

BadBIOS: Raziskava izvedljivosti visokofrekvenčne akustične komunikacije med fizično izoliranimi računalniki

Nika Hočevar in Aleks Klopčavar

Abstract—V članku obravnavamo domnevno zlonamerno programsko opremo BadBIOS (virus z domnevno zmožnostjo obstojnosti v vdelani programski opremi, celo v fizično izoliranih omrežjih), ki naj bi bila zmožna obstati v vdelani programski opremi ter komunicirati med fizično izoliranimi računalniki. Ker navedbe varnostnega raziskovalca Dragosa Ruiua, ki je prvi javno poročal o domnemnem BadBIOS-u, niso bile neodvisno potrjene, izvajamo študijo izvedljivosti (angl. feasibility study) enega izmed opisanih mehanizmov, in sicer domnevne ultrazvočne komunikacije, ki jo preverjamo z visokofrekvenčnim akustičnim kanalom. Preverjamo, ali je tak komunikacijski kanal tehnično izvedljiv z uporabo običajne potrošniške računalniške opreme brez specializiranih oddajnikov in sprejemnikov.

V praktičnem delu smo implementirali komunikacijski sistem z binarno frekvenčno modulacijo BFSK pri frekvencah 18,5 in 19,5 kHz, tik pod mejo ultrazvočnega območja. Sistem smo preizkusili na šestih računalniških napravah z različnimi operacijskimi sistemi, pri čemer smo uporabljali njihove integrirane zvočnike in mikrofone. V testiranih pogojih smo dosegli prenos podatkov na razdaljah do 8 metrov, vendar se je uspešnost sprejema med napravami občutno razlikovala.

Rezultati kažejo, da je visokofrekvenčna akustična komunikacija med omrežno izoliranimi računalniki tehnično izvedljiva tudi brez specializirane zvočne opreme. Njena zanesljivost se je močno razlikovala med sprejemnimi napravami; vzroka (strojna oprema ali operacijski sistem) v naši postavitvi ni bilo mogoče ločiti.

Študija potrjuje izvedljivost enega izmed mehanizmov, pripisanih BadBIOS-u, vendar ne potrjuje obstoja same zlonamerne programske opreme, njene obstojnosti v vdelani programski opremi ali izvajanja akustične komunikacije neposredno iz okolja BIOS oziroma UEFI. Zaradi pomanjkanja preverljivih dokazov ostaja skepticizem glede obstoja BadBIOS-a upravičen.

I. UVOD

Zagotavljanje varnosti računalniških sistemov, ki hranijo občutljive podatke, pogosto zahteva njihovo popolno fizično ločitev od javnih omrežij, pristop, znan kot fizična oziroma omrežna izolacija "air gapping". Čeprav ta ukrep odpravlja najpogostejše vektorje napadov, ni popolnoma zanesljiv; obsežno področje raziskav je pokazalo, da je mogoče podatke iz fizično izoliranih sistemov prenesti preko nenamernih fizičnih pojavov, znanih kot stranski kanali.

Eden izmed bolj dramatičnih primerov domnevne kršitve fizične izolacije je BadBIOS, zlonamerna programska oprema, ki jo je varnostni raziskovalec Dragos Ruiiu javno opisal v seriji objav leta 2013, pri čemer naj bi se težave začele že okoli leta 2010. Ruiiu je opisal zlonamerno programsko opremo z izjemnimi zmogljivostmi: obstojnostjo kljub ponovni namestitvi vdelane programske opreme ter zmožnostjo komunikacije med fizično izoliranimi računalniki preko ultrazvočnih signalov. V tistem času tovrstna

obstojnost vdelane programske opreme kot tudi ultrazvočna komunikacija med izoliranimi sistemi nista bili dokumentirani, kar je varnostno skupnost privedlo do dvomov o veljavnosti njegovih trditev. Kljub temu te trditve nikoli niso bile dokončno ovržene.

Ta članek raziskuje, ali je osrednji domnevni mehanizem BadBIOS-a (ultrazvočna komunikacija med fizično izoliranimi računalniki) tehnično izvedljiv v pogojih, podobnih tistim, ki jih je opisal Ruiiu. Z replikacijo tega mehanizma na dostopni potrošniški strojni opremi želimo preveriti, ali je mogoče takšen način komunikacije izvesti brez specializirane opreme. Čeprav obstoja virusa ne moremo potrditi, rezultati o izvedljivosti mehanizma omogočajo oceno tehnične verjetnosti Ruiiuovih trditev.

V ta namen smo implementirali in testirali sistem za visokofrekvenčni akustični prenos podatkov na več potrošniških računalniških platformah. Med testiranimi napravami so bili tudi računalniki Apple MacBook, ki jih je Dragos Ruiiu v svojih poročilih večkrat omenjal v povezavi z domnevnim delovanjem BadBIOS-a.

Prispevek je zasnovan kot strokovna demonstracija: ne predstavljamo nove metode, temveč preverjamo, kako se preprosto in javno dostopen akustični kanal obnese na sodobnih potrošniških napravah z vgrajenimi zvočniki in mikrofoni ter kakšne razlike med napravami se pri tem pokažejo.

Ruiiu je domnevni kanal opisal kot ultrazvočen. Ker naš sistem uporablja frekvenci 18,5 in 19,5 kHz, ki ležita tik pod običajno mejo ultrazvočnega območja (približno 20 kHz), za naš kanal uporabljamo izraz visokofrekvenčna akustična komunikacija. Del literature (npr. MOSQUITO [19]) območje 18–24 kHz sicer imenuje ultrazvočno.

Preostanek članka je organiziran kot sledi: razdelek II pregleda sorodna dela, razdelek III opisuje metodologijo, razdelek IV predstavlja eksperiment in rezultate, razdelek V razpravo, razdelek VI pa zaključuje.

