Zaprimljen: 9.6.2025.
Odobren za objavu: 23.7.2025.
Stručni rad

SIGURNOSNI IZAZOVI IoT UREĐAJA

Ivan Matasović [1], Mato Galović [2], Mato Kokanović [3], Zoran Crnac [4]
[1] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, imatasovic@unisb.hr
[2] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mgalovic@unisb.hr
[3] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mkokanovic@unisb.hr
[4] Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, zcrnac@unisb.hr

Sažetak: Internet stvari (IoT) predstavlja sveprisutnu tehnologiju modernog doba koja omogućuje međusobnu komunikaciju uređaja i razmjenu podataka putem interneta. S obzirom na sve širu primjenu u pametnim kućama, industriji i kritičnoj infrastrukturi, sigurnost IoT uređaja postaje ključno pitanje. Zbog svoje povezanosti i često nedovoljne razine zaštite, IoT uređaji predstavljaju značajnu metu za različite oblike kibernetičkih napada.
Cilj ovog rada je analizirati osnovne prijetnje koje se odnose na sigurnost IoT uređaja, identificirati ranjivosti, te prikazati moguće metode zaštite i dobre prakse u području kibernetičke sigurnosti. U sklopu praktičnog dijela rada provedeno je testiranje sigurnosti jedne pametne WiFi kamere, kako bi se kroz konkretan primjer pokazale potencijalne slabosti i načini zaštite.
Rad donosi pregled aktualnih sigurnosnih prijetnji, metode sigurnosnog testiranja, kao i prijedloge tehničkih i organizacijskih mjera zaštite u skladu s relevantnim sigurnosnim standardima.

Ključne riječi: Internet stvari, IoT, kibernetička sigurnost, WiFi kamera, ranjivosti, sigurnosno testiranje

