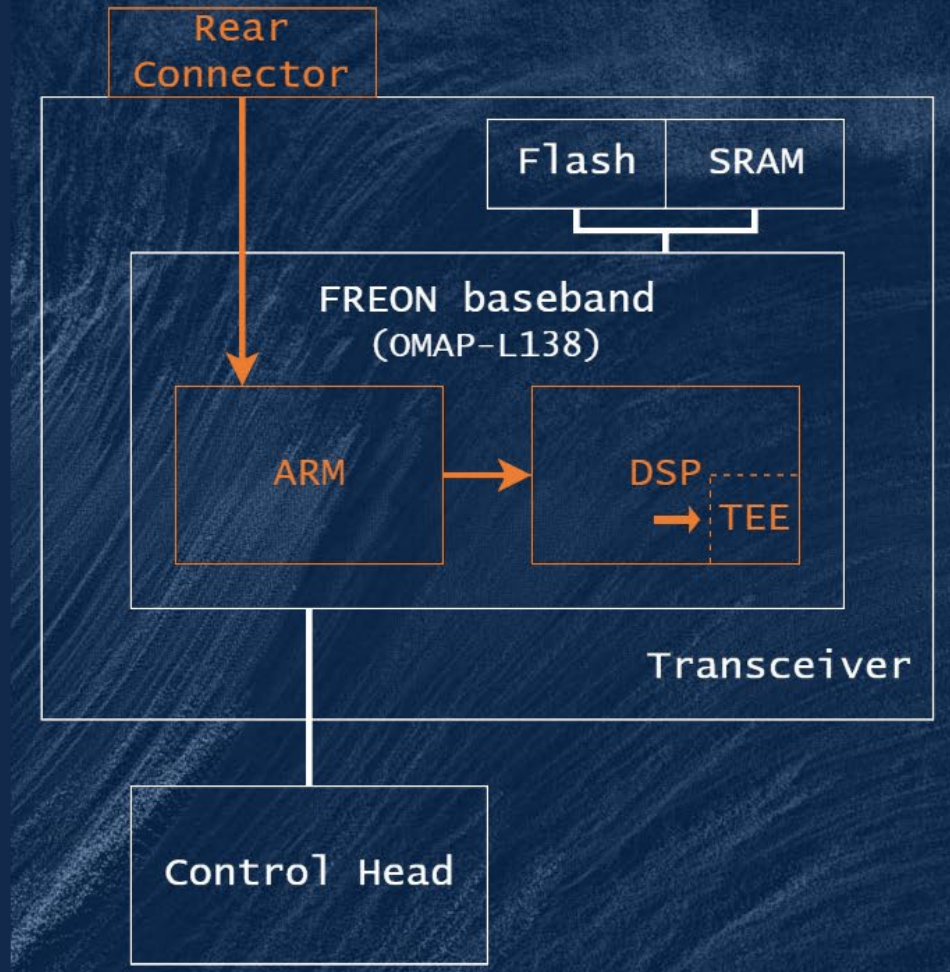
at string → code exec on AP