II. SORODNA DELA

A. Stranski kanali

Računalniški sistemi nenamerno oddajajo informacije preko fizičnih pojavov, ki niso namenjeni komunikaciji, kar imenujemo stranski kanali. Prve raziskave segajo v tajni program NSA TEMPEST [1], ki je preučeval elektromagnetno sevanje elektronske opreme. Leta 1985 je Van Eck javno dokazal, da je mogoče vsebino zaslona CRT monitorja rekonstruirati na daljavo s poceni, doma izdelano anteno, s prestrežanjem elektromagnetnega sevanja monitorja, podobno kot bi nastavil televizijski signal [2]. To je pokazalo, da

tovrstni napadi ne zahtevajo opreme vladne ravni, temveč le ustrezno znanje.

Kocher je leta 1996 dokazal, da je mogoče kriptografske ključke izločiti iz razlik v času izvajanja operacij, kot sta RSA in Diffie-Hellman [3], leta 1999 pa je s sodelavci podobno tehniko uporabil na porabi energije pametnih kartic [4].

Njegovo delo je neposredno preoblikovalo industrijo, saj je spodbudilo uporabo algoritmov s konstantnim časom izvajanja in spremenilo zasnovo varnih čipov.

V nasprotju s stranskimi kanali, ki se izvajajo pasivno, obstaja ožja, namerna kategorija: prikriti kanali, prvič opredeljeni leta 1973 pri Lampsonu kot komunikacijska pot, ki ni bila namenjena prenosu podatkov, a jo napadalec namerno izkoristi z moduliranjem skupnega vira [5]. Takšen mehanizem ustreza domnevni načinu ultrazvočne komunikacije, pripisanemu BadBIOS-u: aktivno generiranje ultrazvočnih signalov za komunikacijo med fizično izoliranimi računalniki.

B. BadBIOS

BadBIOS je bil prvič širše dokumentiran v članku revije Ars Technica "Meet BadBIOS" [6] avtorja Dana Goodina, ki je povzemal originalne objave varnostnega raziskovalca Dragosa Ruiua. Trdil je, da je naletel na prej nedokumentirano zlonamerno programsko opremo z izrednimi zmogljivostmi. Pri analizi svojega sistema je ugotovil, da problem vztraja kljub vsem poskusom odstranitve, celo po popolni ponovni namestitvi vdelane programske opreme. Tri leta kasneje je ob nakupu novega računalnika ugotovil, da je bil ta takoj okužen, kar ga je privedlo do hipoteze, da se virus prenaša med računalniki preko ultrazvočne komunikacije. Ruiu je poročal, da se je domnevna komunikacija ustavila po odstranitvi oziroma onemogočenju zvočnih komponent.

Ars Technica je kasneje objavil še en članek "Researcher skepticism grows over BadBIOS malware claims" [7], ki je podrobno opisal pomisleke skupnosti. Raziskovalec Arrigo Triulzi je po pregledu Ruiuovih objav, izpisov BIOS-a, dnevnikov prometa, datotek pisav in posnetkov diskov, zaključil, da ni dokazov o prisotnosti virusa. Splošno mnenje varnostne skupnosti ostaja, da preprosto ni dovolj dokazov za obstoj BadBIOS-a. Kljub številnim neodvisnim analizam nikoli ni bil dosežen dokončen zaključek.

C. Prikriti komunikacijski kanali fizično izoliranih računalnikov

Čeprav BadBIOS ni bil nikoli dokončno potrjen, so raziskave pokazale, da je prikrita komunikacija med fizično izoliranimi računalniki tehnično izvedljiva. Guri et al. so tovrstne kanale razvrstili v pet kategorij: elektromagnetne, magnetne, optične, termične in akustične.

Elektromagnetni kanali. Leta 2014 so predstavili AirHopper [8], zlonamerno programsko opremo, ki prenaša podatke iz fizično izoliranih računalnikov do bližnjega pametnega telefona preko FM signalov, oddajanih preko ekranskega kabla. Leta 2015 so razvili GSMem [9], ki za prenos podatkov do mobilnih telefonov izkorišča celične

frekvence, generirane na vodilih med RAM-om in CPU-jem. Leta 2016 je sledil USBee [10], ki za generiranje elektromagnetnih signalov uporablja USB vodilo.

Termični kanali. Leta 2015 so predstavili BitWhisper [11], termični prikrit kanal, ki omogoča dvosmerno komunikacijo med dvema sosednjima fizično izoliranimi računalnikoma preko temperaturnih sprememb, ki jih generira CPU oziroma GPU.

Optični kanali. Leta 2017 so razvili LED-it-GO [12], prikrit kanal, ki za prenos podatkov iz fizično izoliranih računalnikov uporablja LED indikator trdega diska. Istega leta so predstavili tudi aIR-Jumper [13], zlonamerno programsko opremo, ki za komunikacijo z izoliranimi omrežji izkorišča IR LED-diode varnostnih kamer.

Magnetni kanali. Leta 2018 so predstavili ODINI [14], zlonamerno programsko opremo, ki prenaša podatke preko nizkofrekvenčnih magnetnih signalov, generiranih preko CPU jeder, ki prodrejo tudi skozi Faradayeve kletke in kovinske ščite. Istega leta so razvili še MAGNETO [15], ki za sprejem prikritih signalov izkorišča magnetni senzor v pametnih telefonih.

Akustični kanali. Akustični prikriti kanali za prenos podatkov uporabljajo neslišne ultrazvočne zvočne valove. Leta 2013 sta Hanspach in Goetz demonstrirala [16] prikrit kanal med fizično izoliranimi prenosnimi računalniki, opremljenimi z zvočniki in mikrofoni, pri čemer sta dosegla razdaljo 19 metrov s hitrostjo prenosa 20 bit/s. Večina akustičnih metod za delovanje potrebuje zvočne naprave; leta 2016 so Guri et al. predstavili Fansmitter [17], ki omogoča prenos podatkov preko zvoka ventilatorjev računalnika brez njihove uporabe. Predstavili so tudi Speake(a)r [18], ki prikrito pretvori slušalke ali ušesne čepke v prisluškovalne naprave z izkoriščanjem funkcije *jack retasking*, ki jo podpirajo zvočni čipi (npr. Realtek) in omogoča programsko spremembo funkcije zvočnega priključka iz izhodnega v vhodni.

