



~#

The Great Seal Bug Historia, teoria i praktyka

Jacek Lipkowski
SQ5BPF



thehacksummit.com



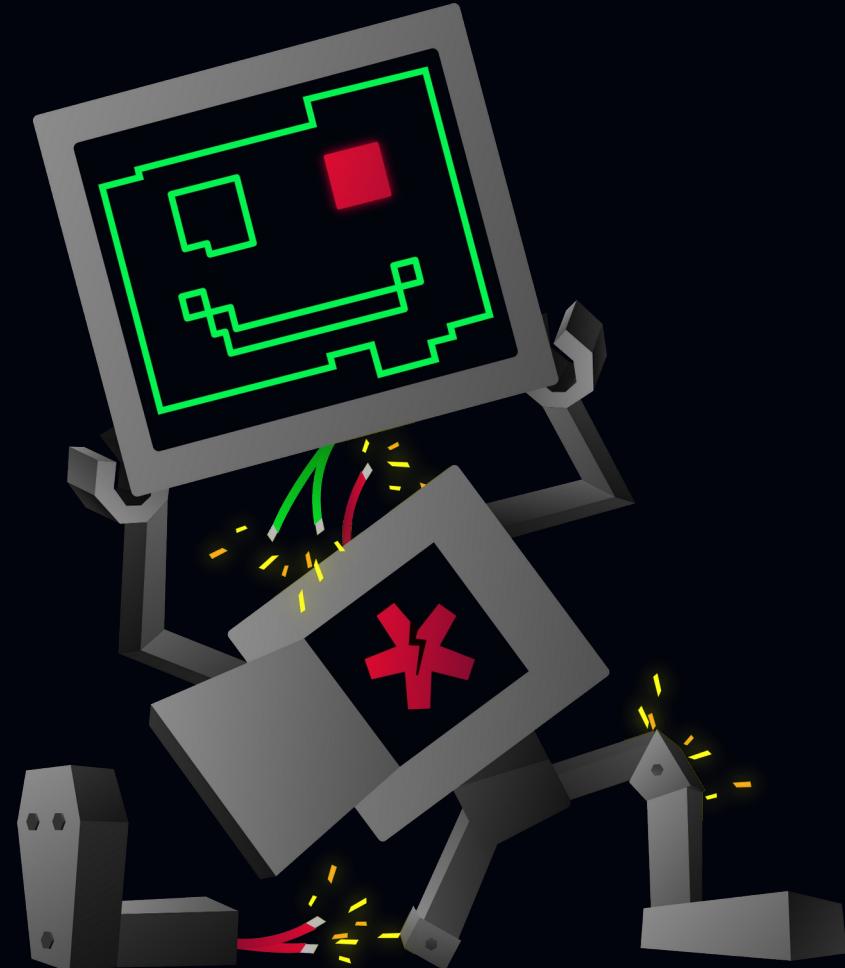
19-20 października 2023



PGE Narodowy
+ Online

ORGANIZATORZY:

ACADEMIC
PARTNERS



~\$ whoami

- Jacek Lipkowski SQ5BPF@lipkowski.org
- Hobby:
- Krótkofalarstwo. Znak SQ5BPF
- (licencja wydana w roku 1993, 30 lat!)
- Unixy, sieci. I ich psucie :) (około 25 lat)
- Elektronika (od zawsze)
- Pracuje w Instytucji Finansowej
- Prezentacja ta jest moja i nie wyraża poglądów pracodawcy.



O czym jest ta prezentacja?

"Great Seal Bug" znany również jako "The Thing"
(pasywny podsłuch mikrofalowy)

Wzmianki o nim są nadal na wielu konferencjach, nawet współczesnych

13th IEEE International Conference on RFID Technology and Applications <https://2023.ieee-rfid-ta.org/the-thing/>

"The Little Seal Bug" BlackHat Asia 2022 <https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-Nassi-The-Little-Seal-Bug.pdf>

"NSA Playset: RF Retroreflectors" DEFCON 22

- Historia
- Zasada działania
- Praktyka :)
- I dalsza historia (aż do czasów teraźniejszych)

Historia

Prezent od rosyjskich
Pionierów w 4 sierpnia 1945 dla
ambasadora USA w Moskwie

„Gest przyjaźni” do sojusznika w
wojnie z państwami Osi

Piękna drewniana replika Wielkiej
Pieczęci Stanów Zjednoczonych

Wisiała do 1952 w biurze
w Spaso House
(rezydencja ambasadora)



Rok 1952

Wedle różnych źródeł, anglicy już wcześniej informowali o możliwym podsłuchu.

W 1952 roku technik używał prostego odbiornika detektorowego do wykrywania podsłuchów.

I okazało się że słyszy głosy ze spotkania w gabinecie ambasadora.



By Austin Mills - IMG_0214, CC BY-SA 2.0, <https://commons.wikimedia.org/w/index.php?curid=596727>

Great Seal Bug

W środku znaleziono coś, „The Thing”

- Nikt wcześniej czegoś takiego nie widział
- Nie wiadomo jak to działa
- tylko metal i plastik
- nie wymaga zasilania, więc może działać latami
- nie podłączone kablami
- w pełni pasywne, brak lamp i półprzewodników
- wymaga jedynie „oświetlenia” nadajnikiem (to odkryto później)

Dalsza historia

Podobno informacje o podsłuchu były wcześniej (1951), a wiadomo było że i tak wszystko jest podsłuchiwanie.

Być może pozostawiony w celu dezinformacji?

„The things he said convinced me that he had indeed had access to information on the discovery of that device and another device in **Warsaw**. ”

„The story says that more than a **100 similar bugs were found**.”

Dużo (sprzecznych) opisów. Część z powodu utajnienia, część pewnie z powodu przypisywania sobie zasług, część pewnie dezinformacja.

Absolutnie najlepsze opracowanie na stronie Murray Associates:

<https://counterespionage.com/great-seal-bug-part-1/>

<https://counterespionage.com/great-seal-bug-part-2/>

<https://counterespionage.com/great-seal-bug-part-3/>

<https://counterespionage.com/great-seal-bug-part-4/>

<https://counterespionage.com/great-seal-bug-part-5/>

W 1 maja 1960 roku rosyjanie zestrzelili U-2 (samolot szpiegowski CIA).

Spowodowało to skandal dyplomatyczny.

Jako przeciwwagę USA pokazało podsłuch na Radzie Bezpieczeństwa ONZ w Paryżu 26 maja 1960.

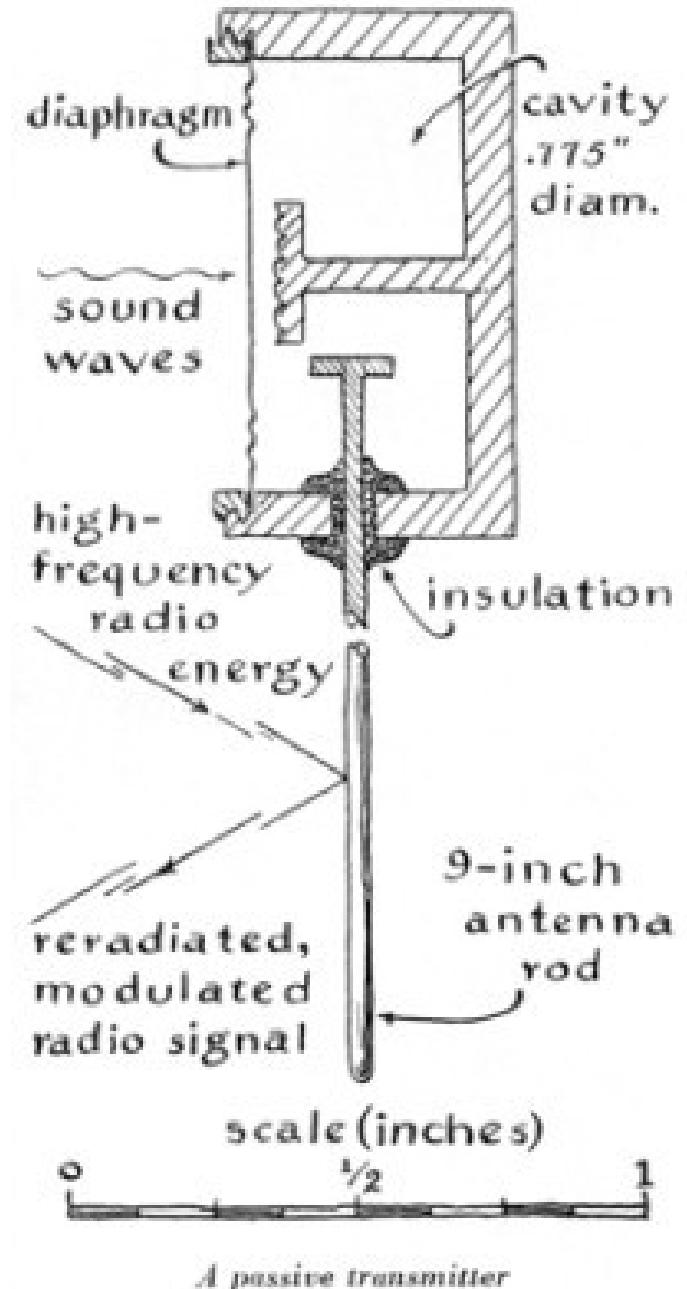
„The Thing” został ujawniony.



Scientific American (u nas wydawany jako Świat Nauki) opublikował w numerze z marca 1968 roku opis.

Mało szczegółów, ale dosyć dokładny obrazek.