to DSP via shared memory

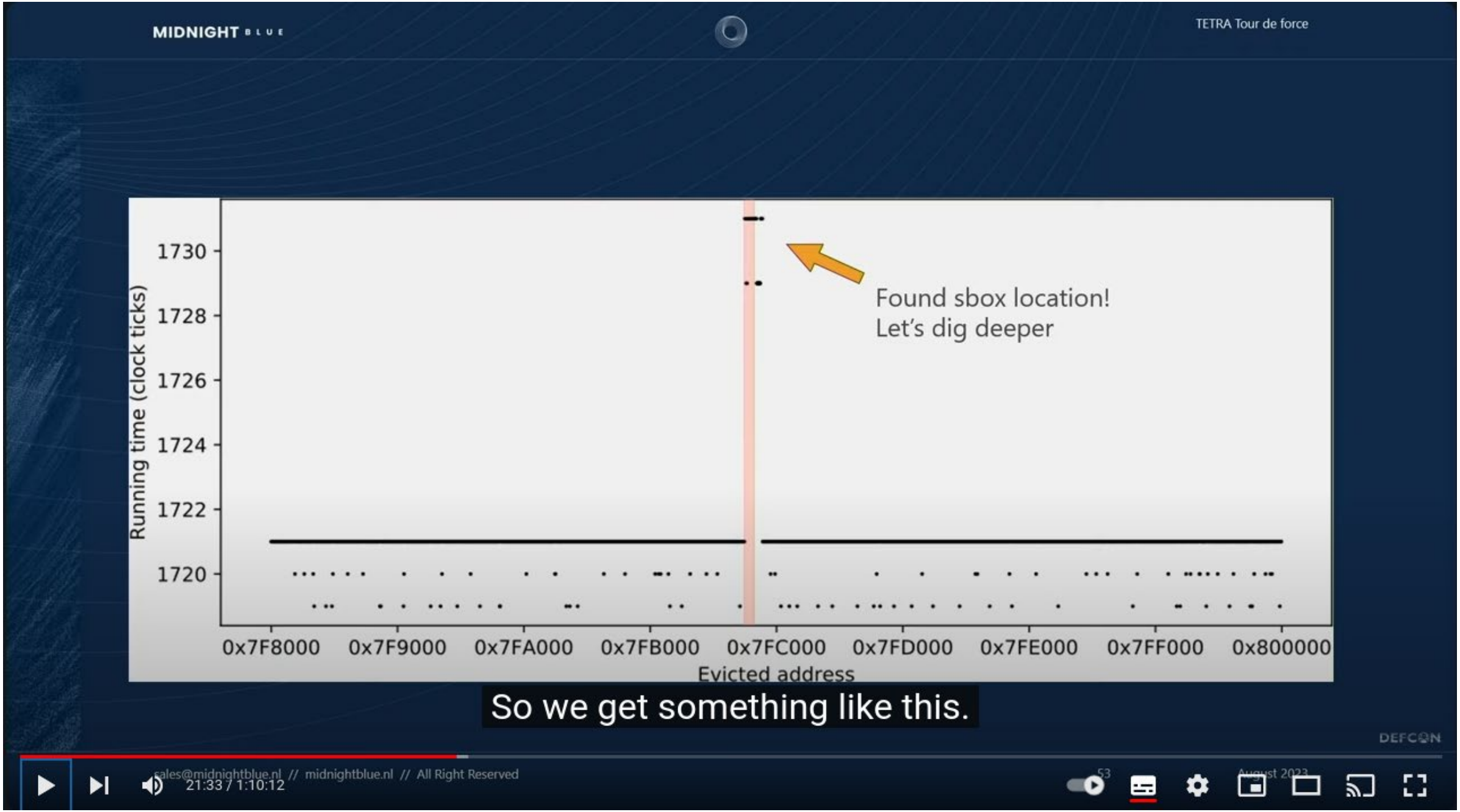
e timing side-channel on TEE

