

TETRA & VIRVE KUUNTELU

Koska tästä asiasta vääntäminen eri yhteyksissä alkaa ns. jurppimaan, ajattelin julkaista nyt kattavan tietopaketin ja ohjeet linkkien muodossa siitä, että [Tetra](#)-verkkoa eli Suomessa siis mm. [Virveä](#) voidaan kuunnella, eli vastaanottaa sen raakadataa. Toisin kun usein luullaan, itse Tetra / Virve signaalin kuuntelu sinällään on melko helppoa ja vaatii vain muutaman sadan euron skannerin, jonka asetukset on oikealla tapaa säädetty kohdalleen skannaamaan oikeata taajuusalueita.

Suomessa oli vielä tovi sitten tilanne, että Tetra-verkossa kaikki data kulki salaamattomana, joten kuuntelusta hyötyikin jotakin. Nykyään Suomessa [on Virve-verkossa käytössä salaus](#), joka estää tuon kuunnellun raakadatan hyötykäytön melko tehokkaasti, koska nykyään ei ole julkisesti tiedossa keinoa murtaa tuota Tetra-verkossa käytettävää [TEA1, TEA2, TEA3 ja TEA4](#) salausalgoritmiä. Itse salausalgoritmit ovat oletettavasti surkeat ja murtuvat varmaan ajallaan ehkä hyvinkin helposti, mutta toistaiseksi julkista tietoa niistä tai niiden murtamisista ei ole. Oletettavaa on, että eri maiden tiedustelupalvelut (NSA, CIA, FAPSI) pystyvät kyseisen salauksen murtamaan melko leikiten, aivan kuten esimerkiksi GSM:n salauksenkin.

Salauksen voi toki kiertää esimerkiksi pääsemällä käsiksi Virven viestikeskusten sisäiseen tai väliseen salaamattomaan liikenteeseen, salakuuntelemalla Virve-laitteiden Bluetoothia käyttäviä hands-free laitteita tai salakuuntelemalla tilaa jossa Virve-laitteita käytetään. Tietysti on myös mahdollista, mikäli henkilö saa käsiinsä "Virve-kapulan", asentaa siihen erilaisia salakuuntelulaitteita ja lähettäviä, tai vaihtoehtoisesti kaivaa kyseisen kapulan salausavaimet sen sisältä jollakin keinolla...vaikka nämä kaksi tapaa eivät vaaranna muuta kuin kyseisen kapulan viestinnän, pääsee niilläkin toki käsiksi ainakin osaan Tetra-verkon viestinnästä.

Jo yksinkertainen logiikkakin sinällään osoittaa, että Tetra-verkon lähete on kuultavissa...jos sitä ei olisi mahdollista kuunnella, yksikään Tetra-verkon päätelaite (puhelin, terminaali, jne.) ei voisi kommunikoida Tetra-verkkoon yhtään mitään eikä vastaanottaa sieltä yhtään mitään. Eli toisinsanoen, jotta verkko voi ylipäätään toimia, se edellyttää, että sitä käyttävät laitteet pystyvät kuulemaan Tetra-verkon signaalin ja jopa itsekin lähettämään jotain tietoa sinne Tetra-verkkoon. Aika simppeleä loppujen lopuksi.

Ainoa poikkeus tästä voi olla, jos käytetään voimakkaasti ja satunnaisesti taajuushypittävää, salattua purskelähetystä, kuten vaikkapa Puolustusvoimien uusissa [digitaalisissa kenttäradioissa](#). Näissä [Tadiranin](#) valmistamissa radioissa viestintä lähetetään lyhyinä, pakattuina ja salattuina purskeina, samalla vaihtaan radion taajuutta hyvin nopeasti (satoja-tuhansia hyppäyksiä sekunnissa) hyvin suurella taajuusalueella. Koska kuuntelija ei tiedä millä millisekunnilla hänen pitäisi mitään kapeata taajuuskaistaa kuunnella - eikä hän voi satunnaisesta kohinasta oikein edes erottaa milloin on osunut oikealle kaistalle - hän ei voi periaatteessa kuunnella viestintää.