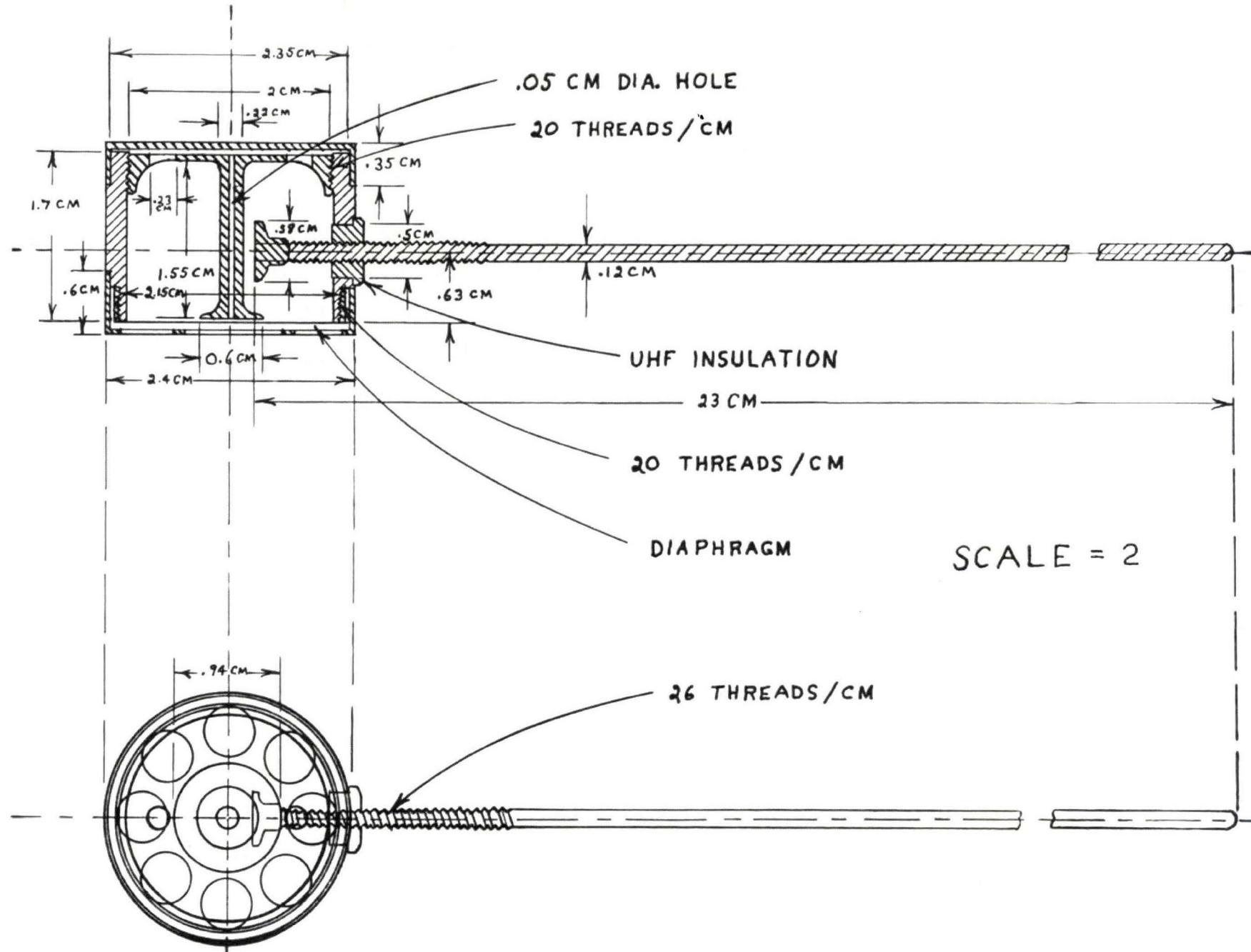
Wystarczająco szczegółowy aby odtworzyć to urządzenie.

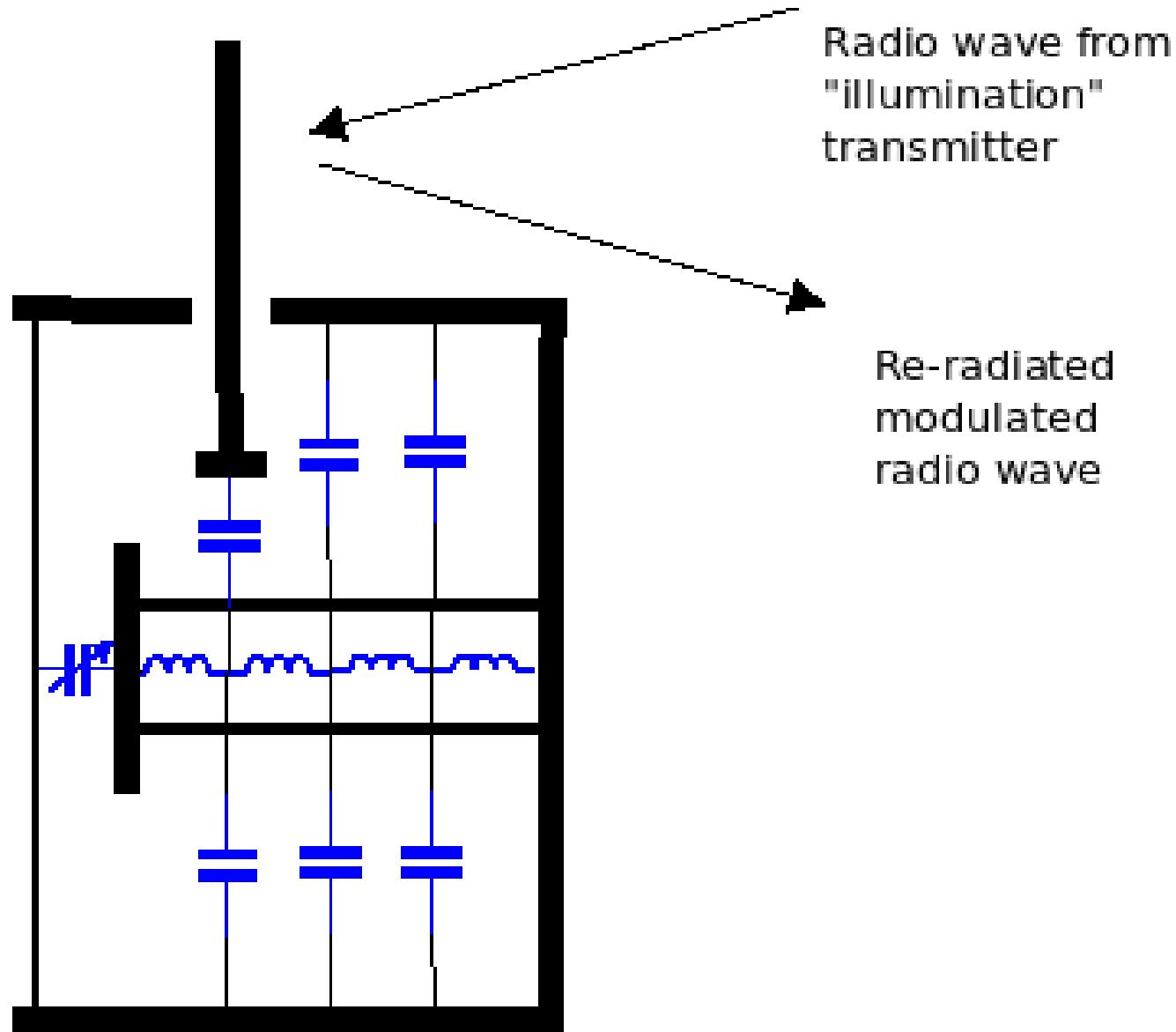
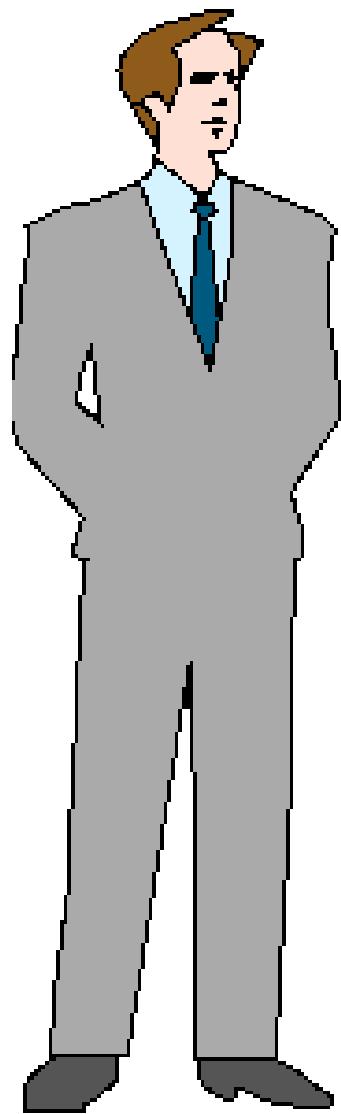


Inne publikacje

- „Spycatcher” („Łowca Szpiegów”) Peter Wright
- <https://www.cryptomuseum.com/cover/bugs/thing/>
- W 2019 roku FBI odtajniło raport z 1952 roku (67 lat później!)
https://www.cryptomuseum.com/cover/bugs/thing/files/GREAT_SEAL_BUG.pdf
- Wiele innych (ale najlepsze z Murray Associates)

Zasada działania





Radio wave from
"illumination"
transmitter

Re-radiated
modulated
radio wave

Drgania membrany mikrofonu powodują zmianę pojemności elektrycznej

Zmiany pojemności przestrajają częstotliwość rezonansową obwodu

Zmiana impedancji obwodu powoduje zmiany siły sygnału wypromienowanego z powrotem przez antenę

Czyli głoś powoduje modulację amplitudy

- Otwory z tyłu „puszki”, dzięki temu membrana nie jest tłumiona
- Antena o długości $N^* \frac{1}{2}$ długości fali
- Częstotliwość pracy około 1.7GHz (długość fali około 17cm). Bardzo zaawansowana technologia jak na tamte czasy!
- Bardzo cienka membrana (łatwa do uszkodzenia)
- Wnętrze posrebrzone (mniejsze straty)

Dlaczego to była taka nowość?

- W pełni pasywne urządzenie, metal i plastik
- Bezprzewodowe
- Niewykrywalne przez 7 lat (a na pewno sprawdzano „prezenty” od rosjan :)
- „Kosmiczna” technologia w kraju w którym zwykła toaleta nie była na porządku dziennym. Obecnie (78 lat później) częstotliwość 1.7GHz nie jest łatwa do opanowania przez wielu krótkofalowców, wtedy wywiad USA miał problemy z kupieniem sprzętu „z rynku” żeby wykrywać takie podsłuchy.
- Koncepcja mogła być użyta do wielu innych urządzeń (i jest :)

Praktyczna implementacja

:)

„This device is simple in concept but very complex in construction.”
<https://counterespionage.com/great-seal-bug-part-1/>

Repliki były już robione:

- (raczej tylko) eksponat z muzeum NSA
- eksponat z <https://www.vintagespycraft.com/>

Dopiero niedawno pokazano działające repliki:

- Uniwersytet w Bordeaux prezentowany na WPW 2022 (czerwiec 2022, zrobiony w 2021)
- Moja replika prezentowana w październiku 2022
- Neil Smith G4DBN dla programu BBC

“The Great Genius of Modern Life”
(prezentowane około marca 2023)



A może by też byśmy mogli?