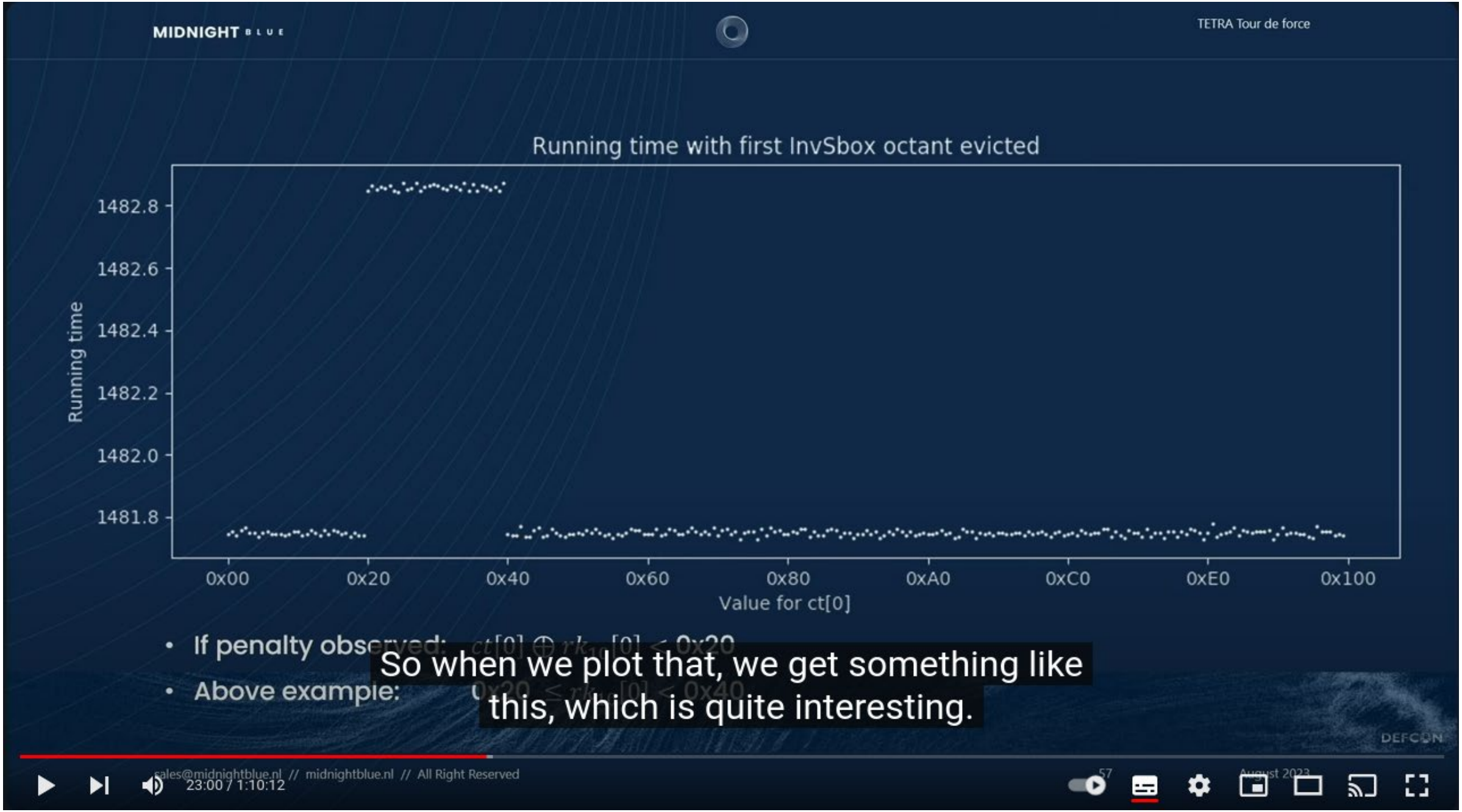
t algos!
d key extraction ...