Tetra-järjestelmässä ei käytetä tämän tyyppistä taajuushypytyä eli ns. hajaspektritekniikkaa, vaikka siellä taajuuksia vaihdellaankin vähän väliä ja jaetaan kanavaa eri käyttäjien kesken jne. Tetrassa on taajuuskaista hyvin kapea, ennalta määrätty ja tiedossa, sekä kanavien jakaminen (4 käyttäjää per kanava) ennalta tunnettu. Ihan millä tahansa kotiradiolla ei Tetraa silti voida järkevästi kuunnella, mutta sopivalla skannerilla se onnistuu.

Viimeksi totean vielä kaikille, että itse raakadatan käsittely, jos sen kryptaamattomana saa, vaatii vielä mm. Tetran käyttämän [puhekoodekin](#) ja muuta "sälää" jos ei omaa laitteita joissa se siis jo entuudestaan on olemassa. Tästä raakadatatista voi sitten erotella eri puheryhmiä ja puheluita ja puhujia haluansa mukaan. Lisäksi Tetra-järjestelmässä on mahdollista käyttää myös päästä-päähän-salausta, joka salaa kaiken viestinnän kahden (tai useamman) tahon välillä luurista luuriin. Normaalisti liikenne on salattu vain luurin ja tukiaseman välillä. Tässä päästä-päähän-salauksessa voidaan käyttää mitä tahansa salausalgoritmiä ja ainakin IDEA salausalgoritmiä on suositeltu. Salausavaimen luo ja toimittaa verkko, joten periaatteessa - jos verkkoon ei voida luottaa - järjestelmä ei ole sen turvallisempi kuin ilman tätä ominaisuuttakaan.

Mitä hyötyä näistä tiedoista sitten on? Kuuntelemalla, tai edes havaitsemalla tämän lähetteen lähistöllään, voi esimerkiksi saada tietoonsa, että lähellä on poliisipartioita vaikkapa suorittamassa liikenteenvalvontaa. Tai häiritsemällä näitä lähetkeitä voi estää viranomaisia kommunikoimasta lähialueilla. Ylipäätään tämän kaiken tietäminen on varmasti palkitsevaa ja uteliaisuutta tyydyttävää. Toivottavasti myös näistä heikkouksista keskusteleminen avaa ovia paremmille ja ennen kaikkea turvallisemmille järjestelmille kuin mitä Tetra / Virve on. :)

LÄHTEITÄ, LAINAUKSIA JA OHJEITA LIITTYEN TETRA & VIRVE KUUNTELUUN JA MUUHUN(KIN), osa 1/2.

[Tetra-kuunteluun soveltuvaa laitteistoa esim. Willtek.com:ssa](#)

"This powerful tool can be used to record, display and analyze the complex course of communication between one or several TETRA mobile stations and a TETRA base station...The TETRA AirAnalyzer simultaneously monitors and analyzes the complete up and downlink of one TETRA carrier (free choice of carriers) including all time slots (eight at the same time). The AirAnalyzer receiver features a very high sensitivity. In addition, the TETRA AirAnalyzer can be used to carry out RF measurements. "

[Hightech Forum artikkeli Virven kuuntelusta](#)

"Uuden viranomaisverkon Virven kuunteluun tarvitaan vain innokas nörtti, tietokoneohjattu vastaanotin ja niin sanottu koodekki, toteaa Skanneri-lehden kouvolaalainen päätoimittaja Mika Niemelä...Kohtuullisen helppoa kuuntelu on hänen mukaansa vain toistaiseksi, kunnes viranomaisverkko salataan tänä vuonna. Sen jälkeen kuuntelu menee vaikeaksi ja kalliiksi, mutta ei mahdottomaksi...Hän kertoo, ettei pankkiryöstäjän tulevaisuudessa tarvitse kuunnella viranomaisia vaan estää heidän kommunikaationsa eli häiritä Virve-verkon toimintaa. "Jokainen vähänkin elektroniikkaa tunteva harrastaja pystyy kasaamaan laitteen, joka estää Virven normaali toiminnan", Niemelä moittii. Niemelän mukaan niin sanottu hyppivätaajuus- tai hajaspektrilähete olisi ollut vaikeammin kuunneltavissa tai häiritävissä. Hän kertoo vielä tarkistaneensa tiedustelu- ja turvallisuuslähteistään, että Virven kuuntelun mahdollistama laite on helppo asentaa vastaanottimeen...Virven erikoissuunnittelija Peteveikko Lyly sanoo, että pelkkä digitaalisuus on huolehtinut siitä, että Virveä on vaikea kuunnella. "Sellaista laitetta ei ole, joka pystyy edes Tetra-standardin mukaista salaamatonta digitaalista vaihdemoduloitua signaalia muuttamaan puheeksi", Lyly toteaa."