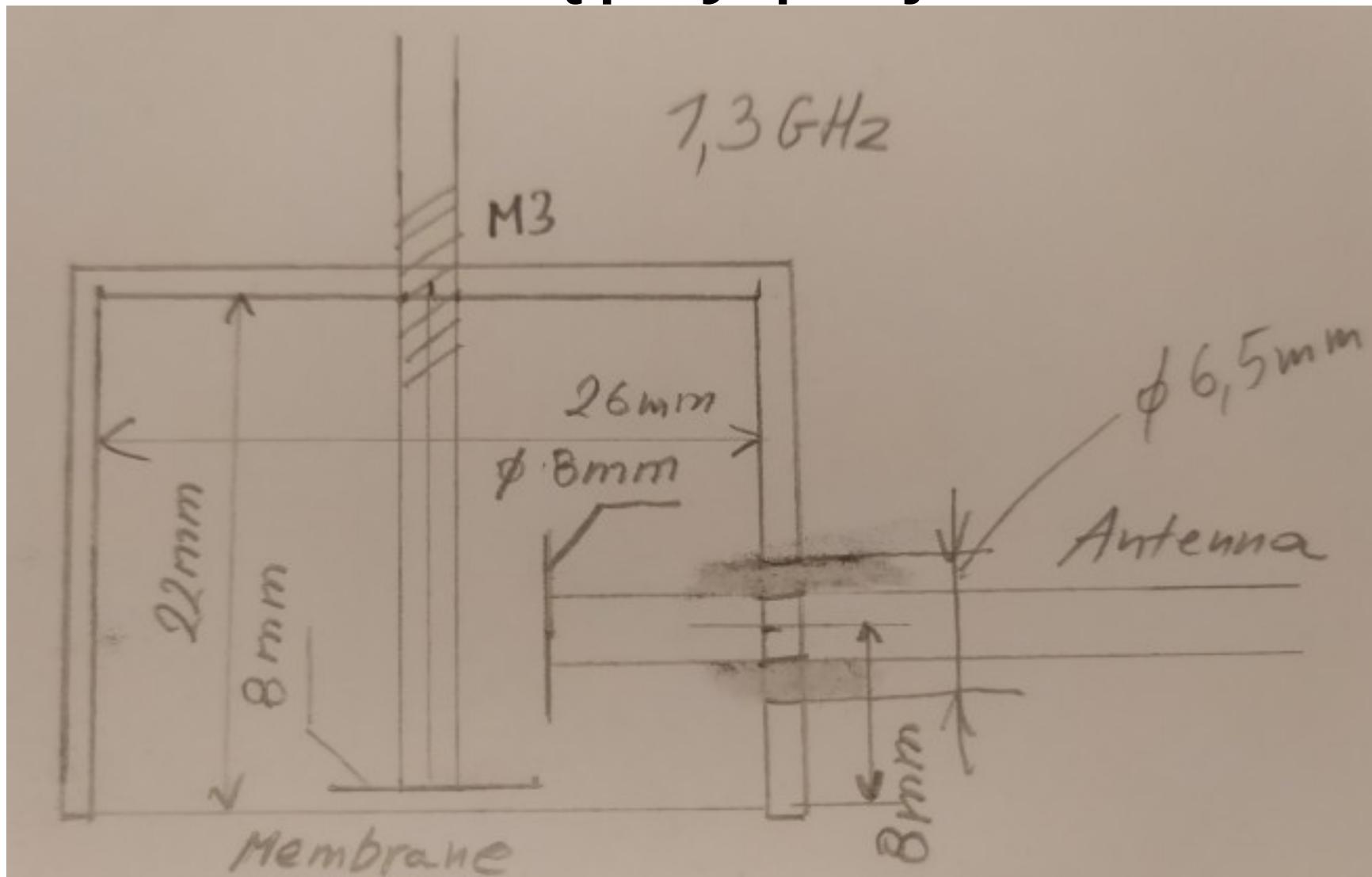
Super-tajna kiedyś-ultra-nowoczesna technologia wojskowa. Wszyscy o tym piszą ale nikt tego nie robi. Czy damy ją radę zbudować?

- Małe fundusze
- Brak drogiego sprzętu
- Jesteśmy amatorami, nie wiemy co robimy
- Jesteśmy amatorami, nie wiemy że czegoś się nie da zrobić.
- Elektronika mikrofalowa i odbiorniki (SDR) są teraz tanie i dostępne
- Mamy tanie części z Aliexpress, srebrną taśmę i mnóstwo inwencji
- Spróbujmy sami to zrobić praktyczną implementację

Założenia

- Orginal działał na 1700MHz (długość fali ok 17cm)
- U nas częstotliwość pracy w paśmie amatorskim 23cm (1240-1300MHz).
- Wszystkie wymiary mnożymy przez $1700 \text{ MHz} / 1296 \text{ MHz} = 1.3$
- Używamy najtańszych materiałów