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





MidnightBlueLabs / **TETRA_burst**

Type / to search

Code | Issues | Pull requests | Actions | Projects | Security | Insights

TETRA_burst

Public

Watch 44 | Fork 7 | Star 61

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

carlicious placeholder for release of tooling — 79056d0 · last year — 2 Commits

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

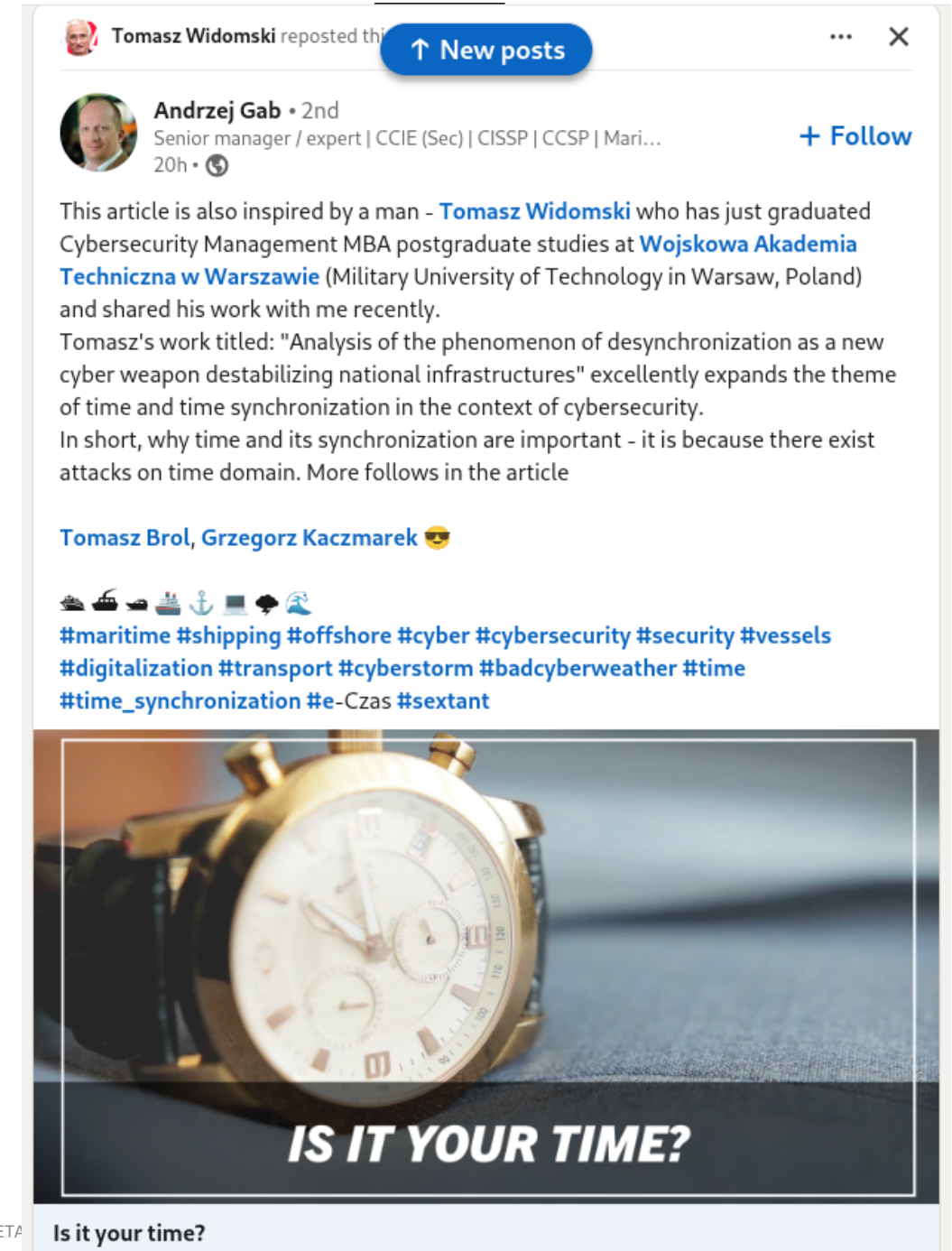
No releases published

Packages

No packages published

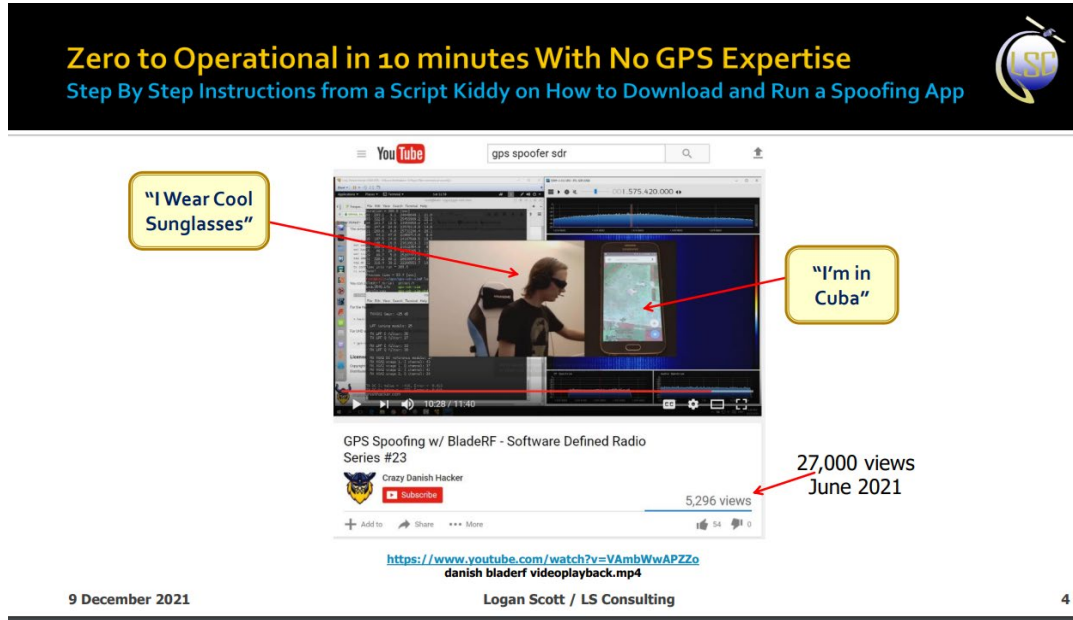
Time as an attack vector?