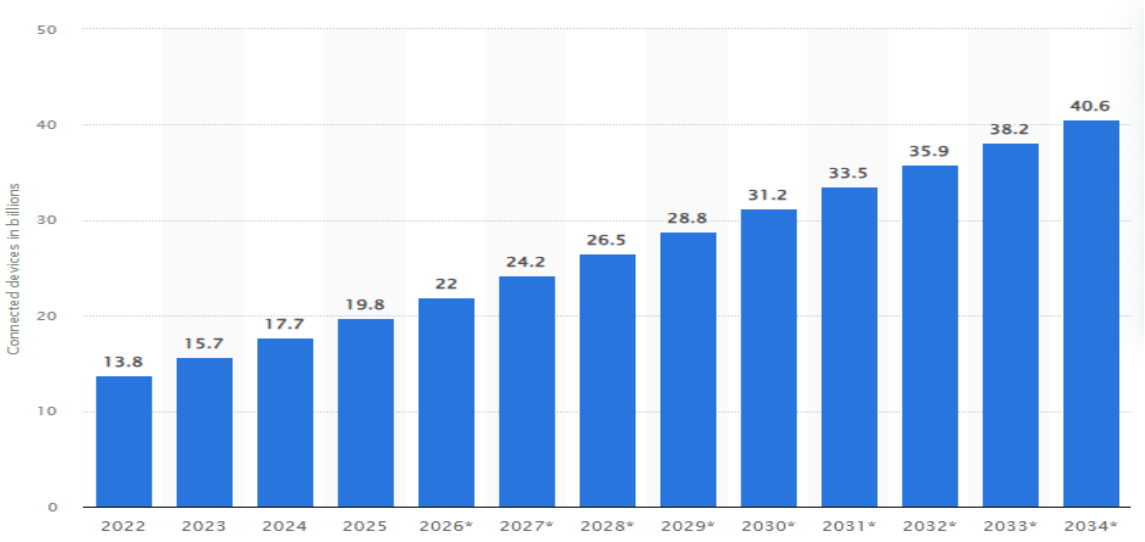
1. Uvod

Internet stvari (Internet of Things, IoT) predstavlja mrežu fizičkih uređaja opremljenih senzorima, softverom i mogućnostima povezivanja putem interneta radi razmjene podataka i upravljanja. Među najrašireniji IoT uređajima nalaze se Wi-Fi nadzorne kamere koje se koriste u pametnim domovima, poslovnim prostorima i industrijskim okruženjima (Sicari i sur., 2015). Iako omogućuju jednostavan i pristupačan videonadzor, sve je veća zabrinutost zbog sigurnosnih rizika koje takvi uređaji predstavljaju.
Prethodna istraživanja pokazala su da mnogi IoT uređaji, uključujući Wi-Fi kamere, često sadrže značajne softverske i hardverske ranjivosti, kao što su nezaštićeni pristupni portovi, slaba enkripcija, korištenje zadano postavljenih lozinki i nepostojanje mehanizama za ažuriranje (Alrawi i sur., 2019). U kombinaciji s činjenicom da su ovi uređaji stalno spojeni na internet, čak i manji propusti mogu rezultirati ozbiljnim kompromitiranjem privatnosti korisnika ili omogućavanjem udaljenog pristupa napadačima (Roman i sur., 2011).
Cilj ovog rada je istražiti i testirati softverske i hardverske ranjivosti konkretne Wi-Fi kamere, kako bi se utvrdila razina njezine sigurnosti. Fokus je stavljen na identifikaciju potencijalno iskoristivih propusta, analizu načina

njihove zloupotrebe i izradu prijedloga za poboljšanje sigurnosti uređaja.
Zadaće koje vode prema ostvarenju ovog cilja uključuju:

- Analizu poznatih sigurnosnih problema povezanih s Wi-Fi nadzornim kamerama;
- Istraživanje specifikacija i arhitekture testiranog modela;
- Provođenje testova sigurnosti softvera (firmware, mrežni servisi, API sučelja);
- Analizu fizičkog sklopa i mogućih hardverskih ulaznih točaka (npr. UART, JTAG);
- Izradu tehničkog izvještaja s preporukama za unaprjeđenje sigurnosti.

Iako je problem sigurnosti IoT uređaja prepoznat u znanstvenoj i industrijskoj zajednici, u praksi i dalje postoji velik broj nesigurnih proizvoda na tržištu. U ovom radu istražuje se konkretan primjer kako bi se na praktičan način ilustrirala širina i ozbiljnost prijetnji koje proizlaze iz nedostatne zaštite Wi-Fi nadzornih uređaja.
Trenutno se procjenjuje da postoji oko 17 milijardi povezanih IoT uređaja, s projekcijama koje predviđaju rast na 22 milijardi do 2026. godine i gotovo 32 milijardi do 2030. godine (https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/). Ovaj rast potaknut je sve većom integracijom IoT rješenja u svakodnevni život i industrijske procese. U kućanstvima, pametni uređaji poput Wi-Fi kamera, termostata i kućanskih aparata postaju sve prisutniji, dok industrijski sektor koristi IoT za optimizaciju proizvodnje, održavanja i logistike.



Slika 1. Broj spojenih IoT uređaja i predikcija za naredne godine (izvor: Statista 2025)

2. Sigurnosne prijetnje u IoT okruženju

U ovome poglavlju opisat ćemo ranjivosti, prijetnje i napade na IoT uređaje. Ranjivosti IoT uređaja možemo podijeliti na četiri kategorije (Mukhtar i sur., 2023):

- Ranjivosti uzrokovane korisničkim rukovanjem
- komunikacijske ranjivosti
- ranjivosti firmwarea i softwarea
- fizička ranjivost uređaja

Što se tiče ranjivosti uzrokovane korisničkim rukovanjem tu se misli na slabe lozinke i zanemarivanje ažuriranja. Mnogi IoT uređaji dolaze s unaprijed postavljenim i jednostavnim lozinkama (Li i Da Xu, 2017), što predstavlja ozbiljan sigurnosni rizik. Iako se preporučuje njihova promjena pri prvom

korištenju, korisnici tu uputu često zanemaruju ili lozinke zamijene lako pamtljivim, ali slabim kombinacijama. Takav pristup značajno povećava rizik od neovlaštenog pristupa i kompromitacije uređaja.