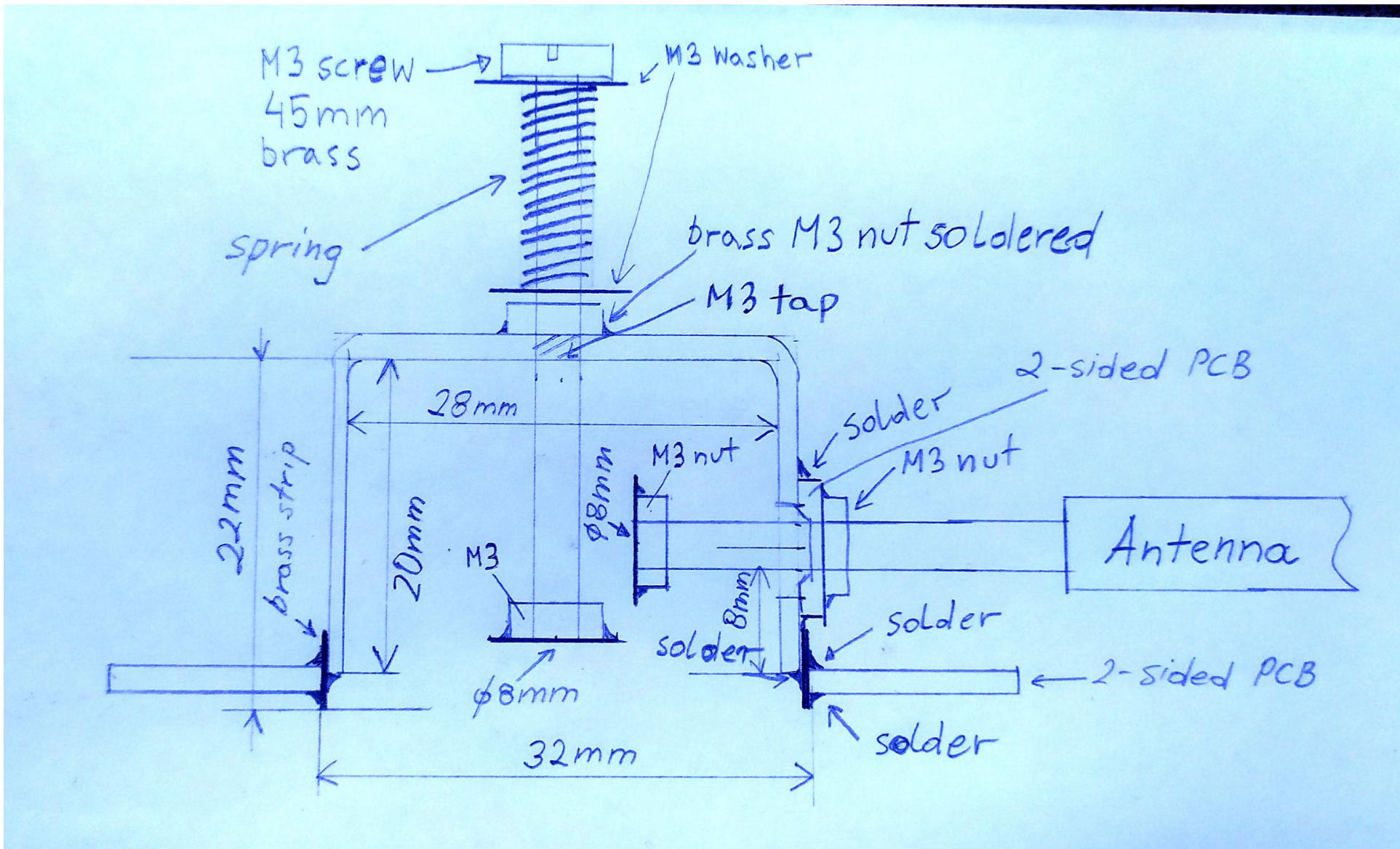
Wstępny projekt



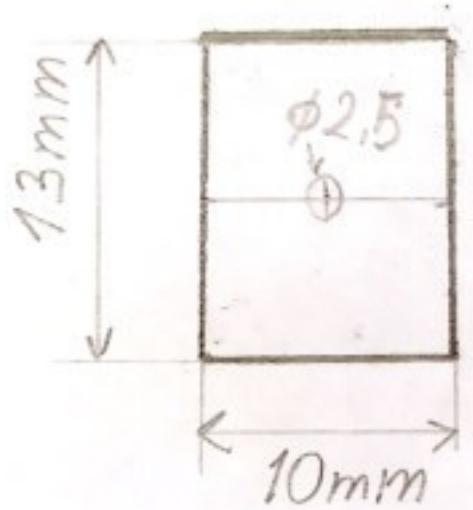
Puszka z zaślepką do rur 28mm



Poprawiony projekt

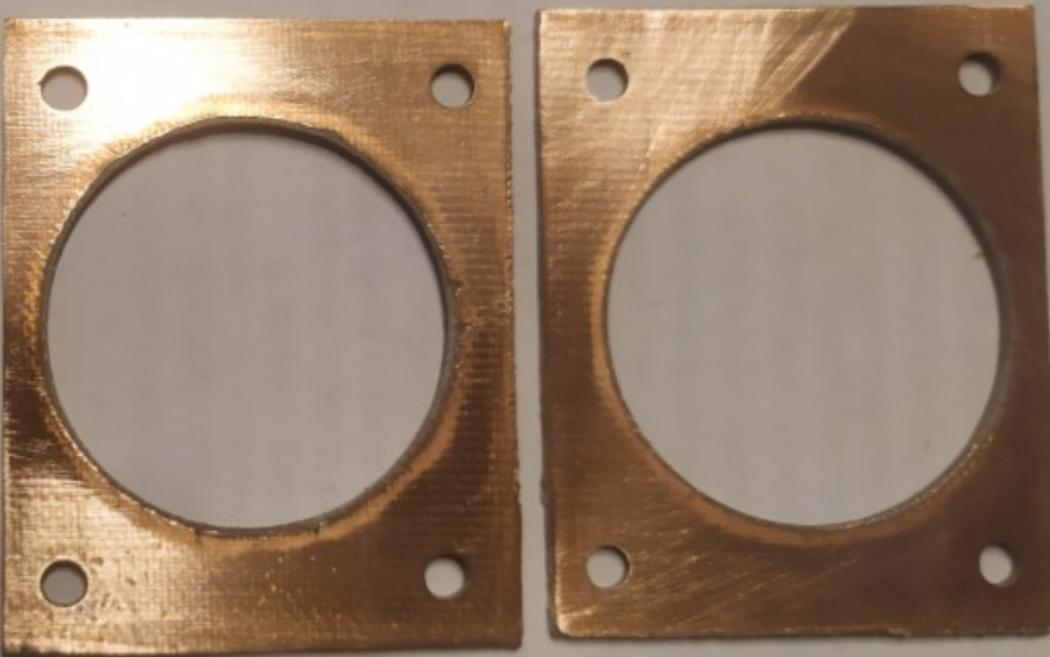
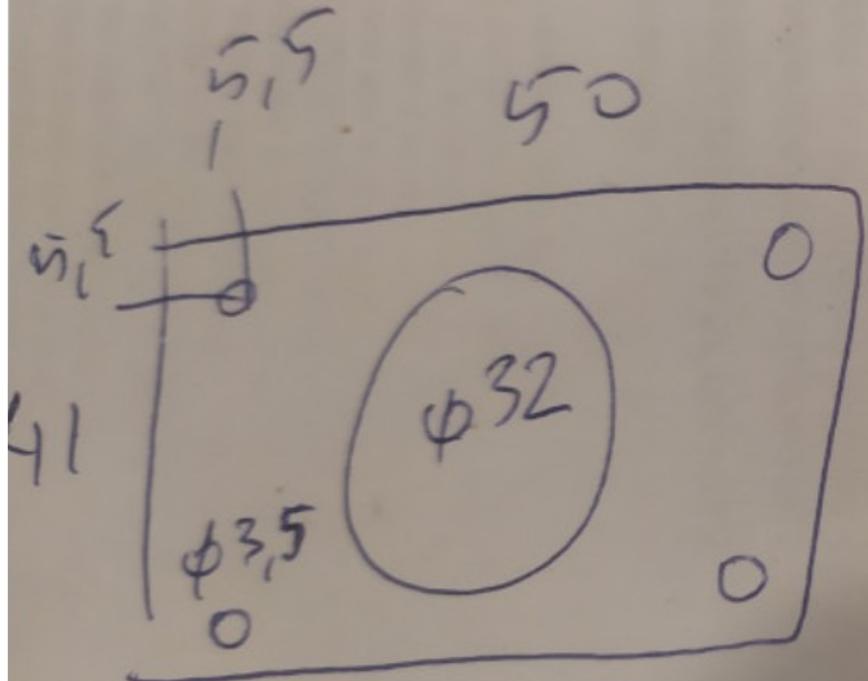


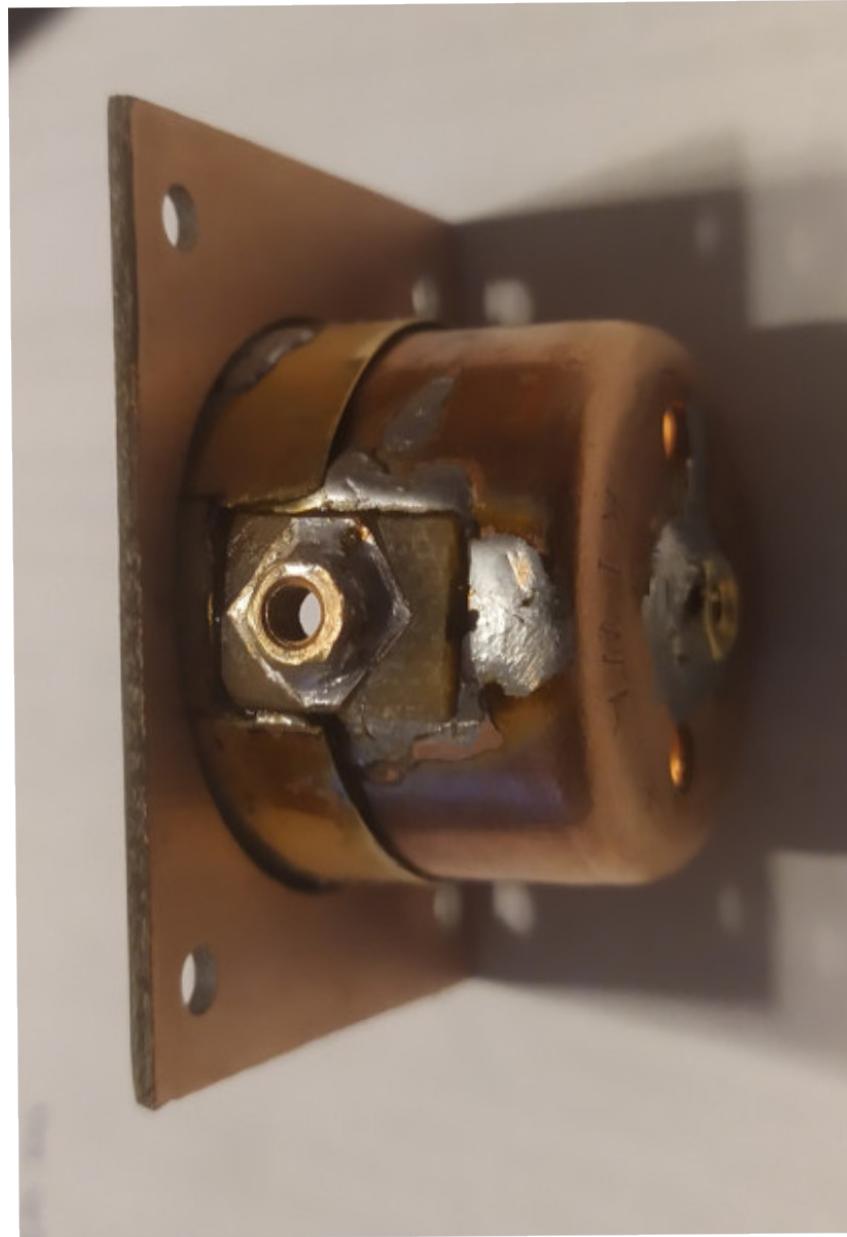
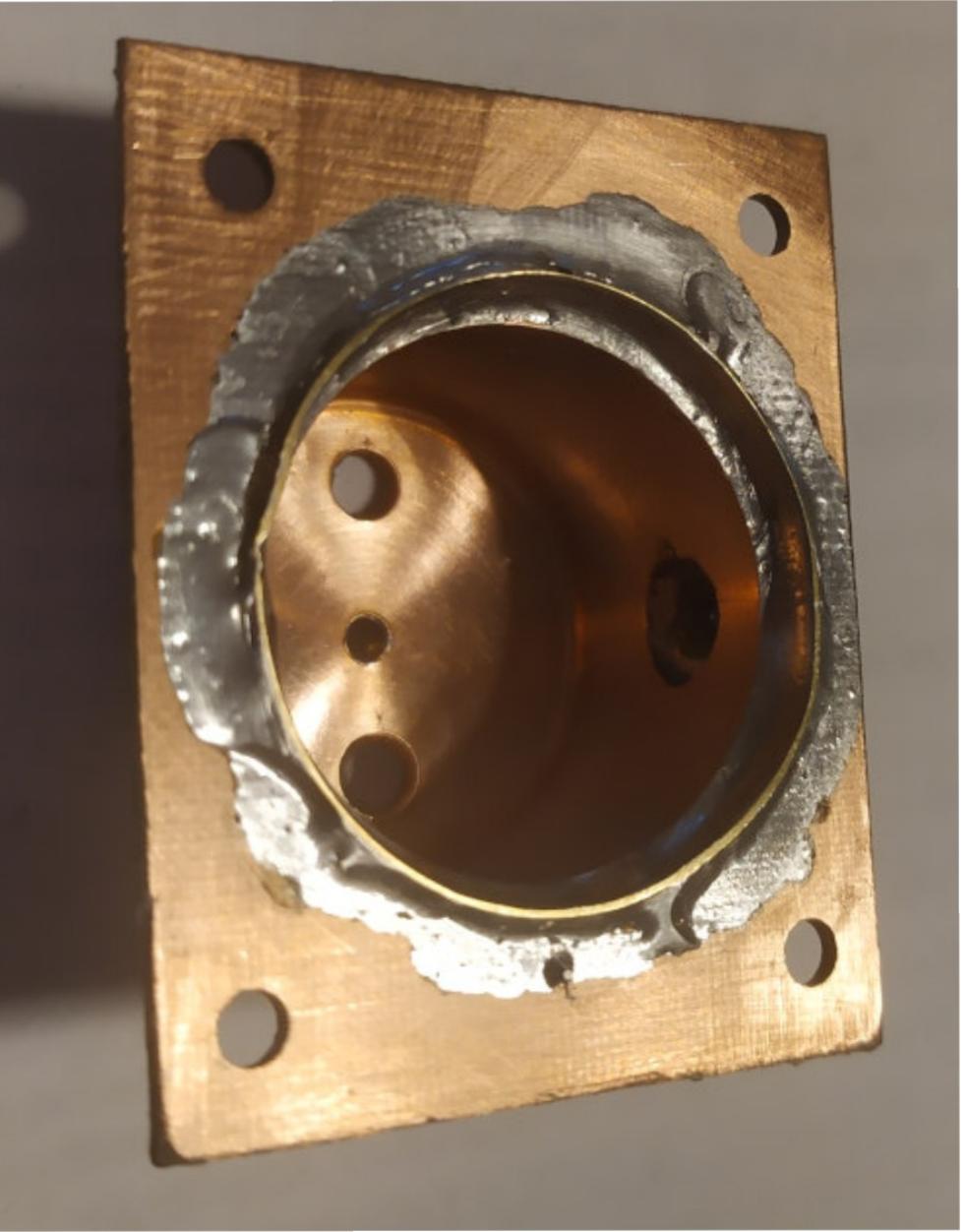










