O entitate necunoscută, posibil extraterestră, a împînzit campusul facultății noastre cu balize ale căror scopuri eludează momentan toate investigațiile efectuate.

Reverse Engineering-ul realizat pînă acum de NSA [1] arată că aceste balize folosesc Bluetooth Classic și au nume de forma **PHNT*n***, unde *n* este o cifră. Ele comunică după protocolul următor:

Clientul transmite ce este scris la promptul C>
Serverul (baliza) răspunde ce este scris la promptul S>

C> AT+UNNNN	U=user; unde NNNN este numărul echipei (3 sau 4 cifre).
S> 210 Authorize XXX	număr de 3 cifre, generat aparent aleator pe server
C> YYYYCCCCC	numărul YYYY se calculează ca NNNN+XXX+PPP la care se apendează CRC16(YYYY), formînd CCCCC în **zecimal**
S> 211 Confirmation code is:	dacă ați introdus corect, primiți acest răspuns
S> RRRRRRR	rezultatul RRRRRRR are o semnificație misterioasă

Clientul calculează YYYY ca sumă a numerelor NNNN (numărul echipei PIA, unic pe facultate), XXX (numărul aleator primit de la server) și PPP (parola secretă). Se calculează și se apendează CRC-16 al șirului YYYY (sub formă **ASCII**) . Rezultatul se ia în **zecimal** (nu hex): valoarea CCCCC [2]

***Exemplu**: echipa 123, nr. aleator generat de server 887, parola secretă 1111: suma =2121, CRC16(șirul ASCII 2121)=30353;*

C> AT+U123
S> 210 Authorize 887
C> 212130353
S> 211 Confirmation code is:
S> RRRRRRRR

Pentru a putea descifra semnificația rezultatului RRRRRR, analiștii NSA au nevoie de cît mai multe astfel de numere. Fiecare echipă de la PIA poate introduce în formular rezultatele de la pînă la 7 balize diferite. Trebuie să căutați în teren balizele, folosind eventual telefonul mobil cu un soft de scanare, de exemplu *Bluetooth 4.0 Scanner*, pt a urmări numele balizelor

și nivelul semnalului – alegeți Bluetooth Classic, urmăriți indicația în dBm pentru a vă apropia cît mai mult de baliză. Balizele pot fi atît în interiorul clădirilor facultății ETTI (nu căutați la Jurnalism!) cît și în curte.

S-a observat că după un timp de cîteva secunde, baliza deconectează clientul, prin urmare nu este posibilă folosirea unui terminal gen *Serial Bluetooth Terminal* pentru a introduce manual datele și CRC-ul. Trebuie să faceți un program pe propria placă ESP32 care să interacționeze cu balizele. Numele balizei trebuie obținut anterior prin scanare, pentru a fi introdus în programul vostru, pentru ca placa ESP32 să se conecteze la acea baliză-server în modul client (vezi exemplele din documentație).

Atenție! dacă la o baliză încearcă să se conecteze simultan mai mulți clienți, ei se pot "bruia" unul pe celălalt și răspunsurile primite pot să fie confuze sau să se deconecteze prematur. Nu vă conectați pînă cînd alt client din apropiere nu s-a deconectat.

Happy Hunting !

P.S. Parola secretă o știu doar electroniștii. Este numărul de 3 cifre al celui mai popular circuit integrat folosit ca generator de semnal dreptunghiular, astabil, monostabil etc. Umblă zvonul că se folosește la lucrarea a 7 dintr-un laborator comun de anul 1.

[1] NSA = *No Such Agency*

[2] CRC-16/X-MODEM: https://crccalc.com/