Na tej osnovi so leta 2018 razvili MOSQUITO [19], metodo za prikrit prenos podatkov med dvema fizično izoliranimi računalnikoma brez uporabe mikrofонов, ki deluje v ultrazvočnem območju med 18 kHz in 24 kHz na razdalji do 9 metrov med zvočniki oziroma do 3 metre med slušalkami.

III. METODOLOGIJA

Cilj eksperimenta je bil preveriti, ali je mogoče z uporabo običajne potrošniške strojne opreme vzpostaviti visokofrekvenčni akustični komunikacijski kanal med dvema fizično izoliranimi računalnikoma. Kot izhodišče smo uporabili raziskavi Hanspacha in Goetza [16] ter MOSQUITO [19]; od MOSQUITO se razlikujemo v tem, da za sprejem uporabljamo integrirani mikrofón. Zanimalo nas je predvsem, ali je primerljivo komunikacijo mogoče vzpostaviti z uporabo integriranih zvočnikov in mikrofónov prenosnih računalnikov brez dodatne specializirane opreme.

Metodologija je razdeljena na dva dela. Najprej predstavimo teoretično zasnovano komunikacijskega sistema na osnovi digitalne obdelave signalov, nato pa opišemo eksperimentalno postavitev in izvedbo meritev.

A. Teoretična zasnova komunikacijskega sistema

Prenos podatkov temelji na binarni frekvenčni modulaciji (Binary Frequency Shift Keying – BFSK), pri kateri je vsak bit predstavljen z eno izmed dveh nosilnih frekvenc. Signal je opisan z enačbo

$$s(t) = \begin{cases} A \cos(2\pi f_0 t), & \text{če je oddan bit 0,} \\ A \cos(2\pi f_1 t), & \text{če je oddan bit 1,} \end{cases}$$

kjer je A amplituda signala, f_0 nosilna frekvenca za bit 0, f_1 nosilna frekvenca za bit 1, t pa čas.

V implementaciji smo uporabili frekvenci $f_0 = 18,50$ kHz in $f_1 = 19,50$ kHz, saj ležita blizu zgornje meje običajno navajanega območja človeškega sluha, hkrati pa ostajata v območju, ki so ga lahko zaznale izbrane testne naprave. Razmik 1 kHz je bil izbran z namenom, da se frekvenčni komponenti pri uporabljeni dolžini analiznega okna dovolj jasno ločita v izračunanem spektru.

Na sprejemni strani je bil signal vzorčen s frekvenco 44,1 kHz. Izbrana vzorčna frekvenca 44,1 kHz zadostuje Nyquistovemu pogoju, saj je več kot dvakrat višja od največje uporabljene nosilne frekvence (19,50 kHz).

Zajeti signal smo analizirali z uporabo hitre Fourierjeve transformacije (FFT) [20], ki predstavlja učinkovit algoritem za izračun diskretne Fourierjeve transformacije (DFT).

$$X(k) = \sum_{n=0}^{N-1} x(n)e^{-j2\pi kn/N},$$

kjer je $x(n)$ vzorčeni signal dolžine N , k indeks frekvenčne komponente, j imaginarna enota, $X(k)$ pa kompleksni frekvenčni spekter.

Primerjava amplitud spektra pri obeh nosilnih frekvencah v posameznem časovnem oknu določa, ali je bil sprejet bit 0 ali bit 1, zaporedje rekonstruiranih bitov pa predstavlja izvorno sporočilo.

B. Teoretična izvedba v okolju BIOS oziroma UEFI

Praktični del raziskave je bil izveden v uporabniškem prostoru operacijskega sistema, kjer dostop do zvočnih naprav omogočajo standardni gonilniki.

Ker je BadBIOS temeljil na domnevi, da se zlonamerna programska oprema izvaja neposredno iz BIOS oziroma UEFI okolja, smo analizirali tudi teoretično izvedljivost takšnega pristopa.

Kot prikazuje slika 1, operacijski sistem pri običajnem predvajanju zvoka skrbi za inicializacijo zvočnega krmilnika in komunikacijo z zvočnim kodekom [21]. V okolju BIOS oziroma UEFI teh storitev ni, zato bi moral zlonamerni program sam inicializirati krmilnik, pripraviti PCM vzorce ter jih poslati zvočni napravi.

Neposredno generiranje visokofrekvenčnih akustičnih signalov iz okolja BIOS oziroma UEFI bi zahtevalo implementacijo gonilnika za uporabljeni zvočni krmilnik ter neposredno upravljanje strojne opreme brez podpore operacijskega sistema. To pomeni inicializacijo zvočnega kodeka,

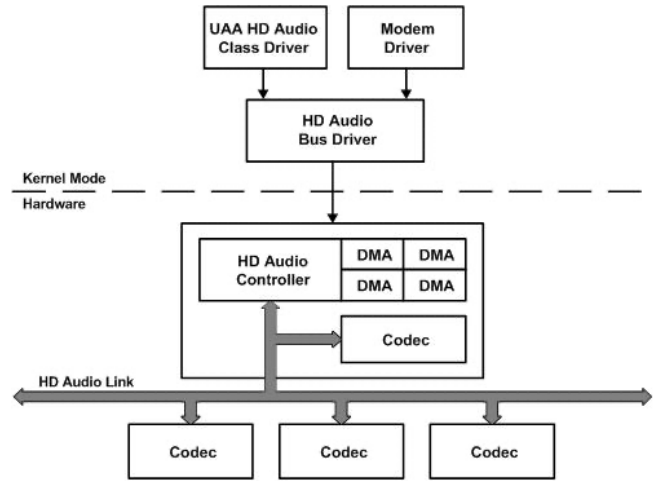


Fig. 1. Poenostavljena arhitektura Intel High Definition Audio. Implementacija v okolju BIOS oziroma UEFI bi morala neposredno inicializirati HD Audio krmilnik in kodek brez podpore gonilnikov operacijskega sistema [21].

pripravo PCM vzorcev in njihovo pošiljanje zvočni napravi preko ustreznega krmilnika.