Dodatni problem predstavlja ignoriranje sigurnosnih ažuriranja. Iako proizvođači povremeno izdaju nadogradnje kojima se ispravljaju poznate ranjivosti, korisnici ih često ne instaliraju. Kada se ta ažuriranja dulje vrijeme sustavno izbjegavaju, uređaji ostaju nezaštićeni od poznatih prijetnji, čime se otvara prostor za iskorištavanje propusta putem zlonamjernog softvera ili ciljanih napada.

Uporaba nesigurnih komunikacijskih protokola predstavlja komunikacijsku ranjivost. U IoT okruženjima uređaji su često međusobno povezani unutar iste lokalne mreže, što znači da kompromitacija jednog uređaja može omogućiti širenje napada i na ostale povezane komponente sustava. Ovakva povezanost povećava rizik od lateralnog kretanja napadača unutar mreže.

Dodatno, zbog ograničenih resursa (procesorske snage, memorije i potrošnje energije), proizvođači često odabiru mrežne protokole koji nude bolje performanse i manji zahtjev za resursima, ali uz kompromis u sigurnosti. Takvi protokoli mogu sadržavati ranjivosti koje otvaraju vrata potencijalnim napadima.

Stoga je nužno pronaći ravnotežu između učinkovitog korištenja dostupnih resursa i implementacije sigurnosnih mehanizama koji mogu zaštititi uređaje i podatke u mreži od zlonamjernih aktivnosti (Li i Da Xu, 2017)

Komunikacijsku ranjivost može uzrokovati i nedostatak enkripcije tijekom prijenosa podataka. Sigurnost IoT sustava u velikoj mjeri ovisi o zaštiti podataka koje prikupljaju senzori na sloju percepcije. Korištenjem enkripcije moguće je zaštititi prijenos podatkovnih paketa i spriječiti neovlašteni pristup osjetljivim informacijama.

Ipak, mnogi IoT uređaji komuniciraju putem nepouzdanih bežičnih medija, a zbog ograničenih hardverskih resursa često nisu u mogućnosti implementirati snažne kriptografske algoritme. Kao rezultat, podaci se ponekad prenose u nešifriranom obliku, što ih čini ranjivima na presretanje, manipulaciju ili neovlašteni pristup (Anand i sur., 2020). Takva ograničenja čine ove uređaje posebno osjetljivima na napade usmjerene na krađu podataka i narušavanje privatnosti korisnika, što dodatno naglašava potrebu za sigurnosno svjesnim dizajnom već u fazi razvoja IoT sustava.

Još jednu vrstu ranjivosti je potrebno spomenuti, a to je ranjivost firmwarea i softwarea. Sigurnost IoT sustava u velikoj mjeri ovisi o pouzdanosti firmwarea i softvera koji omogućuju komunikaciju između hardverskih komponenti i aplikacijskih slojeva. Firmware, kao temeljna programska podrška pohranjena u trajnoj memoriji uređaja, ključan je za njegovo osnovno funkcioniranje. Međutim, mnogi IoT uređaji ne primaju redovita ažuriranja, što ih čini ranjivima na napade koji iskorištavaju poznate sigurnosne propuste. Za razliku od tradicionalnih IT sustava, IoT uređaji često ostaju bez podrške za sigurnosne nadogradnje, čime se povećava vjerojatnost kompromitacije.

Dodatnu prijetnju predstavlja način na koji se nadogradnje provode. U slučajevima kada uređaji koriste nesigurne ili neprovjerene mehanizme ažuriranja, postoji rizik od instalacije zlonamjernog softvera putem korumpiranih datoteka. Takve situacije mogu dovesti do potpunog preuzimanja kontrole nad uređajem, što ima ozbiljne posljedice i za privatne korisnike i za poslovne sustave. Kako bi se izbjegle takve prijetnje, važno je koristiti digitalno potpisana ažuriranja i distribuirati ih preko sigurnih, enkriptiranih kanala.

