SIMULACIJA NAPADA NA KOMERCIALNE SISTEME IOT

Kristjan Brataševec, Matevž Pesek kb90801@student.uni-lj.si, matevz.pesek@fri.uni-lj.si

Izvleček

Internet stvari ali IoT (Internet of Things) definira pametne naprave s senzorji in programsko opremo, ki se povezujejo z drugimi napravami in sistemi, za potrebe analize, nadzora ter avtomatizacije podatkov. Primeri takšnih naprav so pametne luči, pametni pralni, sušilni, pomivalni stroji, termostati, varnostne kamere za domove in druge, ki jih je večinoma mogoče enostavno upravljati tudi preko mobilnih aplikacij. Zaradi cenovne dostopnosti in naraščajoče razširjenosti teh naprav so vse pogostejše tudi težave, povezane s pomanjkljivimi podatkovnimi nabori in odsotnostjo avtomatiziranih posodobitev, kar predstavlja ključen varnostni in funkcionalni dejavnik zlasti pri napravah, ki so nenehno povezane z internetom. Napadalci lahko takšne varnostne pomanjkljivosti izkoristijo za nepooblaščeno zbiranje osebnih podatkov, onemogočanje delovanja naprav ali za zlorabo njihove računske moči naprave za vzpostavitev širših omrežij okuženih naprav (angl. botnet). Članek obravnava kritične probleme naprav skozi različne napade in njihov obseg ter strategije za obvladovanje ter preprečevanje napadov IoT. Dodatno analizira tudi večje pretekle napade, na primeru široko dostopnih naprav, kot so pametne žarnice in prezračevalni sistemi, pa prikaže enostavnost izvedbe napada. Prispevek kritično ovrednoti tudi trenutni trend nadomeščanja enostavnih naprav s "pametnimi" različicami, ki zaradi večje kompleksnosti in pomanjkljive varnostne zasnove postaja vse večji in težje obvladljiv varnostni izziv sodobnega digitalnega okolja.

Ključne besede: IoT, napadi DoS, napadi s ponavljanjem, napadi zaradi slabe avtentikacije, obramba pred napadi

ATTACK SIMULATION ON COMMERCIAL IOT SYSTEMS

Povzetek

Internet of Things (IoT) defines smart devices with sensors and software that connect to other devices and systems for data analysis, control and automation purposes. Examples of such devices include smart lights, smart washers, dryers, dishwashers, thermostats, home security cameras, and others, most of which can be easily controlled via mobile applications. Due to the affordability and increasing prevalence of these devices, problems related to incomplete data sets and the absence of automated updates are also becoming more common, which is a key security and functional factor for devices that are constantly connected to the Internet. Attackers can exploit such security flaws to unlawfully collect personal data, disable devices, or misuse their computing power to build larger networks of infected devices (botnets). The article discusses critical device problems through various attacks and their scope, as well as strategies for managing and preventing IoT attacks. It also analyzes major past attacks, and using widely available devices such as smart light bulbs and ventilation systems to demonstrate the ease of attack implementation. The paper also critically evaluates the current trend of replacing simple devices with "smart" versions, which, due to increased complexity and inadequate security design, is becoming an increasingly challenging and difficult-to-manage security issue in the modern digital environment.

Keywords: attack defence, DoS attacks, IoT, poor authentication attacks, reply attacks

1 UVOD

Internet stvari (IoT) je opredeljen kot omrežje, v katerem so fizični objekti, opremljeni s senzorji in aktuatorji, povezani prek brezžičnih in žičnih omrežij, kar omogoča nemoteno interakcijo in izmenjavo informacij med objekti v fizičnem in virtualnem svetu [1]. Pametne naprave v takšnem omrežju podpirajo analizo, obdelovanje in deljenje podatkov ter avtomatizacijo, s čimer spreminjajo funkcionalnost in uporabno vrednost vsakdanjih predmetov. Primer takšne integracije je sistem Flaura [2], ki preprost lonček za rastlino preoblikuje v avtomatizirano napravo IoT s funkcijo samodejnega zalivanja in oddaljenega obveščanja uporabnika o stopnji vlažnosti substrata na daljavo preko spleta.

Čeprav so mobilni telefoni, računalniki in druge splošno razširjene naprave, povezane na svetovni splet, redno deležne posodobitev operacijskih sistemov in aplikacij – te se pogosto izvajajo samodejno, v ozadju in brez posredovanja uporabnika –, pa naprave IoT, kot so pametne kamere, ključavnice, žarnice, gospodinjski aparati in termostati, takšnih avtomatskih nadgradenj večinoma ne prejemajo.