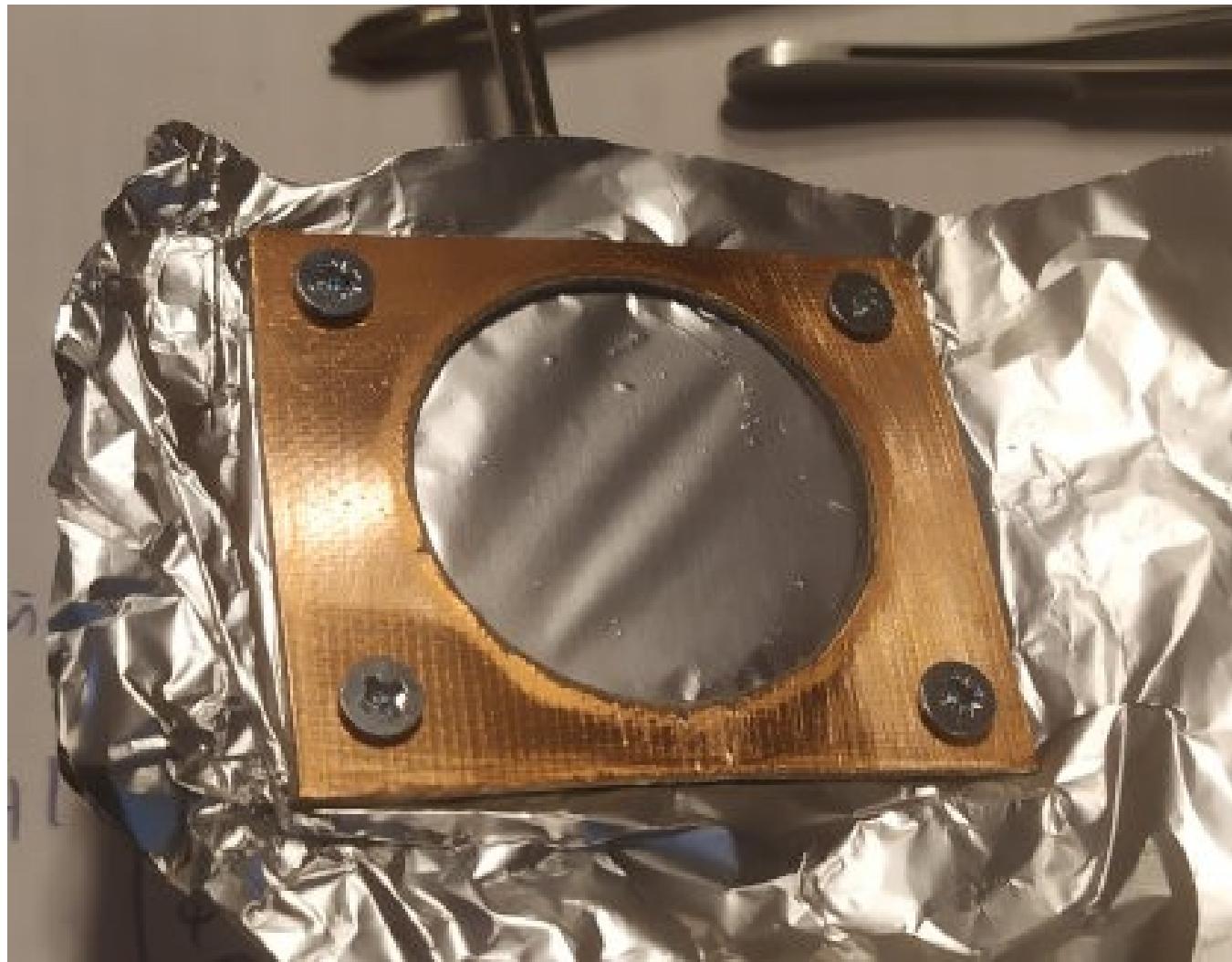




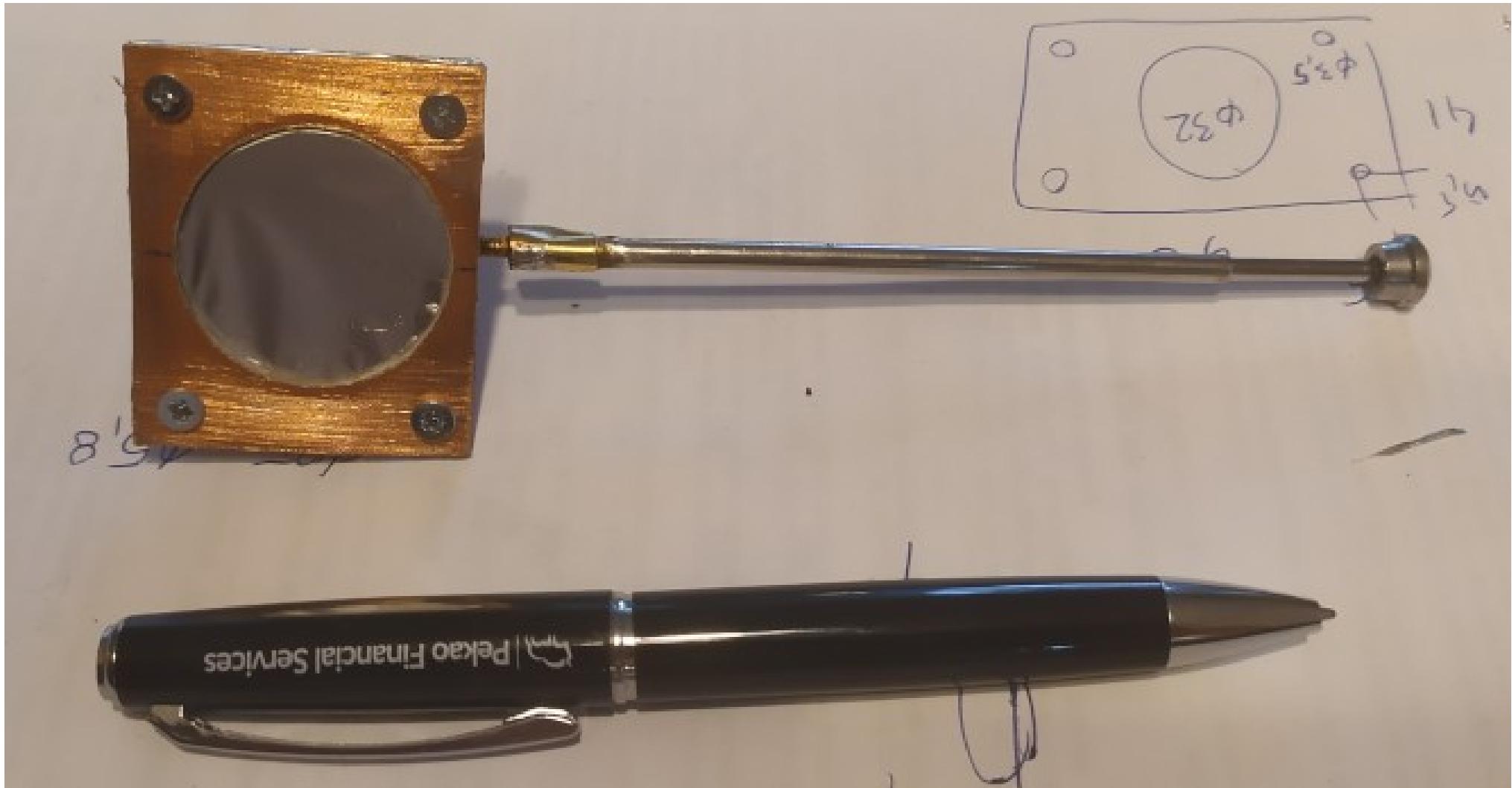
Już zaczyna wyglądać :)



Membrana z kiepskiej folii spożywczej



I mamy tajny zimnowojenny podsłuch :)



DEMO !

**Jak to wygląda
w środku**

Uruchomienie

Źródło sygnału

„ADF4351 signal generator”

Moduł generatora
35 MHz – 4.4 GHz
z Chin

Około 150zł na aliexpress
(październik 2023, w lutym 2021
było 80zł)



Wzmacniacz

Moduł wzmacniacza na SPF5189
z Chin

Wzmacnia sygnał z generatora do
około 50-70mW mocy wyjściowej

Nie jest konieczny do prób „na
biurku”

Około 25zł na Aliexpress
(drożeje! było 12zł).



Anteny

Wybrałem najtańszą
antenę LPDA do
zastosowań GSM

Pasmo ok. 800 MHz –
2.6 GHz

Zysk ok. 10dBi

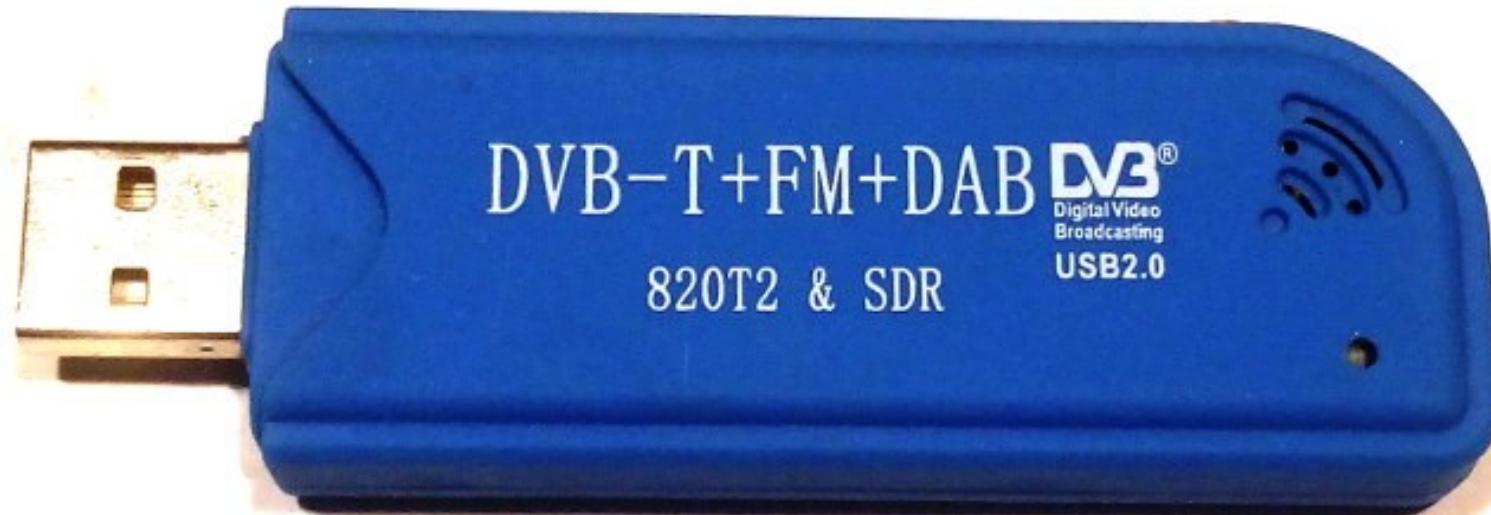
Około 100-150zł na
Aliexpress (też drożeje!)