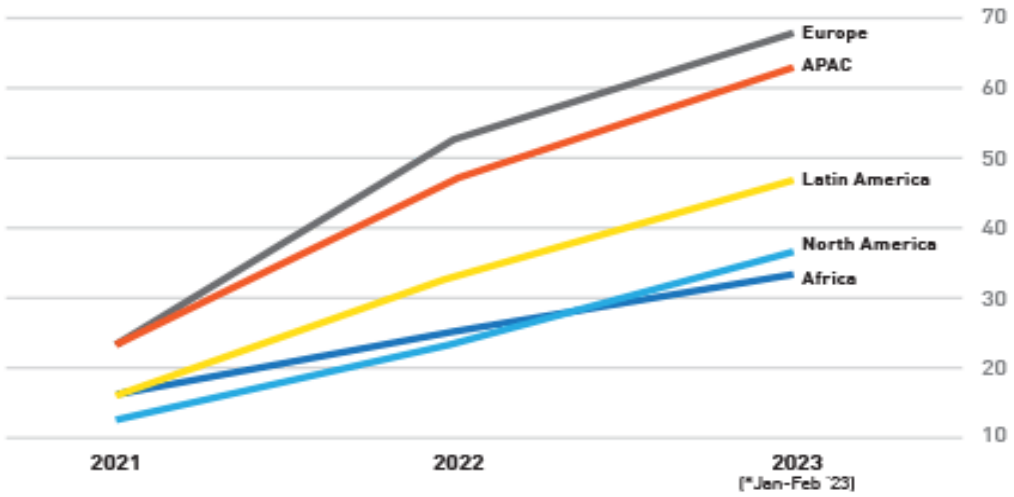
Uz ranjivosti povezane s firmwareom i softverom, značajnu prijetnju predstavljaju i nesigurna web sučelja koja se često koriste za upravljanje IoT uređajima. Ova sučelja ponekad

uključuju slabu autentifikaciju i autorizaciju, što omogućava neovlaštenim osobama pristup osjetljivim funkcijama uređaja. Dodatno, izostanak HTTPS protokola omogućuje presretanje i manipulaciju podacima tijekom prijenosa. Uređaji koji nemaju zaštitu od ponavljanih pokušaja prijave posebno su osjetljivi na napade, čime se dodatno povećava rizik od kompromitacije.
Kombinacija nepouzdanog firmwarea, rijetkih ili nesigurnih ažuriranja i ranjivih web sučelja čini IoT sustave atraktivnim metama za napadače. Stoga je nužno već u fazi dizajna osigurati provjerene sigurnosne mehanizme, kontinuirano održavanje softvera i jasno definirane sigurnosne protokole za upravljanje uređajima.
Fizička sigurnost predstavlja ključni, ali često zanemareni aspekt zaštite IoT sustava. Za razliku od serverskih ili mrežnih komponenti koje se nalaze u zaštićenim prostorima, mnogi IoT uređaji instalirani su na lako dostupnim lokacijama — u kućama, na ulicama, industrijskim postrojenjima ili prometnoj infrastrukturi — što ih čini izloženima fizičkim prijetnjama. Napadač koji fizički pristupi IoT uređaju može izvršiti niz potencijalno destruktivnih ili špijunskih aktivnosti.

Jedan od najčešćih rizika fizičkog pristupa je mogućnost povezivanja s dijagnostičkim sučeljima kao što su UART ili JTAG. Preko tih portova moguće je izravno komunicirati s uređajem, čitati i mijenjati firmware, zaobići autentifikacijske mehanizme ili čak zamijeniti originalni firmware zlonamjernim inačicama. Ovakvi napadi mogu rezultirati potpunim preuzimanjem kontrole nad uređajem bez potrebe za mrežnim iskorištavanjem ranjivosti.

Također, fizički pristup omogućuje napadaču vađenje pohranjenih podataka iz memorije uređaja, uključujući osjetljive informacije poput lozinki, autentifikacijskih tokena ili kriptografskih ključeva. Ako uređaj ne koristi enkripciju memorije, podaci su lako dostupni i mogu se zloupotrijebiti za daljnje napade.