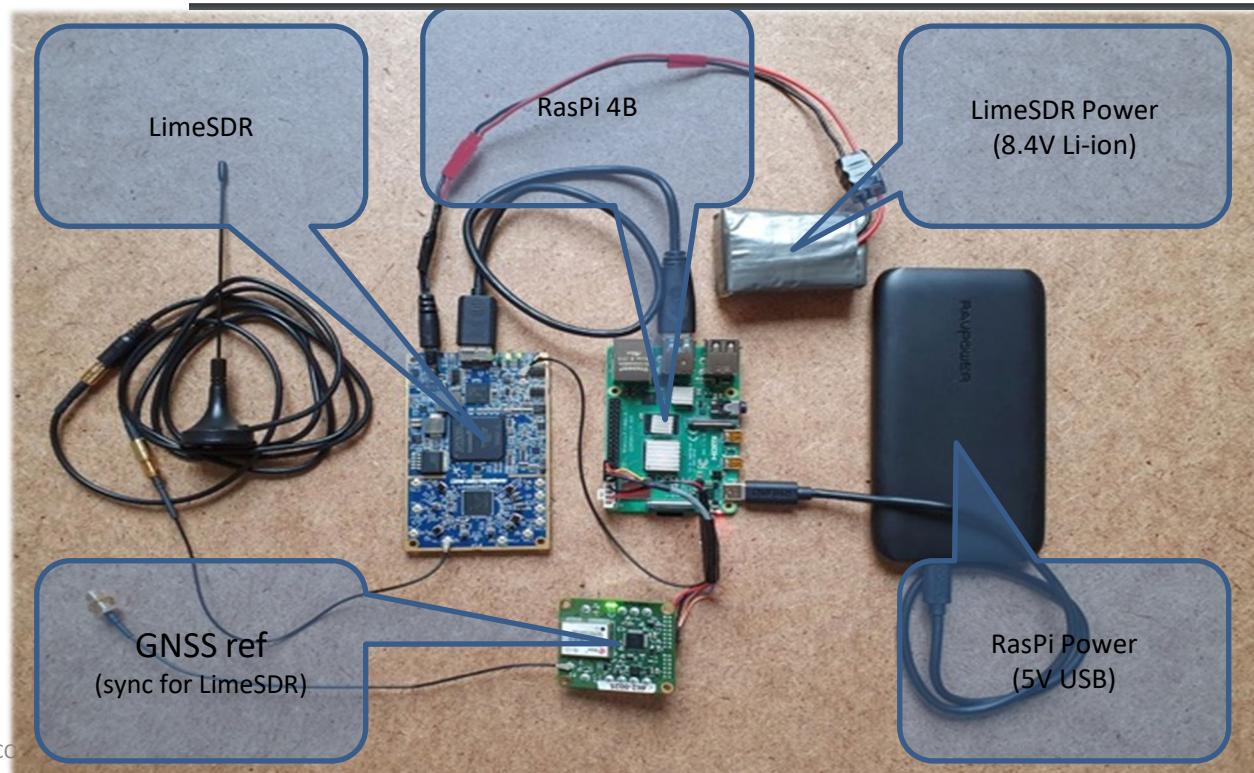
- Previous talks have focused on "de-synchronisation" attacks