Čeprav takšna implementacija presega obseg tega dela, z vidika arhitekture računalniških sistemov ni očitnih tehničnih razlogov, da je ne bi bilo mogoče izvesti. Glavna omejitev je kompleksnost implementacije in neposreden dostop do zvočne strojne opreme brez podpore operacijskega sistema.

C. Postavitev eksperimenta

Za eksperiment smo uporabili šest računalniških naprav z različnimi operacijskimi sistemi. Vse naprave so uporabljale integrirane mikrofone in zvočnike, s čimer smo želeli čim bolj približati pogoje prvotnim opisom BadBIOS-a. Fujitsu LIFEBOOK U7411 je bil uporabljen le kot oddajnik. Specifikacije uporabljenih naprav so prikazane v Tabeli I.

TABLE I
SPECIFIKACIJE TESTNIH NAPRAV

Naprava	Operacijski sistem	Verzija
Namizni računalnik	Windows 11	24H2
Lenovo prenosnik	Windows 11	24H2
HP ZBook	CachyOS	Linux Kernel 6
Fujitsu LIFEBOOK U7411	Ubuntu	26.04 LTS
MacBook Air	macOS	26 Tahoe
MacBook M4 Pro	macOS	26 Tahoe

Kombinacija teh naprav omogoča primerjavo delovanja akustičnega kanala med različnimi napravami, pri čemer vpliva operacijskega sistema in strojne opreme ni mogoče ločiti. Ker je Ruiu o domnevnem BadBIOS-u med drugim poročal v povezavi z računalniki MacOS, MacBook Air predstavlja zgodovinsko najbolj relevantno testno okolje.

Programska orodja, uporabljena pri implementaciji komunikacijskega sistema in izvedbi eksperimenta, so prikazana v Tabeli II.

TABLE II
PROGRAMSKA ORODJA, UPORABLJENA PRI EKSPERIMENTU

Programska oprema	Namen
Python	Implementacija oddajnika in sprejemnika
PyAudio	Zajem in predvajanje zvočnega signala
NumPy	Obdelava signalov in numerični izračuni
SciPy	Generiranje signalov in FFT analiza
Audacity	Snemanje in analiza zvočnih signalov
phyphox	Meritev dominantne frekvence signala

TABLE III
PARAMETRI KOMUNIKACIJSKEGA SISTEMA

Parameter	Vrednost
Modulacija	Binary FSK
Vzorčna frekvenca	44,1 kHz
Nosilni frekvenci	18,5 kHz in 19,5 kHz
Trajanje bita	100 ms
Hitrost prenosa	10 bit/s
Dolžina preambule	24 bitov
Preambula	11100101 00010110 10111000
Prag zaznave preambule	23 od 24 bitov ($\geq 95\%$)
Amplituda oddajnika	0,5 (−6 dBFS)
Okno FFT	4410 vzorcev (100 ms), Hann
Testno sporočilo	hello world (11 znakov)
Velikost sporočila	88 bitov
Velikost paketa	112 bitov
Čas prenosa paketa	11,2 s

D. Izvedba prenosa

Oddajnik in sprejemnik sta bila implementirana v programskem jeziku Python z uporabo knjižnic PyAudio in SciPy. Oddajnik je generiral sinusne signale pri vzorčni frekvenci 44,1 kHz, pri čemer sta bila bita 0 in 1 predstavljena s frekvencama 18,5 kHz oziroma 19,5 kHz. Vsak bit je bil oddan v časovnem intervalu 100 ms, kar predstavlja hitrost prenosa 10 bit/s. Ton vsakega bita z amplitudo 0,5 je bil pomnožen s Hannovim oknom, tako da amplituda na začetku in koncu bita zvezno pade na nič. Pred vsakim paketom je bilo oddanih 0,5 s tišine in 24-bitna preambula za sinhronizacijo sprejemnika (Tabela III).

Sprejemnik je z uporabo integriranega mikrofona zajemal signal pri enaki vzorčni frekvenci. Preambulo je iskal z drsnim oknom s korakom 275 vzorcev (približno 6 ms) in jo štel za zaznano, ko se je ujemalo vsaj 23 od 24 bitov. Nato je signal razdelil na zaporedna, neprekrivajoča se okna dolžine 4410 vzorcev (100 ms, eno okno na bit), vsako pomnožil s Hannovim oknom in izračunal FFT (frekvenčna ločljivost 10 Hz). Bit je bil določen s primerjavo amplitude spektra pri 18,5 in 19,5 kHz. Če je bila relativna razlika med njima manjša od 25 %, je sprejemnik bit določil po dominantni frekvenci v toleranci ± 300 Hz, sicer pa ga je nastavil na 0. Iz zaporedja bitov je bilo rekonstruirano izvirno sporočilo [22].

Sistemska glasnost predvajanja je bila nastavljena na 100 %, ojačanje mikrofona pa na 0 dB (brez dodatnega ojačanja). Sistemsko procesiranje zvoka v Windows (izboljšave zvoka, odstranjevanje šuma, samodejno ojačanje) je bilo izklopljeno.

Kot testno sporočilo smo uporabili niz *hello world*.

E. Pogoji testiranja in zaznavanje

Kot odvisne spremenljivke smo spremljali uspešnost dekodiranja, največji doseg komunikacije ter zaznavnost signala za človeškega poslušalca.

- **Razdalja med napravama:** Testi so bili načrtovani pri različnih razdaljah med 1 in 8 m.
- **Lokacija oziroma raven hrupa:** Test je potekal v običajni učilnici brez dodatne akustične izolacije.

Prisotne osebe so poročale, ali so med prenosom zaznale zvok. Ker ni bil izveden nadzorovan psihoakustični preizkus, teh opažanj ne obravnavamo kot dokaz popolne neslišnosti signala. Telefon z aplikacijo phyphox je bil uporabljen za vizualno potrditev, da signal dejansko oddajamo v predvidenem frekvenčnem območju 18–20 kHz. Vsi prenosi so bili posneti s programom Audacity za naknadno analizo.