Medtem ko se uporabniki prvih že zavedajo, da posodobitve prispevajo k večji varnosti in prinašajo nove funkcionalnosti, ostaja pri napravah IoT to zavedanje nizko, čeprav so varnostna tveganja in ranljivosti primerljive ali celo večje [3]. Poleg tega naprave IoT delujejo v ozadju in redko opozarjajo na razpoložljive varnostne posodobitve ali odpravo kritičnih napak [4]. Proizvajalci takšnih naprav velikokrat ne ponujajo dolgoročne nadgradnje programske opreme, zato po odkritju varnostne pomanjkljivosti ostanejo trajno ranljive in pomenijo stalno grožnjo za uporabnike naprav [5].

Pametne naprave tako pogosto ostajajo neposodobljene bodisi zaradi pomanjkanja uporabnikove aktivne interakcije z napravo, bodisi zaradi razširjenega prepričanja – tako pri uporabnikih kot proizvajalcih –, da naprave IoT same po sebi ne predstavljajo resne nevarnosti ali bistvene grožnje. Prav ta zmotna predstava pa napadalcem ponuja signifikantno možnost za dostop in zlorabo naprav IoT [3]. Takšne naprave napadalci uporabljajo kot orodje za vohunjenje, zbiranje osebnih podatkov in vdor v človekovo zasebnost in dostojanstvo, pri čemer podatke izkoristijo sami ali pa jih prodajo naprej za nadaljnje zlorabe. Pridobljen dostop jim omogoča tudi zlorabo naprav za izvajanje napadov na druge storitve. Najbolj znan primer tovrstne zlorabe je DDoS (angl. Distributed Denial of Service) napad, pri katerem napadalci uporabijo računsko moč večjega števila, navadno nelegalno prisvojenih, pametnih naprav, da z množično obremenitvijo ciljnega sistema povzročijo njegovo nedelovanje. Takšni napadi se izvajajo z različnimi nameni: motenjem delovanja, izsiljevanjem (odkupnina), prikrivanjem drugih dejavnosti ali drugimi zlonamernimi cilji [6].

Namen in struktura članka sta pregleden prikaz trenutnega stanja naprav IoT, demonstracija napada na komercialne naprave IoT, ki so trenutno na voljo v Sloveniji, in ozaveščanje bralca o nevarnostih, povezanih s pomanjkanjem (samodejnih) posodobitev teh naprav. Prikazani napadi so kljub enostavni izvedbi precej resni, saj ne zahtevajo posebnih orodij in obširnega tehničnega znanja, ter izkoriščajo osnovne ranljivosti. Ravno ta enostavnost izvedb problematičnih napadov s proporcionalno malo zahtevanega truda in znanja, pa izpostavlja resnost in pogostost opisanih groženj v današnjem času.

2 PREGLED SORODNIH DEL

Razširjenost naprav IoT in hkrati pojav varnostno zaskrbljujočih napadov, povezanih z njimi, sta spodbudila podrobnejšo analizo in raziskovanje slednjih. Deogirikar in Vidhate sta tipe napadov razdelila na štiri kategorije: fizične, omrežne, programske in enkripcijske [7]. Predstavila sta, kako lahko napadalci škodijo napravam z različnimi pristopi – od fizičnih posegov, kot je neposredno vrivanje zlonamerne kode ali povzročanje fizične škode, do omrežnih napadov, kot je kopiranje RFID značk, in različnih aplikacijskih ter dekripcijskih napadov. Avtorja posebej izpostavljata nevarnost napadov z uporabo t. i. stranskih kanalov (angl. side-channel), ki ciljajo na pomanjkljivosti v implementaciji enkripcije. Pri takih napadih lahko napadalci pridobijo zaupne informacije na podlagi časovnih razlik v izvajanju kriptografskih operacij, ki so odvisne od pravilnosti ali nepravilnosti vnosa podatkov.

Butun idr. so možne napade na naprave IoT razdelili na 2 glavni kategoriji – pasivni in aktivni napadi – z dodatnimi podkategorijami [8]. Poudarili so, da je vsak napad, ki se ga ne da izslediti, kategoriziran kot pasivni napad. Ti napadi so usmerjeni predvsem v kršitev zaupnosti podatkov, npr. s prisluškovanjem. Nasprotno pa aktivni napadi ne posegajo le v zaupnost, temveč tudi v izrabo celovitosti podatkov. Takšne napade je mogoče izslediti, vendar napadalci kljub temu pogosto skušajo ostati čim manj opazni in prikriti svojo dejavnost.