Još jedna prijetnja odnosi se na manipulaciju samim komponentama uređaja. Napadač može fizički onesposobiti senzore, zamijeniti ih ili preusmjeriti njihove ulazne/izlazne signale, što može dovesti do krivih očitanja, donošenja pogrešnih odluka u sustavu ili lažnih alarma. U nekim slučajevima moguće je ugraditi dodatni mikroupravljač ili špijunski modul koji neprimjetno bilježi komunikaciju ili manipulira podatkovnim tokovima (ENISA, 2019)



Slika 2. Porast napada na IoT uređaje (izvor: Check Point Research, 2023)

Na slici 2. se može vidjeti da je Europa trenutno regija koja trpi najviše napada usmjerenih na IoT uređaje, s prosjekom od gotovo 70 takvih napada po organizaciji tjedno. Slijedi regija Azija-Pacifik s 64 napada, Latinska Amerika s 48, Sjeverna Amerika s 37 (uz najveći porast u odnosu na 2022. godinu – 58%) te Afrika s 34 tjedna IoT kibernetička napada po organizaciji (Check Point Research, 2023).

3. Metodologija sigurnosnog testiranja

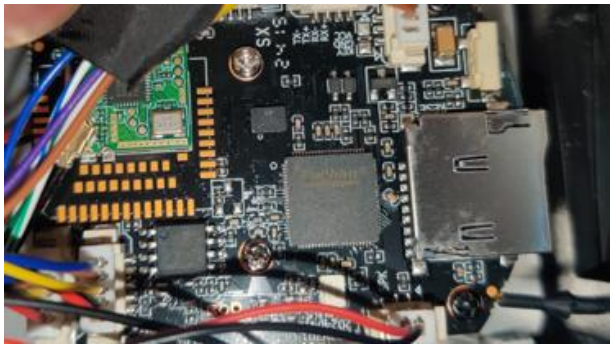
Za testiranje korištena je jedna bežična kamera bez vidljive oznake proizvođača kao što se može vidjeti na slici ispod.

Slika 3. Korištena Wi-Fi kamera za testiranje

Sigurnosno testiranje Wi-Fi kamere provedeno je kroz dva glavna segmenta: hardversko testiranje i softversko testiranje. Ovim pristupom cilj je detaljno identificirati ranjivosti i sigurnosne nedostatke kako na fizičkoj i firmware razini, tako i u mrežnoj komunikaciji uređaja.

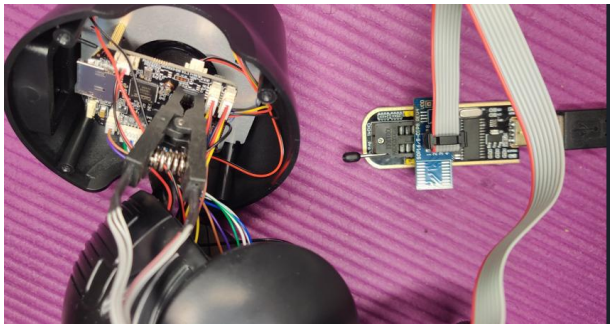
3.1. Hardversko testiranje

Ovo testiranje fokusira se na analizu fizičkih komponenti uređaja i njegove interne programske podrške (firmwarea), s ciljem otkrivanja mogućih sigurnosnih propusta koji proizlaze iz hardverske konstrukcije i implementacije. Prvi korak bio je pažljivo otvaranje kućišta kamere i detaljna inspekcija tiskanih pločica (PCB). Identificirani su ključni čipovi kao što su mikrokontroler, memorijski čipovi i Wi-Fi modul. Fotografiranjem i bilježenjem oznaka omogućena je daljnja analiza proizvođača i modela komponenti, kao i njihova tehnička specifikacija.