Na podlagi rezultatov posameznih sprejemnih naprav smo ocenili, ali je v testiranem okolju mogoče vzpostaviti visokofrekvenčni akustični komunikacijski kanal med računalnikoma ter pri tem uporabljati frekvenčno območje, ki ga večina uporabnikov ne zazna.

Za vsako sprejemno napravo in razdaljo je bilo izvedenih deset poskusov. Kot oddajnika sta delovala MacBook Air in Fujitsu LIFEBOOK U7411 (Ubuntu), vse ostale naprave pa so bile sprejemniki. Meritve smo izvedli pri razdaljah od 1 do 8 m. Tabela IV prikazuje uspešnost glede na operacijski sistem sprejemne naprave; 10 poskusov na posamezno meritev predstavlja skupno število poskusov z obema oddajnikoma, zato rezultati v tabeli niso ločeni po oddajniku. Uspešnost komunikacije je izražena kot delež uspešno dekodiranih sporočil glede na skupno število poskusov.

Omejitve obsega: Obstojnost zlonamerne programske opreme v vdelani programski opremi (firmware persistence), ki je ena izmed ključnih trditev primera BadBIOS, je iz praktičnega testiranja izključena. Gre namreč za arhitekturno kompleksnost, ki presega okvir te demonstracije.

IV. EKSPERIMENT

Eksperiment je bil izveden z namenom preverjanja, ali je mogoče z običajno potrošniško strojno opremo vzpostaviti zanesljiv visokofrekvenčni akustični komunikacijski kanal med omrežno izoliranimi računalniki. Poseben poudarek je bil na preverjanju vpliva uporabljene strojne opreme, največje razdalje prenosa ter uspešnosti dekodiranja sporočil v običajni učilnici.

Za testiranje smo uporabili šest računalniških naprav z različnimi operacijskimi sistemi. Vse naprave so uporabljale izključno integrirane zvočnike in mikrofone brez dodatne zvočne opreme. Prenosi so potekali v običajni učilnici brez dodatne akustične izolacije. Prisotni so bili običajni okoljski zvoki, vendar njihova raven ni bila instrumentalno izmerjena (pogovor, ventilatorji računalnikov in gibanje oseb).

A. Preverjanje frekvenčnega odziva naprav

Pred začetkom komunikacijskih poskusov smo preverili, ali uporabljeni zvočniki omogočajo predvajanje frekvenc v območju 18–20 kHz oziroma ali je prisoten nizkoprepustni



Fig. 2. Eksperimentalna postavitev uporabljenih računalnikov med testiranjem akustične komunikacije.

filter, ki bi preprečeval oddajanje signalov nad približno 15 kHz.

V ta namen smo z uporabo programa Audacity ustvarili frekvenčni sweep od 1 kHz do 22 kHz in ga predvajali preko integriranih zvočnikov. Posneti signal smo analizirali s spektrogramom.

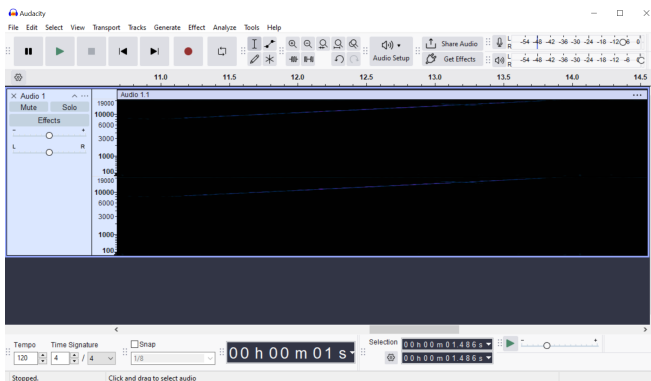


Fig. 3. Spektrogram frekvenčnega sweepa na napravi Windows.

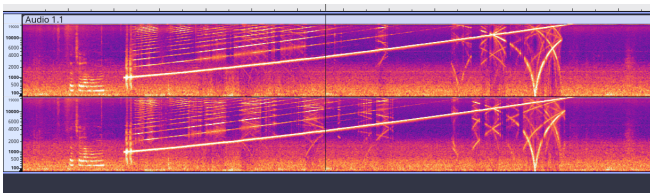


Fig. 4. Spektrogram frekvenčnega sweepa na napravi Linux.

Pri nobeni izmed testiranih naprav nismo opazili izrazitega slabljenja signala v območju med 18 in 20 kHz. Rezultati kažejo, da uporabljeni zvočniki niso vsebovali izrazitega nizkoprepustnega filtra, ki bi preprečeval oddajanje frekvenc v tem območju. Morebitni neuspešni prenosi zato verjetno niso posledica omejitve oddajne strojne opreme.

S tem smo izločili možnost, da bi bile razlike med napravami posledica nezmožnosti oddajanja frekvenc v območju 18–20 kHz. Nadaljnji eksperimenti so se zato osredotočili predvsem na lastnosti sprejemne strani.

B. Doseg komunikacije

Komunikacija je bila preizkušena na šestih računalniških napravah z različnimi operacijskimi sistemi. Pri obeh Windows napravah (namizni računalnik in prenosnik Lenovo) je bila uspešnost prenosa na razdaljah do 4 m približno 60 % (6 od 10 poskusov), nad 4 m pa je uspešnost strmo padla na približno 10 % (1 od 10 poskusov), kar bi lahko bila posledica slabšega odziva integriranih mikrofонов ali filtriranja v gonilniku zvočnega kodeka, ki ga v sistemskih nastavitvah ni mogoče izklopiti (glej razdelek Omejitve). Pri napravah MacBook je bila uspešnost pod 6 m 100 % (10 od 10 poskusov), nad 6 m pa približno 90 % (9 od 10 poskusov). Naprava HP ZBook (Linux) je v prvotni implementaciji sprejemnika dosegala 0 % uspešnosti, čeprav je bil signal uspešno oddan, kar smo pripisali nezdružljivosti uporabljenih zvočnih knjižnic z operacijskim sistemom. Po odpravi te težave je naprava dosegala uspešnost, primerljivo z računalniki MacBook, a nekoliko nižjo: približno 90 % pod 6 m in 80 % nad 6 m.