[Skannerilehden keskustelupalstalla nm. Brunon ohjeet](#)

Kaikki on vuosien saatossa näillä lauteilla jo moneen kertaan sanottu, mutta kun edelleen kysellään että millä taajuuksilla, modeilla, jne. niin laitetaan ne tiedot nyt tänne tiiviissä muodossa. Keskustelu asiasta voisi jatkua tuolla "Voiko VIRVE kuunnella ja miten"-palstalla, niin ei mene lapsi pesuveiden mukana eikä huku hyötysignaali kohinaan.

- 1) VIRVE:n kuuntelussa idea on kuunnella päätelaitteen lähetettä. Siinä ei ole ideana kuunnella tukiaseman lähetettä. Siksi kuunneltavat taajuudet ovat tukiaseman vastaanottoaajuudet (Tukiasema RX).
- 2) VIRVE:lle on Suomessa annettu seuraava taajuusalue tukiaseman vastaanottosuunnassa (so. Uplink): 380,0125 - 384,9875 MHz (4,975 Mhz). Kanavaväli ja lähetteen leveys ovat molemmat 25kHz. VIRVE:n suorakanavalähteet (Direct Mode Operation, DMO) ovat alueilla 380,0125 - 380,1375 MHz ja 390,0125 - 390,1375 MHz. Näilläkin luonnollisesti 25kHz kanavaväli. Lisäksi taajuushallintoviranomaisemme Ficora on allokoinut seuraavan suorakanavalaajennuskaistan DMO-liikenteelle: 395,0125 - 395,9875 / 385,0125 - 385,9875 MHz (0.975MHz). Edelleen 25kHz kanavavälillä ("steppi") Jos haluaa pelata varman päälle, pitäisi nuo yo. taajuudet olla tavalla tai toisella (selaus, muistipaikkaskannaus) kuuntelussa.
- 3) Suorakanavaliikenteessä olisi hyvä kuunnella molempia suuntia, joka taas useimmiten puhuu sen puolesta, että kanavat pitää ohjelmoida muistipaikkoihin. Jos skanneri tukee etsintäpankkien linkitystä, niin sitten selauskin onnistuu. Esimerkki: suorakanavaliikenteen perustaajuudet: 380.0125, 380.0375, 380.0625, 380.0875, 380.1125, 380.1375 Mhz / 390.0125, 390.0375, 390.0625, 390.0875, 380.1125, 390.1375 MHz
- 4) yo. kuuntelussa kuunnellaan vain sitä "fyysistä" signaalia, minkä päätelaite (kapula, autoradio) lähettää. Sieltä kuuluu uplink-suunnassa heikkoa "tikitystä" tai "napsutusta" tai sen sellaista. Sieltä ei kuulu jatkuvaa pörinää. Eriaiset jatkuvat pörinät ja rätinät ovat häiriöitä.
- 5) Kuten edellä jo kerrottiin, on VIRVE-lähetteen leveys aika tarkkaan 25kHz. Lähetteen energia siis täyttää kanavan aika lailla laidasta laitaan. Kuuntelussa olisi hyvä saada mahdollisimman paljon lähetteen energiasta ilmaisimelle, että herkkyyks on hyvä. Skannerin vastaanottomodeilla (AM, NFM, WFM) on erilevyiset päästökaistat. Ne selviävät skannerin teknisistä tiedoista. Mode kannattaa valita joko niiden tietojen perusteella tai sitten kokeilemalla; mikä on sopivin sellaiselle signaalille, jonka leveys on 25kHz. WFM on harkinnan arvoinen.
- 6) VIRVE:n signaali on joka tapauksessa heikko, kiitos sen että se on aikajakoinen ja skannerin filterit eivät useimmiten ole viritetty VIRVE:n "aaltomuodolle". Siksi ulkoantennin käyttö ajoneuvossa on erityisen suotavaa, silläkin uhalla, että varsinkin kaupunkiliikenteessä häiriöitäkin tulee ihan kiitettävästi. Kuten edellä totesin, häiriö on kuitenkin helppo erottaa oikeasta lähteestä. Se keskeisin ongelma on lähinnä skannauksen pysähtyminen häiriöön, jonka aikana possanderi pääsee perälautaan kiinni ja kiinnijäämisen riski kasvaa eksponentiaalisesti.
- 7) Kun sitten käry käy, ei ole häpeä laskea alleen. Saa ainakin hyvät odoorit sinne virka-auton takapenkille kun sinne kuitenkin kutsuvat istumaan. Haju tarttuu uudenkarhean sivarin plynssihin ja pysyy siellä sillain aika tanakasti. Varakalsarit on hyvä olla hanskalokerossa.