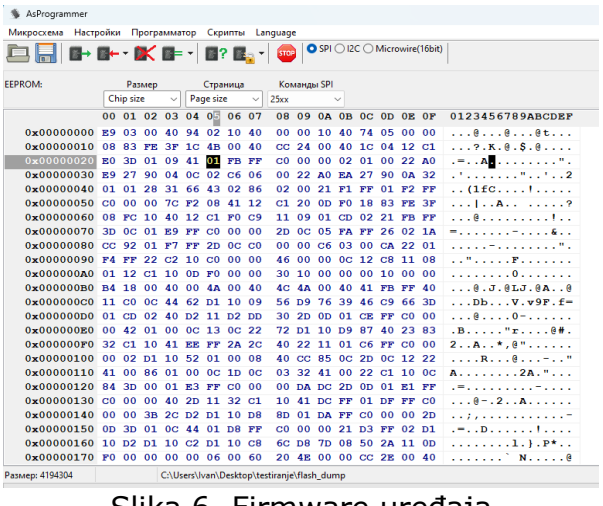


Slika 4. PCB pločica rastavljene kamere

Kamera koristi FH885V201 integrirani krug (SoC) koji ima ugrađeni audio/video podršku, USB podršku, CPU, memoriju, Wi-Fi modul te EEPROM integrirani krug s oznakom FM25Q128A. U EEPROM-u se nalazi firmware uređaja te ga korištenjem specijalizirane opreme možemo „izvući" iz uređaja te detaljnije analizirati kao što je prikazano na slici ispod.

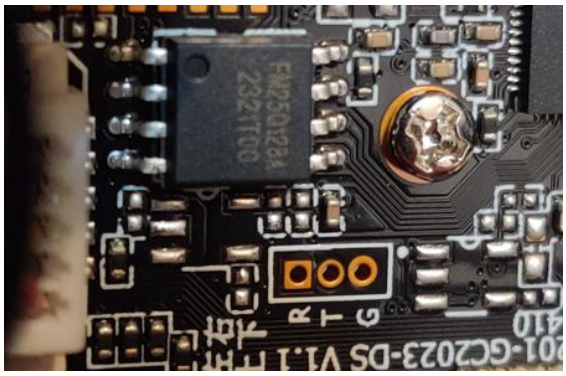


Slika 5. „Izvlačenje" firmwarea uređaja



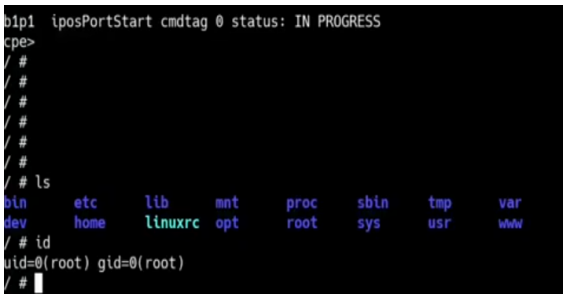
Slika 6. Firmware uređaja

Kada je firmware na raspolaganju može se detaljnije analizirati alatima poput binwalk. U firmwareu se može naći lozinke, SSH/Telnet pristup, web sučelja itd.
Još se može primijetiti pristup serijskoj konzoli, proizvođač nam je olakšao dodatnon pristup time što je označio pinove: R (receive), T (transmit), G (ground).



Slika 7. Pristup serijskoj konzoli

Istom opremom koju smo koristili da dođemo do firmwarea možemo iskoristiti da gledamo tzv. boot poruke i dođemo do root pristupa.



Slika 8. Glavni (root) pristup

3.2. Softversko testiranje

Softversko testiranje fokusira se na analizu mrežnog prometa uređaja i njegove interakcije s ostalim komponentama mreže, s ciljem identificiranja ranjivosti u protokolima i prijenosu podataka. Korištenjem alata Wireshark (verzija 3.4.8) snimljen je promet koji Wi-Fi kamera generira tijekom različitih operacija (povezivanje, prijenos videa, komunikacija s aplikacijom ili oblakom). Analiza snimljenog prometa obuhvatila je provjeru korištenja sigurnih protokola, prisutnost nezaštićenih ili nešifriranih prijenosa, te potencijalne napade presretanja ili manipulacije podacima.
Prilikom snimanja mrežnog prometa s u Wiresharku (verzija 3.4.8) mogu se uočiti sljedeće vrste komunikacije:

- Nešifrirani protokoli i običan tekst: HTTP i RTSP bez enkripcije
- Korištenje zastarjelih ili nesigurnih protokola: Telnet