TABLE IV

USPEŠNOST SPREJEMA GLEDE NA OPERACIJSKI SISTEM SPREJEMNE NAPRAVE (10 POSKUSOV NA MERITEV, SKUPAJ ZA OBA ODDAJNIKA)

Razdalja	Windows	macOS	Linux
1–4 m	6/10	10/10	9/10
5–6 m	1/10	10/10	9/10
7–8 m	1/10	9/10	8/10

C. Uspešnost dekodiranja

Prvotna implementacija komunikacijskega sistema ni vsebovala mehanizma za sinhronizacijo med oddajnikom in sprejemnikom, zaradi česar je sprejemnik pogosto začel dekodiranje sredi prenosa. Posledica so bila nepravilno rekonstruirana sporočila.

Za odpravo te težave smo implementirali preambulo, sestavljeno iz fiksne 24-bitne zaporedja (Tabela III), ki sprejemniku omogoča zanesljivo zaznavanje začetka paketa. Šele po uspešni zaznavi preambule se začne dekodiranje dejanskega sporočila.

Testno sporočilo je vsebovalo 11 ASCII znakov oziroma 88 bitov brez preambule. Uspešnost dekodiranja smo ocenjevali glede na pravilno rekonstruirano celotno sporočilo.

Na sliki 5 je prikazan primer uspešnega sprejema testnega sporočila *hello world*.

Dodatek preambule je bistveno izboljšal stabilnost komunikacije in zmanjšal število napačno dekodiranih sporočil.

D. Primerjava različnih naprav

Eksperiment smo izvedli na šestih računalniških napravah z različnimi operacijskimi sistemi in različno zvočno strojno opremo. Cilj primerjave je bil oceniti, kateri dejavnik ima večji vpliv na uspešnost prenosa.

```

Waiting for preamble...
Preamble detected!
Receiving message...
Received: 'hell/ world'
Bits: 011010000110010101100001011110010000011101110111101110010011010001100100

Waiting for preamble...
Preamble detected!
Receiving message...
Received: 'hel(=Ey)Duç'
Bits: 01101000011001010110001111011010010011001011110010111011101100000111010111100111

Waiting for preamble...
Preamble detected!
Receiving message...
Received: 'hello world'
Bits: 0110100001100101011000110111001000001110111011110111011100100110110001100100

Waiting for preamble...
Preamble detected!
Receiving message...
Received: 'haddo wop,d'
Bits: 011010000110010101100100011001001111100100000111011101111011100000010110001100100

```

Fig. 5. Uspešno dekodiranje testnega sporočila po zaznavi preambule.

Najbolj stabilne rezultate sta dosegla oba računalnika MacBook, pri katerih je bilo dekodiranje praktično vedno uspešno. Obe Windows napravi sta pri večjih razdaljah pogosto zahtevali več ponovitev prenosa, kar bi lahko bila posledica manj občutljivih integriranih mikrofонов. Naprava Linux (HP ZBook) zaradi nezdržljivosti zvočnih knjižnic sprva sploh ni uspela sprejemati signala; po odpravi te težave je dosegla rezultate, primerljive z računalniki MacBook, a nekoliko slabše.

Ker vsaka naprava združuje svoj operacijski sistem in svojo zvočno strojno opremo, vpliva enega in drugega v naši postavitvi ni mogoče ločiti. Rezultati so skladni s hipotezo, da ima pomembno vlogo sprejemna zvočna strojna oprema, vendar tega nismo ločeno preverili.

E. Zaznavnost signala

Zaznavnost signala je ocenjevalo pet prisotnih oseb. Signal je jasno zaznala ena oseba (ženska), medtem ko je druga oseba (moški) signal zaznala le iz neposredne bližine vira. Preostale tri osebe signala niso zaznale. Starost oseb je bila med 20 in 25 let. To je skladno z ugotovitvami psihoakustičnih raziskav, ki kažejo, da se zgornja meja slišnega frekvenčnega območja med posamezniki razlikuje ter da nanjo vplivajo starost, individualne značilnosti sluha in drugi dejavniki. Možen vzrok slišnosti so tudi prehodni pojavi ob preklopu med frekvencama. Oddajnik sicer vsak bit pomnoži s Hannovim oknom, kar robove bitov gladi, vendar amplituda zato desetkrat na sekundo pade na nič; takšna amplitudna modulacija lahko na nelinearnem zvočniku povzroči slišne produkte. Kot izboljšavo predlagamo FSK z zvezno fazo (CPFSK) brez upadov amplitude med biti.

Med testiranjem je bila s pomočjo aplikacije phyphox opažena prisotnost okoljskega hrupa v frekvenčnem območju oddaljenega pogovora, ki pa ni prekrival uporabljenega frekvenčnega pasu (18–20 kHz). Ker raven hrupa ni bila sistematično zabeležena, natančen vpliv hrupa na stopnjo napak ni bil kvantitativno ovrednoten; komunikacija pa je kljub prisotnosti teh zvokov ostala uspešna, kar nakazuje, da hrup v slišnem območju ne moti prenosa v pasu 18–20 kHz.

V. RAZPRAVA

Rezultati eksperimenta kažejo, da je visokofrekvenčna akustična komunikacija v frekvenčnem območju 18–20 kHz

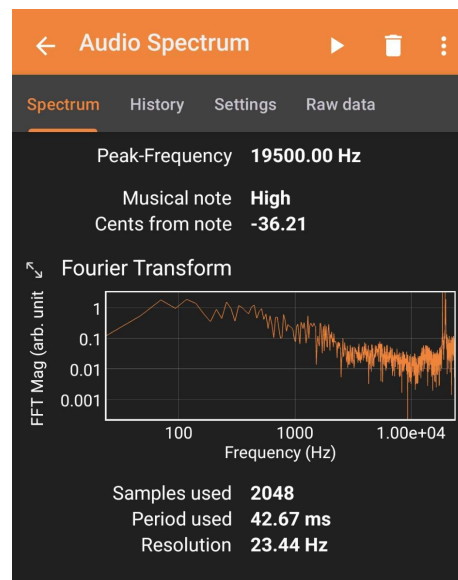


Fig. 6. Meritev oddanega signala z aplikacijo phyphox. Izmerjena dominantna frekvenca znaša približno 19,5 kHz.

tehnično izvedljiva z uporabo običajne potrošniške strojne opreme. Komunikacijski kanal je deloval na vseh testiranih operacijskih sistemih, vendar z zelo različno uspešnostjo: na napravah macOS in Linux je bil prenos uspešen v 80–100 % poskusov do 8 m, na napravah Windows pa le v 60 % poskusov do 4 m in v 10 % pri večjih razdaljah.