Cyber Security for Time

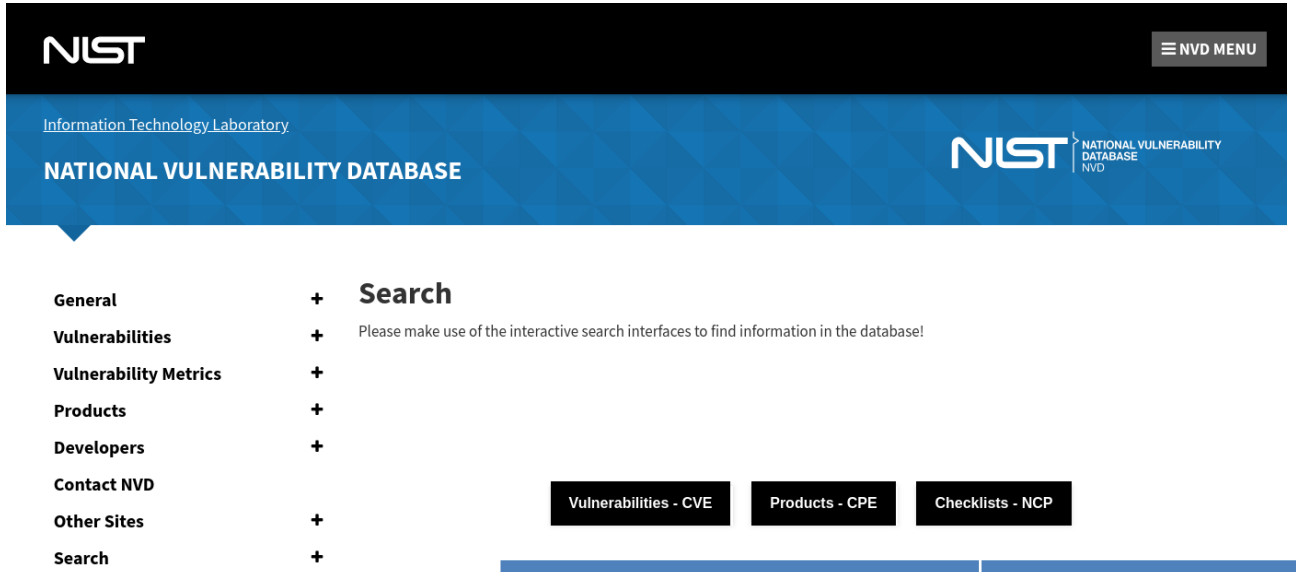
- Not just threats from the network... GNSS RF signal inherently vulnerable
- Jamming (DoS) - Spoofing (MITM)
- Space-based attacks, Space Weather





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*)

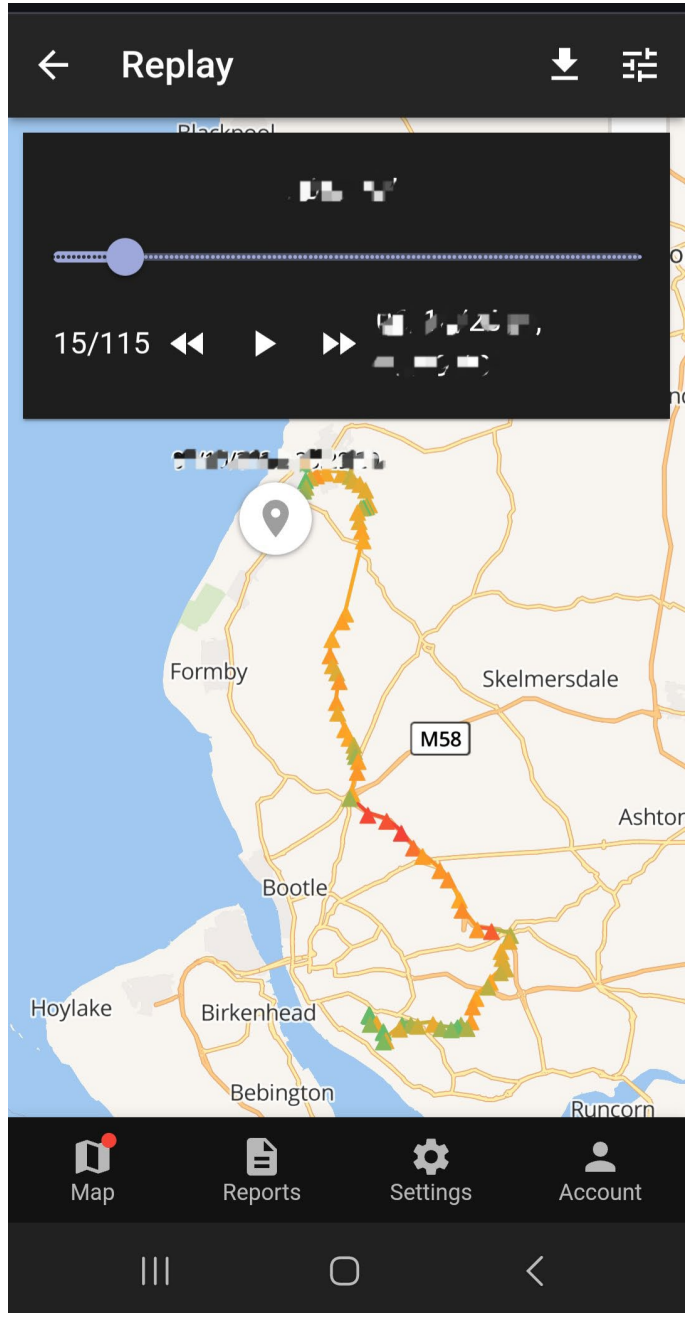


VULNS: (May 2024)		(Apr 2025)
GNSS	31	35
gpsd	9	10
chrony	11	12
PTP	36	57
NTP	201	221
SNMP	498	546

  - 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)



Mitigations: ARM CHERI

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

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.

