

Prezentacija i usporedba tema za diplomski rad

Zagreb, siječanj 2026.

Autor: Ante Čavar
Mentor: prof. Stjepan Groš

Pregled

1. Predstavljanje tema
2. Prednosti
3. Mane
4. Usporedba
5. Zaključak
6. Literatura

Osjetilna sposobnost ESP32 uz pomoć WiFi-a i CSI podataka

- CSI (Channel State Information): stalno prisutan izvor informacija (OS obično te informacije skriva no Linux i ESP-IDF omogućuju čitanje tih informacija)
- Korištenje ESP32 platforme -> OGROMAN iskorak u polju “nevizualnog” nadziranja (špijunaža, nadziranje starijih, nadzor u osjetljivim prostorijama...)
- 3 stanja obrade signala
 - Uklanjanje šuma -> ekstrakcija značajki -> klasifikacija (prazna soba, x osoba prisutno, osoba stoji/sjedi/leži...)
 - U generativnim dubokim modelima zadnji korak je zamjenjen sa modeliranjem (prostora)
- Točnost klasifikacije u “divljini” iznosi između 69% i 76%

Prednosti - WiFi

- Privatnost bez kamera
 - vizualna privatnost (spavaće sobe, kupaoalice...)
- Niska cijena i sveprisutnost
 - ESP32 pločice koštaju manje od 10€ te se ne mora mijenjati postojeća infrastruktura
- Bez prepreka
 - WiFi signal prolazi kroz zidove za razliku od infracrvenih i fotonskih signala (toplina i svjetlost) te se sa 2-3 pločice može osigurati pokrivenost cijelog stana (ovisi o veličini i rasporedu i materijalu zidova)
- Neiskorišten potencijal i nezasićeno tržište
 - Na tržištu ne postoji rješenje koje je ovdje opisano a vjerujem da bi se ljudi osjećali sigurnije kad ih ne bi konstantno kamera promatrala

Mane - WiFi

- Ograničena publika
 - Broj ljudi/ustanova kojima je ovo rješenje potrebno nije velik
 - Eventualno zdravstvene ustanove, starački domovi, moteli...
- Nepouzdati podatci
 - U “divljini” je teško dobiti točne oznake podataka zbog previše varijabli koje utječu na CSI
- Sigurnosni rizici
 - Kako je tema podskup pametnih domova izložena je istim napadima
 - Zlonamjerni aktori mogu iskoristiti naše rješenje za prisluškivanje
 - Alternativna tema: Izgradnja open-source sustava poput AntiSense i ScatterShield koji služe kao ometači CSI informacija; trenutno se primjenjuju u korporativnom okruženju i u visokosigurnosnim uredskim prostorima (npr. sastanak u SOA-i)

Trovanje/Lažiranje digitalnog otiska (u tražilicama)

- Tražilice prikupljaju veliki broj suptilnih informacija (konfiguracija sustava, hardware, software) kako bi izgradile UUID (Unique User Identifier)
 - Canvas Fingerprinting, WebGL i AudioContext, nabranje ekstenzija, sistemski podatci
 - Informacije skupljene koristeći JavaScript API
- Na temelju tog tog otiska se gradi psihološki profil korisnika od strane više različitih “trackera” koji međusobno razmjenjuju informacije
- Lažiranje
 - Zamjena podataka generičkim ili uobičajnim vrijednostima
 - Chameleon
- Trovanje
 - Dodavanje nasumičnog šuma običnim podacima
 - CanvasBlocker

Prednosti - Fingerprinting

- Ne bi bilo “izmišljanje tople vode”
 - Trenutna rješenja se fokusiraju na JavaScript dok WASM (WebAssembly) i dalje ostaje netaknuto područje
- Gašenje ili onemogućavanje JS-a dovodi do slomljenih stranica
 - WASM bi nam omogućio trovanje/lažiranje u kompletno novoj domeni
- Beskonačna igra mačke i miša
 - Ne postoji konačno rješenje već se strane prilagođavaju promjenama i poboljšanjima

Mane - Fingerprinting

- **Neznanje**
 - WASM mi je nepoznato područje te nisam ni siguran bi li mogao uspješno napraviti programsko rješenje
- **Zasićenost**
 - Većina ljudi je dovoljno sretna s postojećim rješenjima te se očekuje od autora trenutnih rješenja da će se prilagođavati kako “trackeri” budu pametniji
- **Teško naplativo i upitna publika**
 - Ovakve usluge svi očekuju za besplatno
 - Tema je jedinstvena te ovakvo rješenje bi bilo zanimljivo samo nekom tko je dovoljno osviješten

Usporedba

	Osjetilna sposobnost ESP32 uz pomoć WiFi-a i CSI podataka	Trovanje/Lažiranje digitalnog otiska (u tražilicama)
Izvedivost	5	5
Naplativost	4	2
Apriori znanje	3	1
Korisnost	3	5
Prezentabilnost	4	3
Ocjena	$5+4*2+3*2=19 /5= 3.8$	$2*5+3+2+1=16 /5= 3.2$

Zaključak

- Smatram da je projekt sa ESP32 mnogo realniji a uz to je ostvarivo i lakše ga je monetizirati
- Ja nemam ništa protiv ijedne ideje te sam otvoren za savjete
- Uz limit od otprilike 4-5mj. (rok je u 7. mjesecu) smatram da je tema sa WiFi i ESP32 daleko ostvarivija

Literatura

- M. Cominelli, F. Gringoli, and R. Lo Cigno, "AntiSense: Standard-Compliant CSI Obfuscation Against Unauthorized Wi-Fi Sensing," *Computer Communications*, vol. 185, no. 4, pp. 200–210, Mar. 2022.
- Y. Chen and J. Wang, "ScatterShield: Defending Against Unauthorized WiFi Sensing with Backscatter Tags," *IEEE Transactions on Mobile Computing*, vol. 24, no. 12, Dec. 2025.
- J. Strohmer, R. Sterzinger, C. Stippel, and M. Kampel, "Through-Wall Imaging Based on WiFi Channel State Information," *arXiv preprint arXiv:2401.17417*, Jan. 2024.
- Y. Zhang, R. Bao, and X. Shi, "A Novel WiFi-Based Personnel Behavior Sensing with A Deep Learning Method," *Sensors*, vol. 25, no. 6, Mar. 2025.
- M. S. M. S. Annamalai, I. Bilogrevic, and E. De Cristofaro, "Beyond the Crawl: Unmasking Browser Fingerprinting in Real User Interactions," in *Proc. WWW Conf.*, 2025, pp. 3896–3907.
- S. Shahcheraghi, J. Link, M. Cominelli, and A. Asadi, "Fingerprinting detection in the WebAssembly era: Defenses and gaps," *Computers & Security*, vol. 157, Oct. 2025.
- P. N. Bahrami, D. Cutler, and I. Bilogrevic, "Byte by Byte: Unmasking Browser Fingerprinting at the Function Level Using V8 Bytecode Transformers," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2025, pp. 3723–3736.
- B. Amin Azad, O. Starov, P. Laperdrix, and N. Nikiforakis, "Taming The Shape Shifter: Detecting Anti-fingerprinting Browsers," in *Proc. DIMVA*, 2020, pp. 189–209.

Kraj