Meritve z uporabo programa Audacity niso pokazale prisotnosti izrazitega nizkoprepustnega filtra, ki bi preprečeval predvajanje frekvenc nad približno 15 kHz. Dodatno je aplikacija phyphox med oddajanjem zaznala dominantno frekvenco približno 19,5 kHz, kar kaže, da so uporabljene naprave dejansko oddajale signal pri predvidenih frekvencah.

Uspešen sprejem smo dosegli na napravah z operacijskimi sistemi Windows, Linux in macOS, kar kaže, da noben od njih kanala ne onemogoča. Ali so razlike v uspešnosti posledica strojne opreme ali operacijskega sistema, pa v naši postavitvi ni mogoče ločiti, saj ima vsaka naprava svojo kombinacijo obeh.

Pri obeh napravah Windows smo pri večjih razdaljah opazili izrazit padec uspešnosti dekodiranja, medtem ko sta oba računalnika MacBook sporočila sprejemala zanesljivo tudi pri večjih razdaljah. Ker so bile uporabljene enake frekvence, enaka implementacija in primerljivi pogoji testiranja, rezultati nakazujejo, da ima pomembno vlogo sprejemna stran. Ker je bilo sistemsko procesiranje zvoka v Windows izklopljeno, sta možni razlagi predvsem frekvenčni odziv integriranega mikrofona in morebitno filtriranje v gonilniku zvočnega kodeka, ki ga v sistemskih nastavitvah ni mogoče izklopiti. Teh dejavnikov nismo ločeno preverili. Zaradi omejenega števila testiranih naprav dokončnega sklepa o vplivu posameznih dejavnikov ni mogoče podati.

Pri interpretaciji rezultatov je treba upoštevati tudi omejeno velikost vzorca. Posamezna meritev je bila ponovljena desetkrat, zato rezultati predstavljajo predvsem primerjalno

oceno uspešnosti med različnimi napravami in ne statistično analizo z veliko populacijo vzorcev.

Implementacija preambule se je izkazala za pomembno izboljšavo komunikacijskega protokola. Brez sinhronizacije je sprejemnik pogosto začel dekodiranje sredi prenosa, kar je povzročilo napačno rekonstruirana sporočila. Po uvedbi preambule so bili prenosi v večini primerov uspešno dekodirani že v prvem poskusu.

Dosežene razdalje so istega reda kot pri raziskavi MOSQUITO [19] (do 9 m), ki pa za sprejem uporablja zvočnik namesto mikrofona, zato rezultati niso neposredno primerljivi. Bližje naši postavitvi je delo Hanspacha in Goetza [16], ki sta z zvočniki in mikrofoni prenosnikov dosegla do 19 m. Z enostavnim protokolom BFSK brez kodiranja za popravljanje napak smo na napravah macOS in Linux dosegli uspešen prenos do 8 m.

Ker sta oba testirana računalnika MacBook dosegla najbolj stabilne rezultate, medtem ko sta obe Windows napravi kazali opazno slabši sprejem, naši rezultati ne nasprotujejo Ruiuovim opisom, ki so temeljili predvsem na računalnikih MacBook. Ker smo testirali sodobne naprave, pa iz rezultatov ne moremo sklepati, kako bi se tak kanal obnesel na strojni opremi iz obdobja okoli leta 2010.

Rezultati potrjujejo tehnično izvedljivost visokofrekvenčne akustične komunikacije med fizično izoliranimi računalniki. Vendar sama izvedljivost komunikacijskega kanala še ne predstavlja dokaza za obstoj BadBIOS-a oziroma njegovih drugih domnevnih zmožnosti, kot je obstojnost v vdelani programski opremi. Naše delo potrjuje zgolj, da je eden izmed osrednjih mehanizmov, opisanih v primeru BadBIOS, tehnično izvedljiv.

Ruiu je o BadBIOS-u javno poročal oktobra 2013, približno v istem času, ko sta Hanspach in Goetz objavila akademski dokaz izvedljivosti akustičnih prikritih kanalov med prenosniki [16]. Kasneje je izvedljivost potrdila tudi raziskava MOSQUITO [19]. To ne potrjuje Ruiuovih trditev, kaže pa, da opisani komunikacijski mehanizem sam po sebi ni bil tehnično nemogoč.

A. Omejitve raziskave

Eksperiment je bil izveden na omejenem številu naprav, zato vpliva operacijskega sistema ni bilo mogoče ločiti od vpliva posamezne izvedbe zvočne strojne opreme. Frekvenčnega odziva mikrofona nismo ločeno izmerili, ravni hrupa v prostoru nismo instrumentalno beležili, vsaka meritev pa je bila ponovljena le desetkrat, pri čemer rezultati niso ločeni po oddajniku. Uspešnost smo merili samo kot delež pravilno sprejetih celotnih sporočil; stopnje bitnih napak (BER) nismo računali, protokol pa ne vsebuje kodiranja za odkrivanje ali popravljanje napak, ki bi uspešnost lahko izboljšalo. Nadaljnje raziskave bi morale vključevati več računalnikov z enakimi operacijskimi sistemi in različnimi zvočnimi napravami, kar bi omogočilo natančnejšo analizo vpliva mikrofona ter analognih filtrov na uspešnost akustične komunikacije.