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.

16:06 16:07 16:08 16:10 16:11 16:12 16:21 63%

NIST CSRC

Search CSRC

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

NIST IR 8425A (Initial Public Draft)

Obsoleted on September 10, 2024
8425A

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Routers cy security b practices - ITSAP.80.(

From: Canadian Security

October 2022 |

Alternate form cyber security b ITSAP.80.019 (P

Chances are you home have a wic internet-connect as computers, ta smartphones, pr and various Inte (IoT) devices. Ro

D.med software

Cyber Se Standar 81001-5 IEC 606(

D.med Software
Fri 11 Nov

The aim of this overview about the regulate the cyber Device, they are:

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

National C Security C

PAGE 40 OF 5

Device secu manufactu

GUIDANCE

Device S Guidanc

Guidance for or choose, configu securely

Pages

Device Security

Platform Guide

Getting ready

Policies and set

Managing depl

Principles to the design c connected d

These devic produced b Security Ce with the De Innovation help organi that enterp are protect cyber secur

The primary

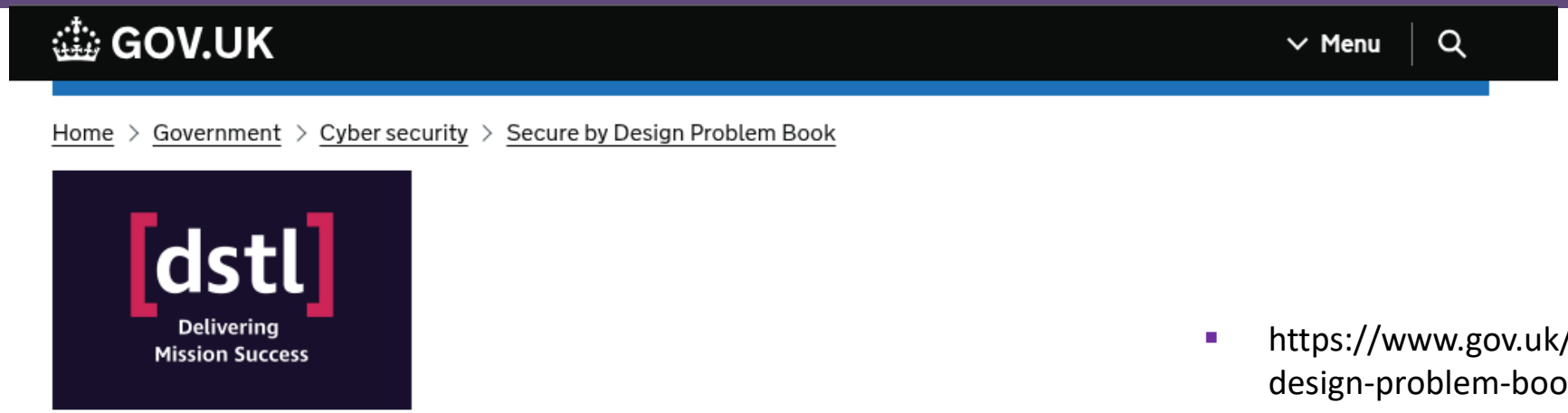
Co

- **UL 2900-1** addr security attribu
- **UL 2900-2-1** ac integration of s
- **IEC 81001-5-1** c management risks (which, in can help orgar types of risk ar manufacturer' to the custome their environm support custor
- **AAMI TIR 57** ac management risks and is infc in UL 2900-2-1.
- **ISO 13485** help nimize spec defects.

principles

Guides for the design of cyber secure systems

Pages



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

Cyber Time: Summary

- TETRA multiple failures in philosophy, implementation

- Zero Trust + Secure by Design
  - Architecture
  - Hardware, Software, Protocol including hardening against reverse engineering

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

CHRONOS TECHNOLOGY