Da naprave IoT niso edini možni vektor napada preko programskih in strojnih ranljivosti, so predstavili Alrawi idr., ki so poudarili, da zasnova IoT ni omejena le na fizično napravo, temveč vključuje tudi vse spremljevalne komponente, ki omogočajo njeno delovanje [9]. Skoraj vsaka naprava IoT ima namreč pripadajočo mobilno aplikacijo, ki je pogosto lahko ranljiva že sama po sebi. Ker naprave te aplikacije prepoznajo kot zaupanja vredne, lahko napadalci izkoristijo ranljivosti aplikacij za pridobitev dostopa do naprav. Te aplikacije pogosto trpijo za pomanjkljivostmi, kot so dovoljenja s prevelikimi privilegiji, napake v programski kodi ter trdo kodirani (angl. hard-coded) občutljivi podatki. Dodatno varnostno tveganje predstavljajo tudi oblačne storitve tretjih oseb, ki so lahko napačno konfigurirane ali pa same uporabljajo ranljive storitve, kar povzroča nevarnosti pri prenosu podatkov. Veliko naprav namreč še vedno uporablja zastarele protokole, kot je UPnP, in redko kriptirajo informacije v lokalnem omrežju, kar jih dela dovzetne za napade s posrednikom (MITM).

Za zaščito naprav IoT sta Bhunia in Gurusamy predstavila novo ogrodje, imenovano SoftTings, ki temelji na zasnovi programsko določenih omrežij (SDN) in omogoča preprečevanje 98% vseh napadov na naprave IoT [10]. Avtorja sta prikazala, kako je mogoče stikala s podporo za tehnologijo SDN uporabiti za dinamično dodeljevanje in upravljanje pravil na omrežju. Na najnižji ravni omrežja se nahajajo same naprave, katerih promet usmerja stikalo SDN in ga posreduje nadrejenemu krmilniku. Krmilnik se v začetni fazi "nauči" običajnega obnašanja naprav – spremlja npr. število poslanih zahtevkov, neuspešnih prijav, porabo pasovne širine in podobno. Na podlagi vedenjskega vzorca nato sproti posodablja pravila, zaznava odstopanja in v primeru anomalij promet blokira, omeji ali preusmeri v karanteno. Poleg profiliranja običajnega vedenja naprav mora krmilnik za učinkovito delovanje imeti tudi dostop do znanih varnostnih informacij, kot so primeri že znanih napadov (npr. DDoS, poplavljanje TCP), naslovi prepovedanih IP številk na t. i. črni listi (angl. black list) in podobno.

3 ZGODOVINSKI PREGLEDI VEČJIH NAPADOV

3.1 NAPADI NA PROGRAMSKO OPREMO - MIRAI BOTNET

Mirai botnet je eden izmed najbolj prepoznavnih napadov na naprave IoT [4]. Leta 2016 se je pojavila prva različica Mirai botneta, kadar sta ponudnik strežnikov OVH, ter ponudnik internetnih storitev Dyn zaradi obsežnih napadov nenadno prenehala delovati. Izkazalo se je, da je OVH utrpel napad z obsegom 1.17TB prenosa podatkov na sekundo, medtem ko je izpad storitve Dyn povzročilo nedelovanje več spletišč, kot so Twitter, Netflix, Reddit in Github. Mirai je sestavljen iz 4 delov - robota (angl. bot) oz. zlonamerne kode, nadzornega strežnika (angl. command and control (C&C) server), nalagalnika (angl. loader), ki prevaja stojno kodo za različne arhitekture procesorjev, ter strežnika za poročila (angl. report server), ki shranjuje podatke o napadih. Mirai se širi z iskanjem naključnih IP-naslovov na vratih TCP od 23 do 2323. Na odkritih napravah s slabimi varnostnimi nastavitvami poskuša pridobiti dostop z uporabo slovarja gesel in v primeru uspešnega vdora pridobi dostop do ukazne lupine (angl. shell). Nadzornemu strežniku nato sporoči podatke o sami napravi, na napravo z orodjem `wget` pa prenese in zažene zlonamerno programsko kodo. Okužena naprava lahko nato prejema ukaze nadzornega strežnika in tako napade druge strežnike.

3.2 NAPADI NA STROJNO OPREMO - STUXNET

Razvijalci naprav IoT ne razvijajo le programske kode, ki je lahko izpostavljena napadom, ampak tudi napravo, kot fizično entiteto. Relevantni so torej tudi napadi preko stranskih kanalov, kjer napadalci izkoriščajo ranljivosti izven programske opreme. Ti napadi lahko temeljijo na zaznavanju večjega magnetnega sevanja, porabe energije ali branju pomnilnika med delovanjem, kjer napadalci zajamejo pomnilnik ter z njega preberejo zaupne podatke. Poleg tega je lahko tudi ena izmed šibkih točk naprav nezaščiten dostop preko serijske povezave na matični plošči, preko katere lahko napadalci z napravo upravljajo. Prav tako je napade mogoče izvesti s spremembo zunanjega stanja, kot je npr. zunanja temperatura [11].