Odbiornik

Jako odbiornik najtańszy SDR z tunera telewizyjnego na układach RTL2832 i R820T (albo R820T2).

Oprogramowanie np GQRX (pod linuxem)



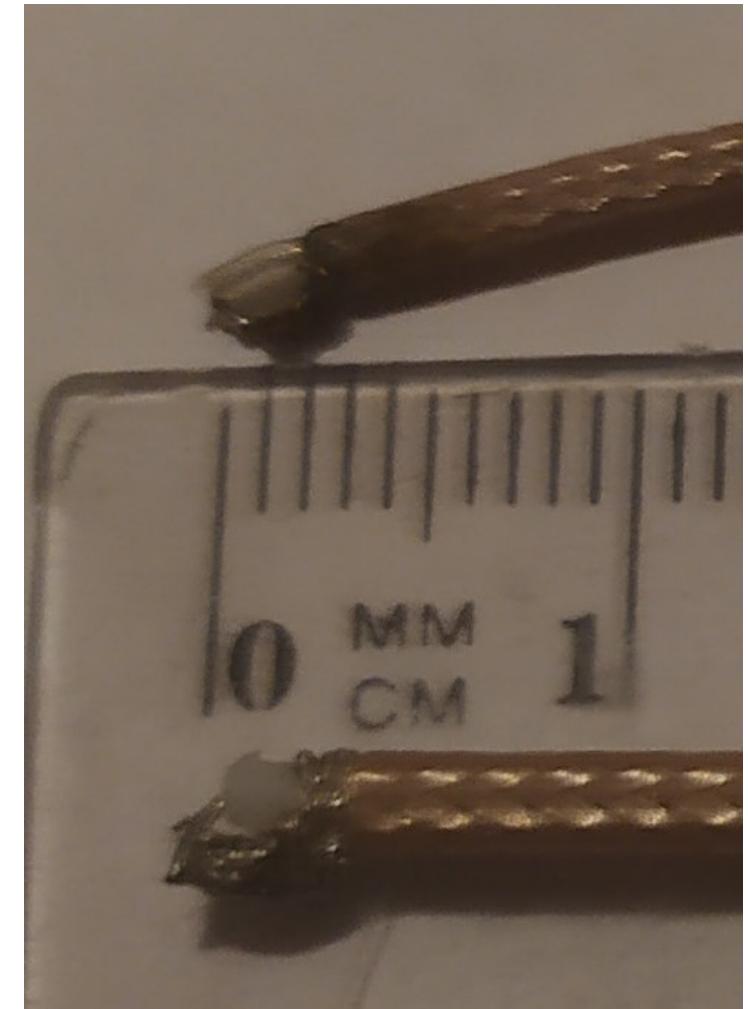
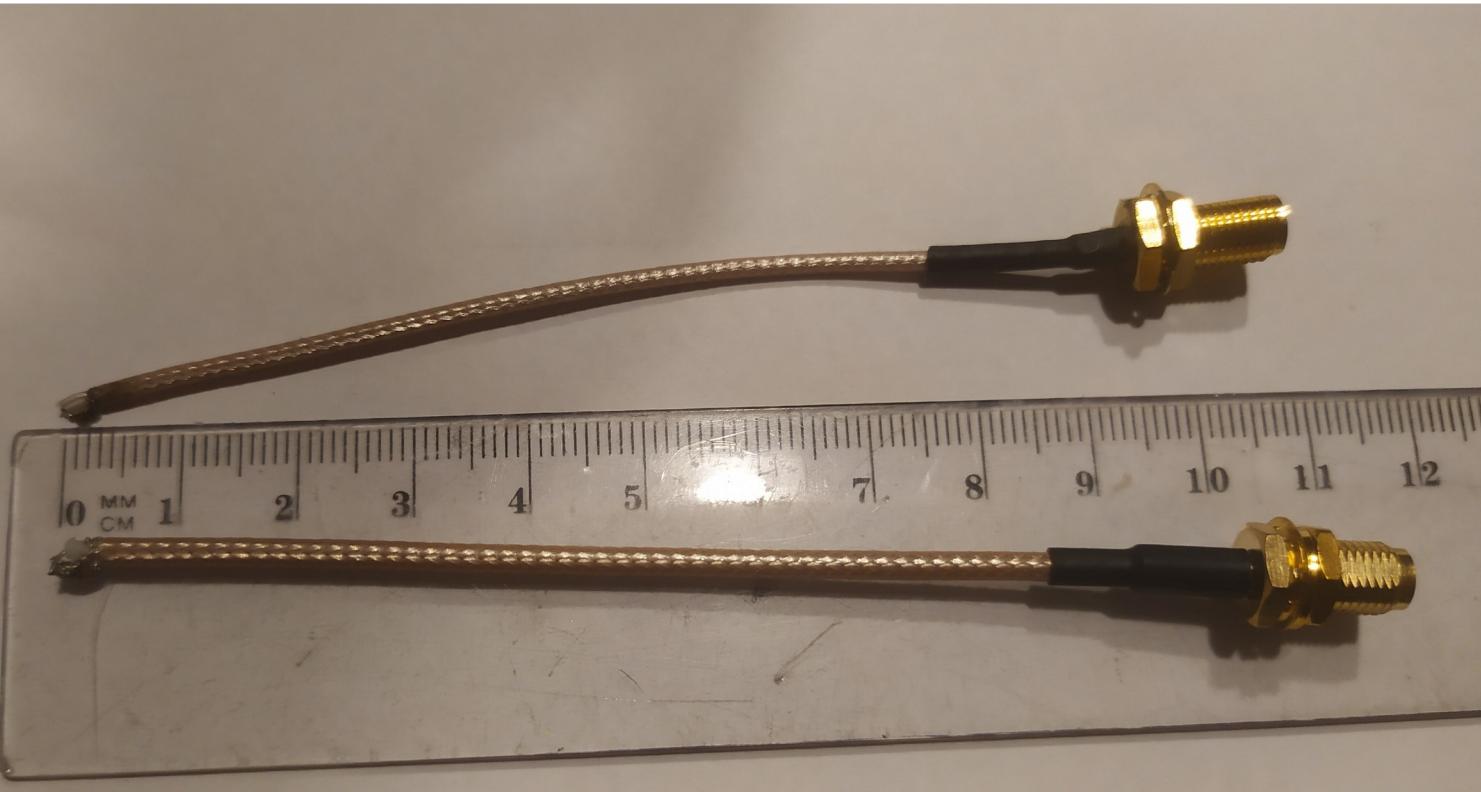
DEMO!

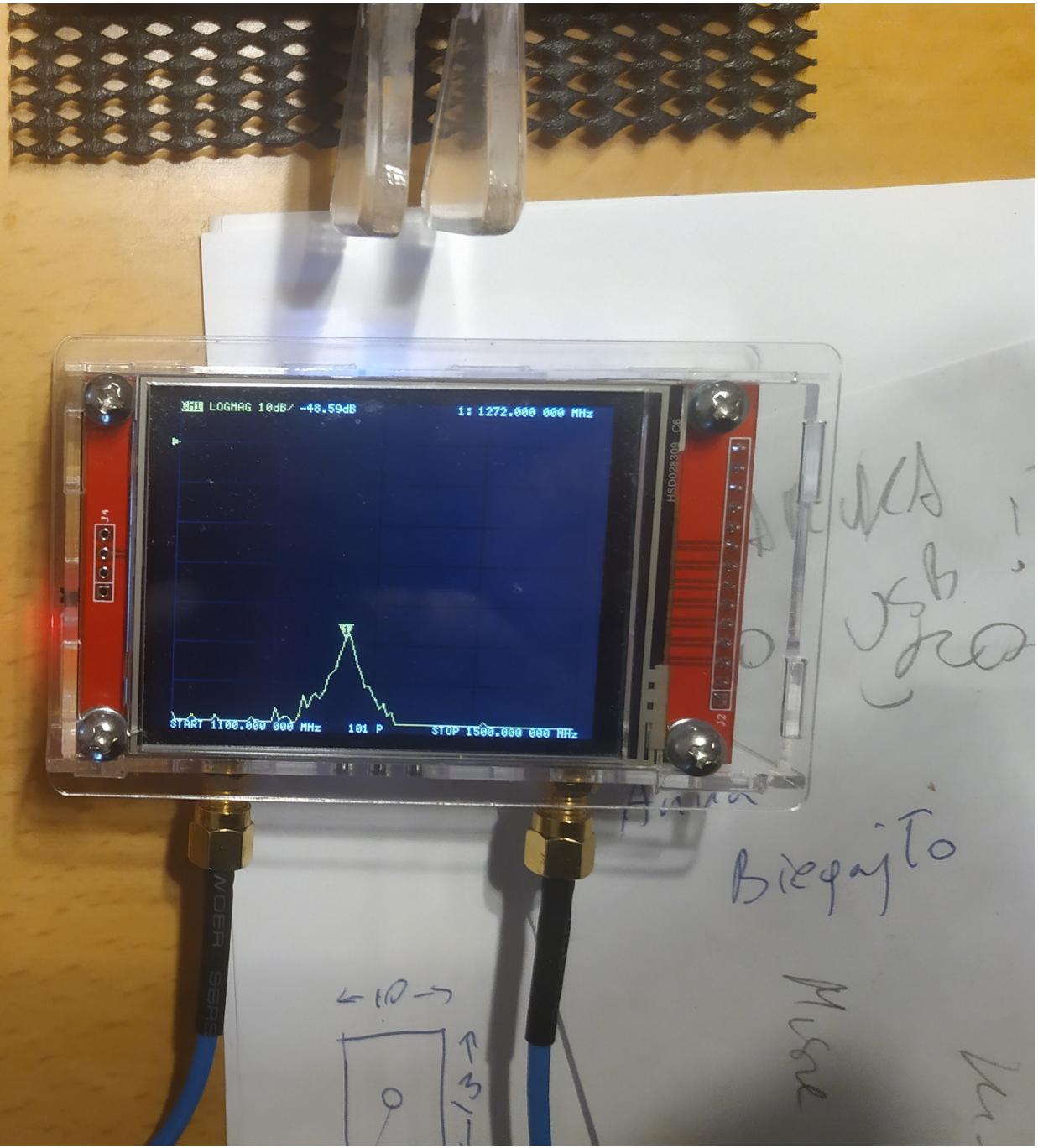
Czy to dziala? :)

Uwagi do uruchamiania

- Bardzo ważna duża dobroć rezonatora. Nie działa ze stalową śrubą, z mosiężną śrubą działa na biurku, po kiepskim posrebrzeniu na 10m.
- Antena powinna mieć $N * 1/2$ fali (N – liczba całkowita). Ja użyłem 22.5cm.
- Strojenie jest bardzo ciężkie! DEMO wymagało wielu prób.
- Ustawiamy na zadanej częstotliwości generator i odbiornik (w modułacji AM). Dmuchając w podsłuch ostrożnie przestrajamy go, aż usłyszymy „dmuchanie” w odbiorniku. Potem próbujemy, czy nie będzie lepiej słyszać na 1, 2 lub 3MHz niżej/wyżej.