4. Rezultati i rasprava

U ovom istraživanju korištena je bežična Wi-Fi kamera nepoznatog proizvođača, čije kućište i unutarnji sklop predstavljaju tipičan primjer jeftinijih IoT uređaja na tržištu. Sigurnosno testiranje uređaja provedeno je kroz dva komplementarna segmenta, hardversko i softversko testiranje, s ciljem što detaljnijeg otkrivanja sigurnosnih ranjivosti. Otvaranjem kućišta i analizom tiskane pločice identificirani su ključni hardverski elementi uređaja, među kojima se ističe integrirani krug FH885V201, koji obuhvaća procesorsku jedinicu, Wi-Fi modul, audio/video podršku i memoriju. Također je prisutan EEPROM s firmwareom uređaja, koji je uspješno „izvučen" korištenjem specijalizirane opreme.
Pristup serijskoj konzoli dodatno je olakšan fizičkim označavanjem pinova za primanje (R), prijenos (T) i masu (G), što je omogućilo nadzor boot poruka i stjecanje root pristupa uređaju. Ovakva razina pristupa potvrđuje mogućnost fizičkog iskorištavanja ranjivosti na firmware razini, što ukazuje na slabosti u zaštiti uređaja protiv neovlaštenog pristupa.
Softverska analiza usmjerena je na mrežni promet generiran od strane kamere tijekom različitih funkcionalnosti poput povezivanja, prijenosa video zapisa i komunikacije s upravljačkim aplikacijama ili oblakom. Korištenjem Wiresharka detektirani su različiti protokoli, među kojima su istaknuti nešifrirani protokoli poput HTTP i RTSP koji se koriste bez adekvatne enkripcije.

Također je uočeno korištenje zastarjelih i nesigurnih protokola poput Telneta, što dodatno ugrožava sigurnost uređaja.

5. Zaključak

Internet stvari (IoT) značajno mijenja način na koji upravljamo svakodnevnim uređajima, uključujući i Wi-Fi nadzorne kamere, koje su sveprisutne u kućanstvima i industriji. Međutim, provedeno istraživanje i testiranje konkretne Wi-Fi kamere otkrilo je brojne sigurnosne ranjivosti, kako na hardverskoj tako i na softverskoj razini. Slaba zaštita pristupnih portova, prisutnost nešifriranih komunikacijskih protokola te lakoća stjecanja root pristupa putem fizičkog priključka ukazuju na ozbiljne sigurnosne propuste. Ovi nalazi potvrđuju da nedostatna zaštita IoT uređaja može ugroziti privatnost korisnika i sigurnost mrežnih sustava. Stoga je nužno da proizvođači unaprijede sigurnosne mehanizme, redovito izdaju i implementiraju ažuriranja te educiraju korisnike o sigurnosnim praksama, kako bi se smanjili rizici od kibernetičkih napada u rastućem IoT ekosustavu.

6. Literatura

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). SoK: Security Evaluation of Home-Based IoT Deployments. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2019.00031

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access, 8, 168825-168853, https://ieeexplore.ieee.org/document/9189773

Check Point Research, https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

ENISA. (2019). Good Practices for Security of Internet of Things in the context of Smart Manufacturing. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Li, S., Da Xu, L. (2017). Securing the internet of things. Syngress.

Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study, https://www.mdpi.com/2073-8994/15/11/1978

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. Computer, 44(9), 51–58. https://doi.org/10.1109/MC.2011.291

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Statista.com, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

SECURITY CHALLENGES OF IoT DEVICES

Summary: The Internet of Things (IoT) represents a ubiquitous modern technology that enables communication between devices and the exchange of data via the internet. Given its widespread use in smart homes, industry, and critical infrastructure, the security of IoT devices has become a key concern. Due to their connectivity and often insufficient levels of protection, IoT devices are a significant target for various forms of cyberattacks.
The aim of this paper is to analyze the main threats related to the security of IoT devices, identify vulnerabilities, and present possible protection methods and best practices in the field of cybersecurity. As part of the practical section, a security test was conducted on a smart WiFi camera to demonstrate potential weaknesses and methods of protection through a concrete example.
This paper provides an overview of current security threats, methods of security testing, and offers proposals for technical and organizational protection measures in accordance with relevant security standards.

Keywords: Internet of Things, IoT, cybersecurity, WiFi camera, vulnerabilities, security testing