Znani napad na strojno opremo je bil Stuxnet leta 2010. Širil se je prek lokalnih omrežij in USB ključev ter povzročal fizično škodo na industrijskih sistemih. Njegova tarča so bile centrifuge iranske jedrske elektrarne, katerih hitrost vrtenja je povečal do te mere, da je prišlo do njihovega fizičnega uničenja. Napad je bil zelo prikrit, saj iz sistemskega nadzora ni bilo mogoče zaznati nobenih posebnosti [12].

3.3 NAPADI NA TEHNOLOGIJE VERIŽENJA BLOKOV - IOTA

Tehnologijo veriženja blokov (angl. blockchain tehcnology), prvotno razvito kot osnova za kriptovalute, so v preteklih letih začeli uporabljati tudi v različnih projektih IoT, kot sta DECENTER [13] ter BUILDCHAIN [14]. Njena uporaba omogoča številne prednosti, med katerimi izstopajo odprava enotnih točk odpovedi, izboljšana celovitost podatkov ter odpornost proti napadom DDoS [15], prinaša pa tudi določene izzive. Eden izmed njih je napad z 51-odstotnim nadzorom, pri katerem napadalci prevzamejo več kot polovico računske moči rudarjenja na verigi, kar jim ob uporabi tehnologije *proof-of-work* omogoča popoln nadzor nad verigo blokov. Poleg tega so za prenos podatkov uporabljene pametne pogodbe (angl. smart contracts), ki lahko vsebujejo varnostne ranljivosti v programski kodi. Te napake lahko privedejo do napačnega delovanja ali pa odprejo vrata zlonamernim napadom [16].

Zgovoren primer tovrstne ranljivosti se je zgodil leta 2020, ko je bila denarnica Trinity Wallet, ki jo je uporabljala platforma IOTA, tarča napada zaradi ranljivosti zunanje knjižnice, uporabljene v programski kodi pametne denarnice [17]. Napadalcem je uspelo pridobiti zasebne ključe uporabnikov in ukrasti kriptovaluto IOTA v

vrednosti 2 milijonov ameriških dolarjev. Ta dogodek je tako pokazal, kako lahko že najmanjše varnostne pomanjkljivosti v podpornih komponentah resno ogrozijo celoten sistem.

4 EKSPERIMENTALNA IZVEDBA NAPADOV

Za demonstracijske primere smo izbrali dve pametni napravi IoT - pametno žarnico tujega proizvajalca in pametni sistem za prezračevanje zraka. Napravi sta bili izbrani naključno, saj sta bili že na voljo, med analizo pa smo pri obeh zaznali različne možne oblike napadov. V okviru eksperimenta smo prikazali postopke napada z vidika napadalca. Predstavili smo obliko napada, katere pomanjkljivosti izkorišča, kakšen je njegov glavni namen in kako je videti iz omrežnega vidika. Nato smo opisali, kako napadalci zaznajo ranljivosti na ciljni napravi, katera orodja potrebujejo za izvedbo napada in kako poteka priprava na napad. Na koncu sledi še praktična predstavitev napada na izbrano napravo.

Napade smo izvedli v okolju, v katerem se pametni napravi najbolj uporabljata - to je navadno domače omrežje, v katerem se nahajajo vsakodnevne naprave uporabnikov s privzetimi varnostnimi nastavitvami usmerjevalnika, katere operaterji privzeto uporabnikom določijo. V to omrežje smo preko brezžične povezave povezali računalnik z operacijskim sistemom Linux, iz katerega smo nato naprej po omrežju prisluškovali, prestrezali in izvajali napade. Takšni napadi so bili ponovljeni večkrat, tudi tako, da smo naprave postavili na drugo omrežje, kjer smo simulacijo ponovno uspešno ponovili, tako da smo potrdili njihovo konsistentnost in prisotnost. Glavna omejitev eksperimentov je testiranje le dveh naprav IoT, katere so široko komercialno dostopne uporabnikom, vendar ne vključujejo širšega okolja drugih naprav IoT, predvsem naprav visoko zaupnih proizvajalcev.