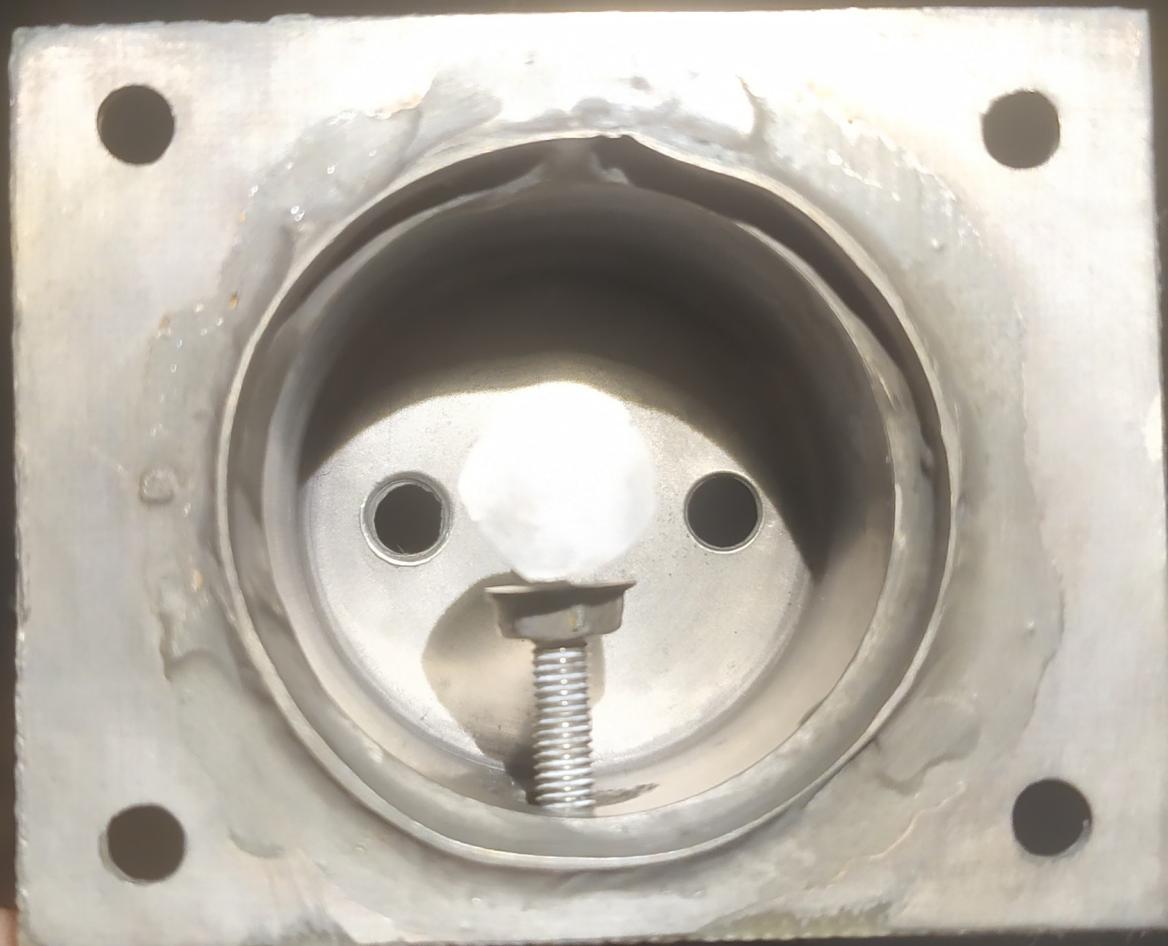
Strojenie





Srebrzenie (Stefan Sękowski „Galwanotechnika domowa”)





Zalety:

- „The Thing” było całkowicie pasywnym urządzeniem bez półprzewodników.
- Bez przewodów
- Niewykrywalne technologią z lat ‘50
- Niewykrywalne technologią z lat ‘70 - półprzewodniki można wykryć detektorem złącz nieliniowych (NLJD – Non-linear junction detector).
- Nie wymaga zasilania, więc może działać przez długi czas.

Wady:

- Podsłuch trzeba „oświetlić” stosunkowo silnym sygnałem
„Our problem was to keep from **sterilizing people** with the signal at the LP end.” :)
- Mikrofon mógłby być czulszy

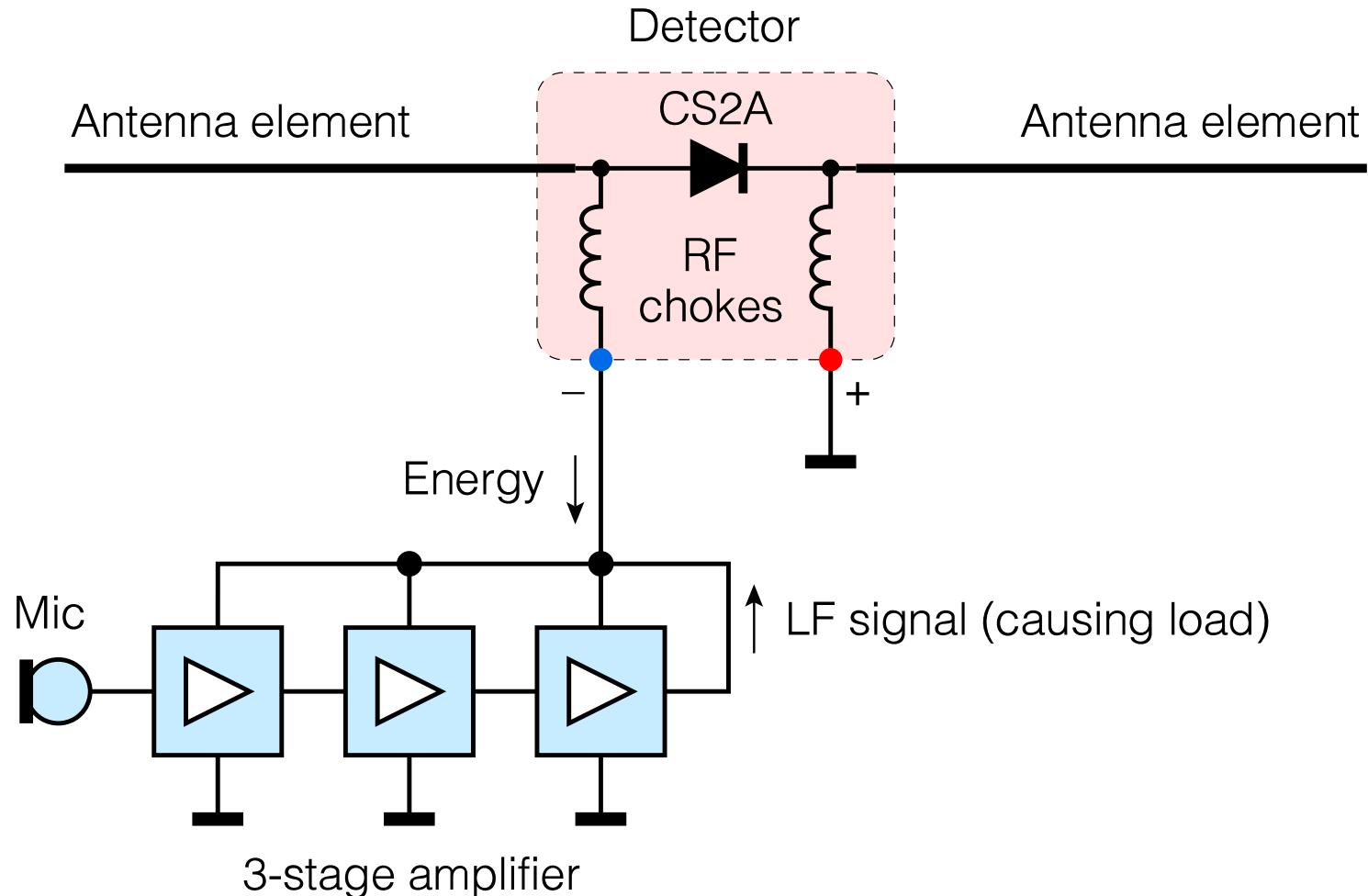
I dalsza historia...

:)

Kopie

- Anglicy zrobili kopię i nazwali to SATYR (wedle książki „Łowca Szpiegów” Petera Wrighta)
- USA uruchomili cały program pod kryptonimem EASY CHAIR
<https://www.cryptomuseum.com/convert/bugs/ec/index.htm>

EASY CHAIR mk1 (rok ~1955)



<https://www.cryptomuseum.com/cover/bugs/ec/ec1/index.htm>

Czy EASY CHAIR coś nam przypomina? :)

NSA ANT Catalog

https://en.wikipedia.org/wiki/ANT_catalog

I szukamy słowa „retroreflector” :)



LOUDAUTO

ANT Product Data

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components are COTS and so are non-attributable to NSA.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability (Rohde & Schwarz FSH-series portable spectrum analyzers, etc.) LOUDAUTO is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

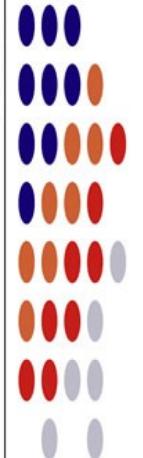
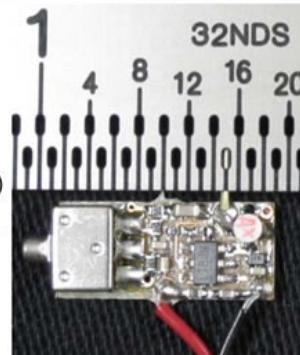
Unit Cost: \$30

Status: End processing still in development

POC: [REDACTED], S32243, [REDACTED], [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

07 Apr 2009



TAWDRYYARD

ANT Product Data

(TS//SI//REL TO USA,FVEY) Beacon RF retro-reflector. Provides return when illuminated with radar to provide rough positional location.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) TAWDRYYARD is used as a beacon, typically to assist in locating and identifying deployed RAGEMASTER units. Current design allows it to be detected and located quite easily within a 50' radius of the radar system being used to illuminate it. TAWDRYYARD draws as 8 uA at 2.5V (20uW) allowing a standard lithium coin cell to power it for months or years. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities being considered are return of GPS coordinates and a unique target identifier and automatic processing to scan a target area for presence of TAWDRYYARDs. All components are COTS and so are non-attributable to NSA.