B. Protiukrepi

Najzanesljivejši protiukrep na fizično izoliranih računalnikih je fizična odstranitev ali izklop mikrofona in zvočnikov, kar je skladno tudi z Ruiuovim poročilom, da se je domnevna komunikacija ustavila po onemogočenju zvočnih komponent. Kjer to ni mogoče, lahko nizkoprepustni filter v gonilniku ali zvočnem kodeku (npr. pri približno 16 kHz) odstrani frekvence, ki jih uporablja takšen kanal, za večino uporabnikov pa ne vpliva na slišni zvok. Možno je tudi programsko ali strojno zaznavanje neobičajnih signalov nad približno 17 kHz ter aktivno motenje tega frekvenčnega pasu s šumom.

VI. ZAKLJUČEK

V tem članku smo implementirali in testirali visokofrekvenčni akustični komunikacijski kanal med fizično izoliranimi računalniki z namenom ovrednotenja tehnične izvedljivosti koncepta BadBIOS. Eksperiment je pokazal, da je prenos podatkov z FSK modulacijo v območju 18–20 kHz mogoč na potrošniški strojni opremi brez specializirane opreme, pri čemer se je uspešnost dekodiranja med sprejemnimi napravami močno razlikovala: naprave Windows so bile slabše že do 4 m, pri večjih razdaljah pa je njihova uspešnost padla na 10 %.

Rezultati nakazujejo, da je omejujoči dejavnik predvsem sprejemna stran, saj so vse naprave signal uspešno oddajale, sprejem pa se je med njimi močno razlikoval. Ali gre za frekvenčni odziv mikrofona ali filtriranje v gonilniku, nismo ločeno preverili.

Vpliva operacijskega sistema in strojne opreme v naši postavitvi ni bilo mogoče ločiti; najboljše rezultate so dosegli sprejemniki naprav MacBook.

Dobljeni rezultati kažejo, da ultrazvočna komunikacija, kakršno je opisal Dragos Ruiu, ni v nasprotju s tehničnimi zmožnostmi sodobne potrošniške strojne opreme.

Rezultati potrjujejo izvedljivost konkretnega visokofrekvenčnega akustičnega komunikacijskega kanala v testiranih pogojih. Ne potrjujejo obstoja BadBIOS-a, njegove domnevne obstojnosti v vdelani programski opremi, samodejnega širjenja ali izvajanja komunikacije neposredno iz okolja BIOS oziroma UEFI. Nadaljnje raziskave bi morale ločeno izmeriti frekvenčni odziv mikrofona in vpliv gonilnikov ter podrobneje preučiti vpliv različnih zvočnih kodekov, analognih filtrov in implementacije komunikacije neposredno v okolju BIOS oziroma UEFI, kar ostaja odprto raziskovalno vprašanje.

REFERENCES

- [1] M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in *Information Hiding*, vol. 1525, pp. 124–142, Springer, 1998.
- [2] W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," *Computers & Security*, vol. 4, no. 4, pp. 269–286, 1985.
- [3] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances in Cryptology — CRYPTO '96*, pp. 104–113, Springer, 1996.
- [4] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO '99*, pp. 388–397, Springer, 1999.
- [5] B. W. Lampson, "A Note on the Confinement Problem," *Communications of the ACM*, vol. 16, no. 10, pp. 613–615, 1973.
- [6] D. Goodin, "Meet BadBIOS: The Mysterious Mac and PC Malware That Jumps Air Gaps," *Ars Technica*, Oct. 2013. [Online]. Available: <https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/>
- [7] D. Goodin, "Researcher Skepticism Grows Over BadBIOS Malware Claims," *Ars Technica*, Nov. 2013. [Online]. Available: <https://arstechnica.com/information-technology/2013/11/researcher-skepticism-grows-over-badbios-malware-claims/>
- [8] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "AirHopper: Bridging the Air-Gap Between Isolated Networks and Mobile Phones Using Radio Frequencies," in *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*, pp. 58–67, IEEE, 2014.
- [9] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," in *USENIX Security Symposium*, pp. 849–864, 2015.
- [10] M. Guri, M. Monitz, and Y. Elovici, "USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, pp. 264–268, IEEE, 2016.
- [11] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert Signaling Channel Between Air-Gapped Computers Using Thermal Manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*, pp. 276–289, IEEE, 2015.
- [12] M. Guri, B. Zadov, and Y. Elovici, "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED," pp. 161–184, Springer International Publishing, Cham, 2017.
- [13] M. Guri, D. Bykhovsky, and Y. Elovici, "air-jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)," *arXiv preprint arXiv:1709.05742*, 2017.
- [14] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields," *arXiv preprint arXiv:1802.02700*, 2018.
- [15] M. Guri, A. Daidakulov, and Y. Elovici, "MAGNETO: Covert Channel Between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields," *arXiv preprint arXiv:1802.02317*, 2018.
- [16] M. Hanspach and M. Goetz, "On Covert Acoustical Mesh Networks in Air," *Journal of Communications*, vol. 8, no. 11, pp. 758–767, 2013.
- [17] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers," *arXiv preprint arXiv:1606.05915*, 2016.
- [18] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Speake(a)r: Turn Speakers to Microphones for Fun and Profit," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, USENIX Association, 2017.
- [19] M. Guri, Y. Elovici, and B. Zadov, "MOSQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Computers Using Speaker-to-Speaker Communication," *arXiv preprint arXiv:1803.03422*, 2018. [Online]. Available: <https://arxiv.org/pdf/1803.03422>
- [20] A. V. Oppenheim and R. W. Schaffer, "Discrete-Time Signal Processing," 3rd ed., Pearson, 2010.
- [21] Intel Corporation, "High Definition Audio Specification," Rev. 1.0a, Jun. 2010. [Online]. Available: <https://www.intel.com/content/dam/www/public/us/en/documents/product-specifications/high-definition-audio-specification.pdf>
- [22] Duckpedia, "BadBIOS: FSK Ultrasonic Communication Demo," *GitHub*, 2026. [Online]. Available: <https://github.com/Duckpedia/BadBIOS>