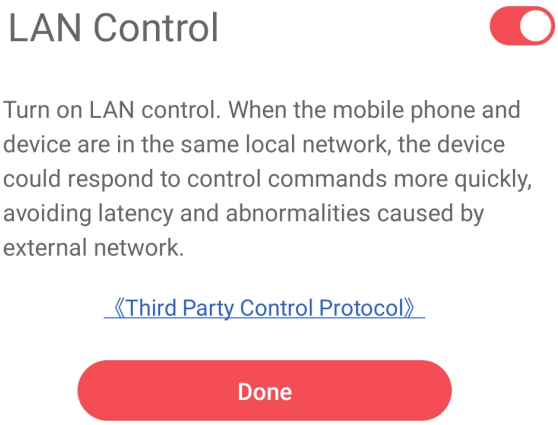
4.1 NAPAD ZARADI SLABE AVTENTIKACIJE

Napadi, ki izkoriščajo slabo avtentikacijo, so razmeroma enostavni za izvedbo. Zaradi odsotnosti avtentikacijskih mehanizmov ali slabe implementacije varnostnih praks lahko napadalci pridobijo neposreden dostop do naprave preko slabo zavarovanega vmesnika - bodisi z uporabo vmesnika API (Application Programming Interface), ki je namenjen pošiljanju strukturiranih, računalniško razumljivih ukazov (npr. v obliki JSON - JavaScript Object Notation) preko specifičnih vrat naprave, ali pa z uporabo spletnega vmesnika naprave. Ker vmesniki API pri takšnih napravah pogosto ne vključujejo mehanizmov za avtentikacijo, lahko napadalci napravi pošiljajo zahteve brez predhodne overitve. Prav tako pa so tudi nevarni spletni vmesniki naprav, saj velikokrat uporabljajo privzete oz. splošno znane prijavne podatke, kot so *admin, user, password, 123456* in podobne [18]. Zaradi teh šibkih nastavitev so naprave ranljive za napade s t. i. slovarji gesel (angl. password dictionaries), pri katerih napadalci s pomočjo računalnika ali druge naprave izvajajo avtomatizirano preverjanje velikega števila kombinacij uporabniških imen in gesel z namenom ugotavljanja uporabniških poverilnic.

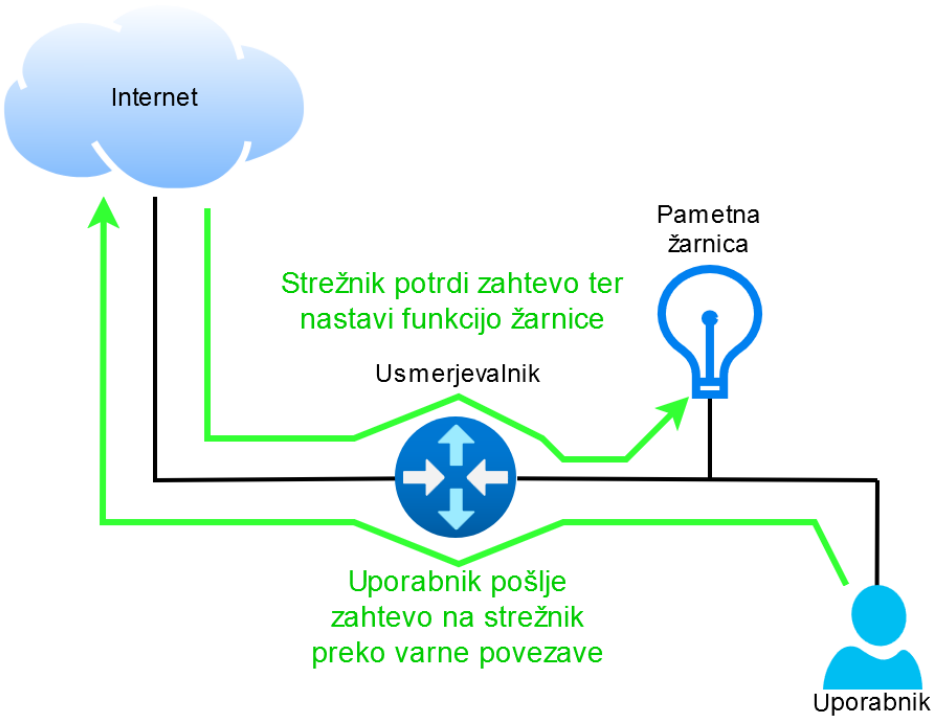
Za ponazoritev tega varnostnega problema smo uporabili pametno žarnico. Ob prvemu povezovanju žarnice z lokalnim omrežjem aplikacija ponudi možnost vklopa t. i. lokalnega (LAN) nadzora, kot je prikazano na Sliki 1.