LÄHTEITÄ, LAINAUKSIA JA OHJEITA LIITTYEN TETRA & VIRVE KUUNTELUUN JA MUUHUN(KIN), osa 2/2.

Skannerilehden keskustelupalstalla nm. Mikan ohjeet

Hommaan soveltuvat Skanneri-vastaanottimet (aakkosjärjestyksessä) AOR 3000/5000/8000/8200/Mk2/Mk3/8600 ja AOR One. Icom IC-R20. Uniden UBC-3000/9000 ja uudemmat mallit, jotka kattavat 380-400MHz taajuusalueen. Yupiteru MVT-7100/7200/7300/9000/mk2 ja modis-mallit M2.x ja M3.x (mvt-700 on hiukan hidas).

Sci.crypt uutisryhmästä poimittua Tetran salausalgoritmeista

DAGwyn@null.net

>"With no information to go on, there is no reason to
>consider them secure, nor to be certain that they are
>insecure. Going purely by historical statistics, one
>would a priori assume a system is vulnerable, and the
>burden of proof to the contrary would rest with its
>promoters. "

ggr@qualcomm.com

>"Based on its age and provenance, I would expect
>that the TETRA algorithms are multiple-LFSR
>nonlinear filter algorithms. They were designed
>well before the current algebraic attacks
>(Courtois, Armknecht(?sp), Pieprzyk, etc.) and I
>think they have a high chance of being
>academically broken by this kind of attack."

Tallentimia viranomaisten ja verkonhaltijoiden hoitamaan Tetra-verkon liikenteen tallentamiseen on saatavilla esimerkiksi Testme.fi:stä

Toimitusohjelmaamme kuuluu puheentallentimia, joilla voidaan tallentaa TETRA-verkkojen puhelut. Nokian (tai Motorolan) verkoista voidaan tallentaa keskitettyä tallennusta käyttäen:

- . kaikki puheryhmät
- . kaikki yksittäiset puhelut
- . kaikki lankaverkkoon menevät puhelut

Puheluja voidaan hakea radion ID-numerolla, puheryhmän ID-numerolla, käyttäjän nimellä ja kello- ja kalenteritiedon perusteella. Vaikka tallennustiedon keruu tehdään keskitetysti, voivat eri organisaation tallentaa omat puhelunsa omiin paikallisiin tiedostoihinsa. Keskitetty tallennus Nokian verkosta vaatii TCS- ja ESF-liitännät, jotka ovat saatavilla Rel 4.1 alkaen.

Tetra saattaa olla takaportitettu NSA:ta varten, varoittaa EU (Cryptome.org artikkeli).

An internal document from the European Union warns of a "major risk that could result from the omnipresence of US companies that supply radio communication equipment to the European police forces". This document originated from the STOA (Scientific and Technological Options Assessment) answerable to the European Parliament voiced its "serious concerns" over the domination of the US industry in the European telecommunication networks and in particular those dedicated to the emergency services.

Several of the US companies have been explicitly named for their "infiltration strategy" in Europe. According to the note "Motorola played a crucial role in defining the Tetra European standard, with the collaboration from the National Security Agency, in order to guarantee for the US government the possibility that Tetra networks could be eavesdropped

Erinomainen kirja liittyen Tetran tietoturvaan

"Tetra-järjestelmän sotilaalliset käyttömahdollisuudet,
Maj Ilkka Korkiamäki, 2001
ISBN: 951-25-1217-3"