(U) Concept of Operation

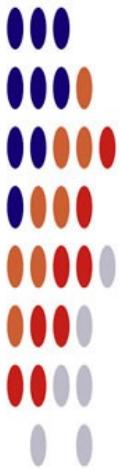
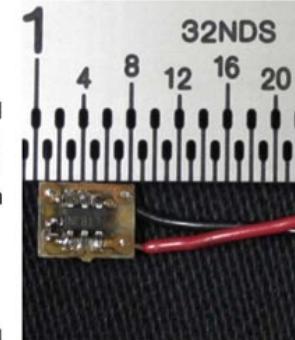
(TS//SI//REL TO USA,FVEY) The board generates a square wave operating at a preset frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal, the illuminating signal is amplitude-modulated (AM) with the square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the clock signal. Typically, the fundamental is used to indicate the unit's presence, and is simply displayed on a low frequency spectrum analyzer. TAWDRYYARD is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Unit Cost: \$30

Status: End processing still in development

POC: [REDACTED], S32243, [REDACTED], [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108





Coś do „oświetlania” celu też jest :)

Moc do 2W

Moc z zewnętrznym wzmacniaczem do 1kW :)

„Our problem was to keep from sterilizing people with the signal at the LP end.” :)

CTX4000
ANT Product Data

8 Jul 2008

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.



(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob
- User-selectable high- and low-pass filters.
- Remote controllable
- Outputs:
 - Transmit antenna
 - I & Q video outputs
 - DC bias for an external pre-amp on the Receive input connector
- Inputs:
 - External oscillator
 - Receive antenna

Unit Cost: N/A

Status: unit is operational. However, it is reaching the end of its service life. It is scheduled to be replaced by PHOTOANGLO starting in September 2008.

POC: [REDACTED], S32243, [REDACTED], [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

„The NSA Playset: RF Retroreflectors”

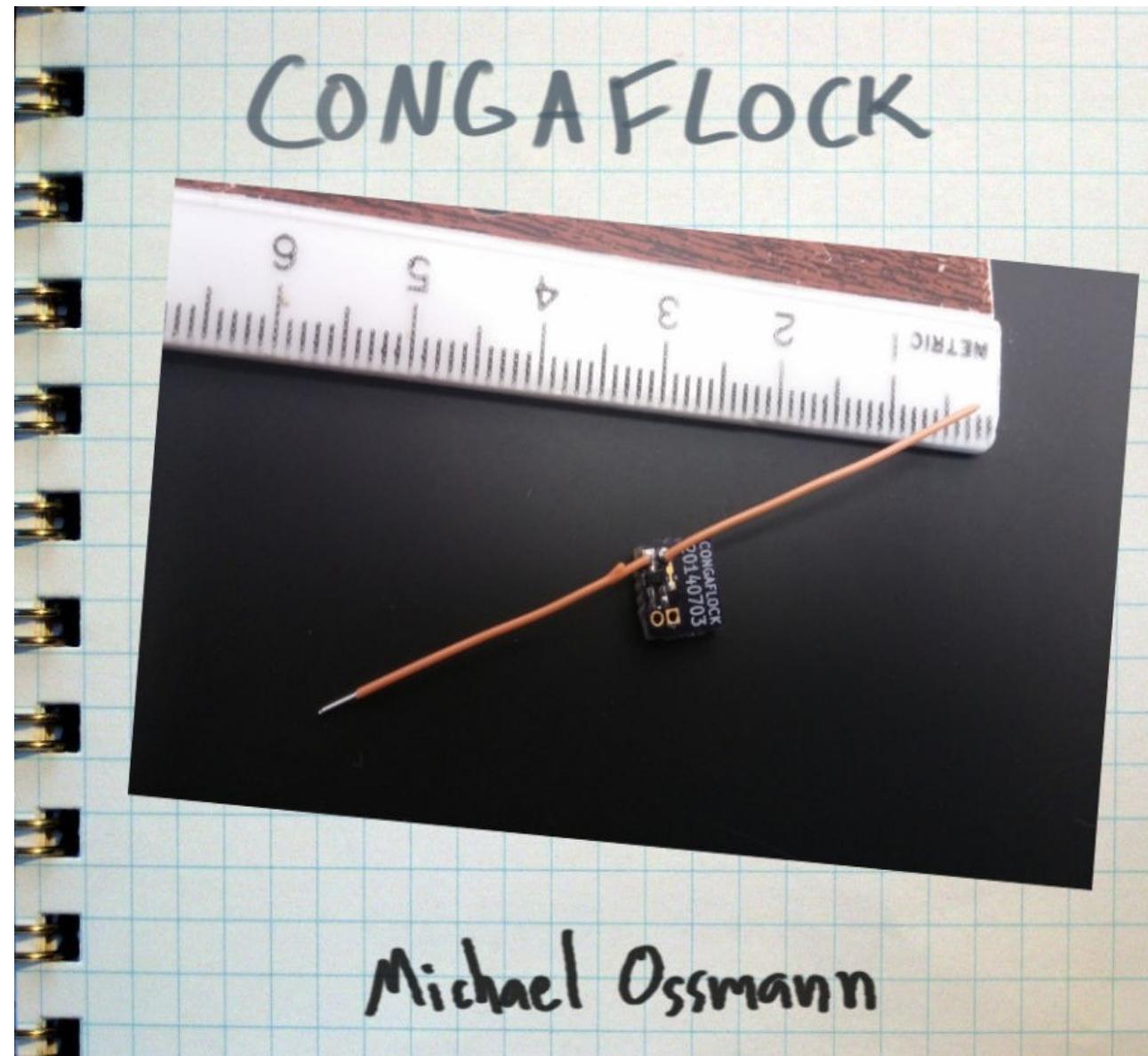
Mike Ossman, DEFCON 22

<https://defcon.org/html/defcon-22/dc-22-speakers.html#Ossmann>

Eksfiltracja sygnałów cyfrowych np z klawiatury.

<http://www.nsaplayset.org/congaflock>

<https://github.com/mossmann/retroreflectors>



RFID

- Cywilna technologia
- Urządzenie bierze zasilanie z nadajnika który je „oświetla”

Tak naprawdę to reimplementacja EASY CHAIR :)

Czy ten podsłuch jest w ogóle potrzebny?

Technika mikrofalowa nie jest obecnie takim problemem.

Krótkofalowcy używają powszechnie pasm < 50 GHz (wyższych też, ale to jest mniej popularne).

Wiele rzeczy w naszym otoczeniu może działać tak jak Great Seal Bug: wypromieniowywać/odbijać/rozpraszać fale radiowe i mieć na tyle dużą powierzchnię aby stanowić dobry mikrofon.

PYTANIA?

BARDZO PROSZĘ

O POZYTYWNĄ OCENĘ PREZENTACJI POD NAGRANIEM :)

VY 73

Jacek Lipkowski SQ5BPF

SQ5BPF@lipkowski.org

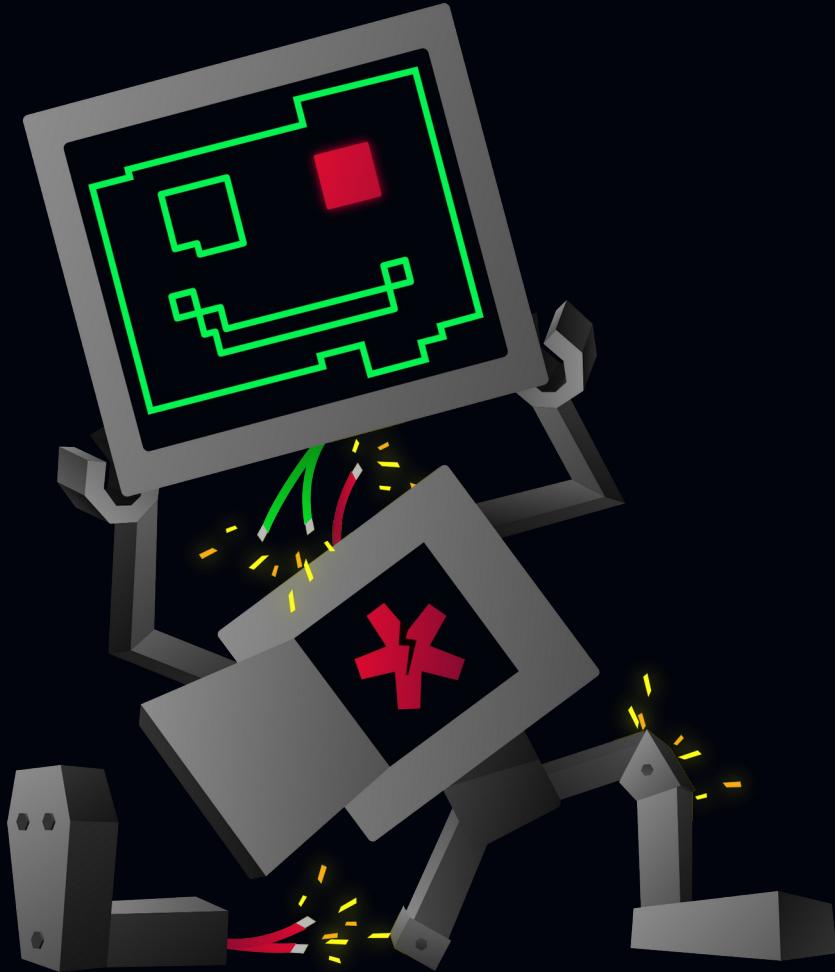
Link do prezentacji:

<https://github.com/sq5bpf/misc/blob/master/ths2023.pdf>



Dziękujemy za uwagę!

Zapraszamy do **zadawania pytań**
oraz **oceny wystąpienia**
pod nagraniem.



thehacksummit.com



19-20 października 2023



PGE Narodowy
+ Online

ORGANIZATORZY:

ACADEMIC
PARTNERS