Brez uporabe te možnosti nadzor nad pametno žarnico lahko poteka le tako, da uporabniki z uporabo pametne naprave pošljejo zahtevo na oddaljen strežnik, le ta pa nazaj odgovori, ter ukaz pošlje na pametno žarnico. Celoten proces uporablja varovan protokol TLS, kjer je komunikaciji v celoti zavarovana pred napadalci proti napadom, kot sta ponavljanje ali prisluškovanje. Potek komunikacije je razviden na Sliki 2.

Ta možnost je zelo zavajajoča – uporabnikom namreč sporoča, da bo z vklopom te možnosti naprava hitreje odzivna na lokalnem omrežju. Poleg tega je ta možnost že privzeto vključena. Besede 'naprava', 'hitreje' in 'izogibanje zakasnitvam' uporabnike prepričajo, da gre za funkcijo, ki izboljša uporabniško izkušnjo, in jo zato pustijo vključeno. Opozorilo o potencialnih varnostnih tveganjih oziroma dejanski razlagi funkcionalnosti 'LAN nadzora' je na voljo šele s klikom na diskretno označeno modro besedilo 'Third Party Control Protocol' (nadzorni protokol tretje osebe). Glede na statistične podatke, da kar 91 % uporabnikov pogojev uporabe ne prebere [19], lahko sklepamo, da večina uporabnikov tudi tokrat ne bo prebrala teh informacij. Obenem smo z uporabo orodja Wireshark ugotovili, da pametna žarnica kljub vklopljeni možnosti LAN nadzora in povezavi mobilne naprave z istim omrežjem, ukaze še vedno pošilja na zunanji strežnik. V primeru izpada internetne povezave – ob sicer delujočem lokalnem omrežju – pametna žarnica ne deluje, kar pomeni, da je funkcionalnost 'LAN nadzora', ki je privzeto vklopljena in predstavlja veliko varnostno luknjo, zavajajoča in se je pri naši analizi izkazala za popolnoma lažno.



Slika 1: Vklop možnosti LAN nadzora



Slika 2: Potek nadzora pametne žarnice

Ta funkcionalnost v resnici omogoča dostop do naprave preko lokalnega omrežja na vratih 55443. Pri analizi uporabe na teh vratih nismo zaznali nobenega omrežnega prometa, kar pojasnjuje, zakaj žarnica brez internetne povezave ne deluje. Napadalci lahko to privzeto nastavitev zlorabijo s pomočjo javno dostopne dokumentacije [20].

Z uporabo različnih orodij lahko napadalci identificirajo IP-naslov pametne žarnice, nato pa z uporabo programa, kot je *telnet*, pošiljajo ukaze neposredno napravi v strukturirani obliki, kot je navedena v proizvajalčevi dokumentaciji [20]. Za vzpostavitev povezave mora napadalec v ukazu telnet navesti IP-naslov naprave (v našem primeru 192.168.1.64) ter vrata (55443). Z zagonom ukaza `telnet 192.168.1.64 55443` se vzpostavi povezava z napravo, napadalec pa lahko prične s pošiljanjem ukazov. Iz dokumentacije je razvidno, da je za izklop luči uporabljen ukaz, predstavljen na Sliki 3:

```
{"id":1,"method":"set_power","params":["off", "smooth", 5]}
```

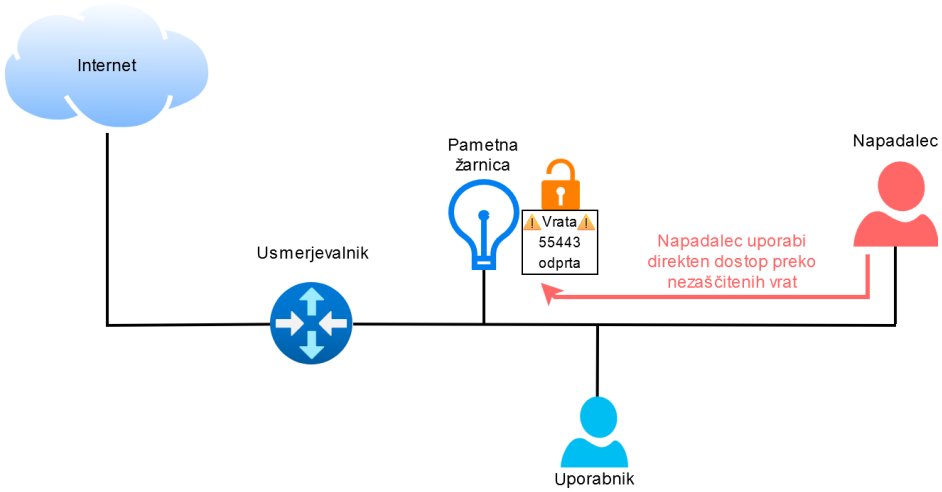
Slika 3: Ukaz za izklop luči z uporabo nadzora LAN

Ukaz vsebuje več polj, ki nadzirajo funkcionalnost pametne žarnice:

- Polje 'id' je identifikator, ki ga bi ga lahko uporabili za enolično identificiranje naprave, če bi razvijali aplikacijo za nadzor več luči. To nam omogoča enostavnejši nadzor nad več napravami, zato je v našem primeru vrednost tega polja lahko poljubna.
- Polje 'method' vsebuje ime metode, ki bo uporabljena. Ker želimo spremeniti stanje luči (vklop/izklop), bomo uporabili metodo 'set_power'
- Polje 'param' sprejme število podatkov, odvisno od zahtevane metode. Ukaz 'set_power' sprejme 3 parametre (opcijsko 4): Prvi parameter določa stanje luči. Za vklop je treba nastaviti vrednost 'on', za izklop pa 'off'. Drugi parameter določa način spremembe stanja. Možnosti sta 'sudden', kjer se sprememba zgodi takoj, in 'smooth', kjer sprememba poteka postopoma v času, določenem v tretjem parametru. Tretji parameter določa čas v milisekundah, ki je potreben za enakomerno spreminjanje vrednosti, če je izbran način spremembe 'smooth'. Čeprav je relevanten zgolj pri slednjem, mora biti čas definiran tudi v načinu 'sudden'.

Za vklop luči moramo parameter 'off' zamenjati z 'on', če želimo spremeniti svetilnost luči na 50 %, pa uporabimo metodo 'set_bright' in namesto parametra 'on' oziroma 'off' podamo numerično vrednost svetilnosti v odstotkih - v tem primeru 50.

Zaradi slabe informiranosti uporabnikov s strani proizvajalca lahko tako napadalci pridobijo popoln nadzor nad pametno žarnico in z njo upravljajo brez dovoljenja uporabnika, kot je prikazano na Sliki 4.

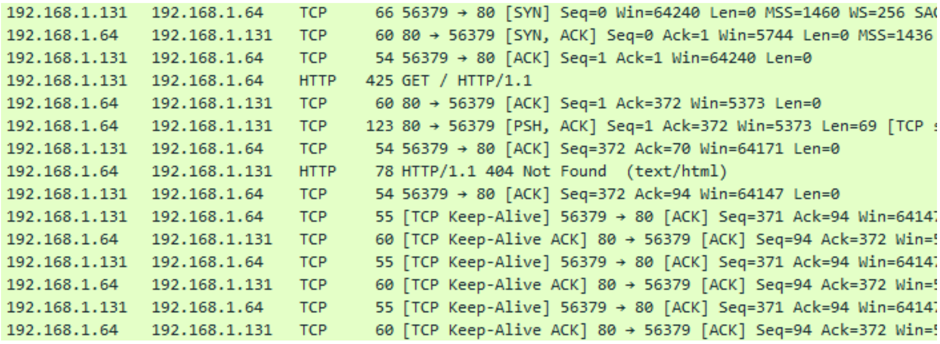


Slika 4: Potek napada preko vrat 55443

4.2 NAPAD DOS

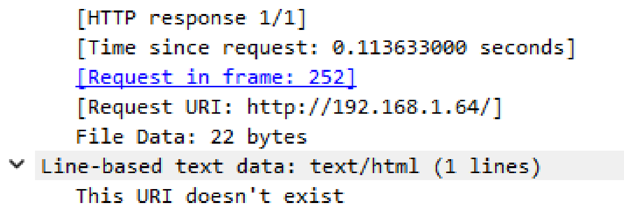
S poplavljanjem naprave z zahtevki napadalci dosežejo, da naprava postane neodzivna ali nedosegljiva za običajne uporabnike. Temu pravimo napad DoS (Denial of Service). Tako kot je več pametnih naprav skupaj dovolj zmogljivih, da z napadom DDoS (distribuiran DoS, ki poteka iz več naprav) ohromijo druge naprave ali strežnike, pa so lahko tudi same žrtev enakega napada ali preprostejšega napada DoS, ki se izvaja iz ene same naprave. Ker imajo pametne naprave omejene računske zmogljivosti, jih je lažje ohromiti že z enostavnim napadom DoS, nasprotno pa je za uspešen napad na zmogljivejše naprave in strežnike potreben večji sistem, ki ga zagotavlja DDoS.

V našem primeru smo analizirali pametno žarnico, ki je ranljiva za napad DoS, zaradi delujoče storitve **HTTP** na vratih **80**. Ko v spletni brskalnik vpišemo njen IP-naslov, naprava odgovori s sporočilom 'This URI does not exsist', z uporabo orodja Wireshark pa lahko preverimo komunikacijo med računalnikom, ki je poslal zahtevo, in pametno žarnico.



Slika 5: Komunikacija pametne žarnice z orodjem Wireshark

Z analizo prometa, prikazano na Sliki 5, smo potrdili, da naprava uporablja navaden protokol HTTP. Računalnik pošlje zahtevo tipa GET, pametna žarnica pa nanjo odgovori s prej omenjemin sporočilom. Odgovor je prikazan na Sliki 6.



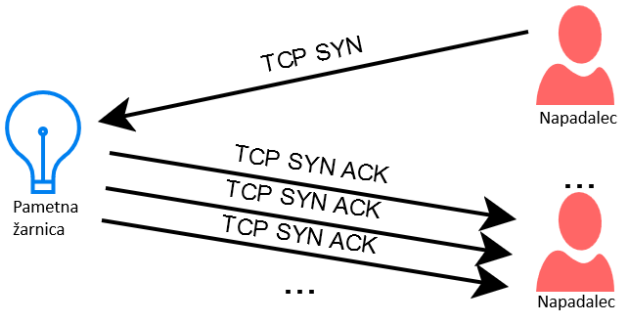
Slika 6: Odgovor pametne žarnice na HTTP zahtevo

Kljub temu da je odgovor velik le 22 bajtov, lahko za izvedbo napada DoS izkoristimo že samo delovanje protokola HTTP, saj temelji na protokolu TCP na transportni plasti. TCP ima sicer številne prednosti, kot so preprečevanje izgub, podvajanja, napačnega vrstnega reda in napak paketov, vendar ima tudi slabost, saj mora ob vsaki vzpostavitvi povezave opraviti t. i. trojno rokovanje. Na strani strežnika (v našem primeru pametne žarnice) to predstavlja nezanemarljivo obremenitev virov. Napadalci lahko to šibkost izkoristijo v napadu TCP SYN s poplavljanjem tako, da na žarnico pošljejo veliko TCP SYN (sinhroniziraj, angl. synhronize) zahtev. Zaradi množice teh zahtev je vsa računska moč žarnice porabljena za TCP ACK (potrdi, angl. acknowledge) odgovore, kot prikazuje Slika 7. Žarnica je s tem preobremenjena in zato ne bo uspela obdelati ukazov, ki jih bodo poslali legitimni uporabniki preko aplikacije.

Za izvedbo napada DoS uporabimo orodje *hping3* za pošiljanje paketov na izbrani naslov in na ta način preobremenimo pametno žarnico do točke, ko postane neodzivna na uporabnikove zahteve.

Kot je razvidno s Slike 8, ukaz *hping3* vsebuje več dodatnih parametrov:

- Parameter **-c** (vrednost **10000**) določa število poslanih paketov pred zaustavitvijo programa.
- Parameter **-d** (vrednost **150**) določa velikost podatkovnega dela vsakega paketa v bajtih.



Slika 7: Potek napada DoS

```
hping3 -c 10000 -d 150 -S -w 64 -p 80 --flood --rand-source 192.168.1.64
```

Slika 8: Zagon programa hping3 z ustreznimi parametri

- Parameter **-S** je uporabljen za pošiljanje paketov **TCP SYN**.
- Parameter **-w** (vrednost **64**) določa velikost okna TCP, ki pove, koliko podatkov je lahko prenesenih, pred prejemom potrdila s strežnika (TCP ACK).
- Parameter **-p** (vrednost **80**) predstavlja vrata, na katerih teče strežnik. V našem primeru uporabimo 80, ki so privzeta za protokol HTTP.
- Parameter **–flood** omogoča način 'poplavljanja', kjer pošiljamo pakete čim hitreje, kar je ključnega pomena za napad DoS.
- Parameter **–rand-source** doda naključno generiranje izvornih IP-naslovov, ki lahko oteži zaznavanje napada in morebitno filtriranje s strani ciljne naprave.
- Na koncu je naveden še **IP-naslov** ciljne naprave (v tem primeru **192.168.1.64**).

Kot je razvidno iz izpisa orodja Wireshark (Slika 9), je zabeležen velik obseg prometa iz naključno generiranih IP-naslovov, ki je usmerjen proti pametni žarnici. Gre za izvedbo napada DoS. Zaradi velike količin zahtev je žarnica preobremenjena z obdelavo dohodnega prometa in se posledično ne odziva več na uporabnikove zahteve v aplikaciji (Slika 10).

Ko se izvajanje programa zaključi, se promet na omrežju zmanjša in posledično pametna žarnica po krajšem času ponovno postane odzivna na uporabnikove ukaze.

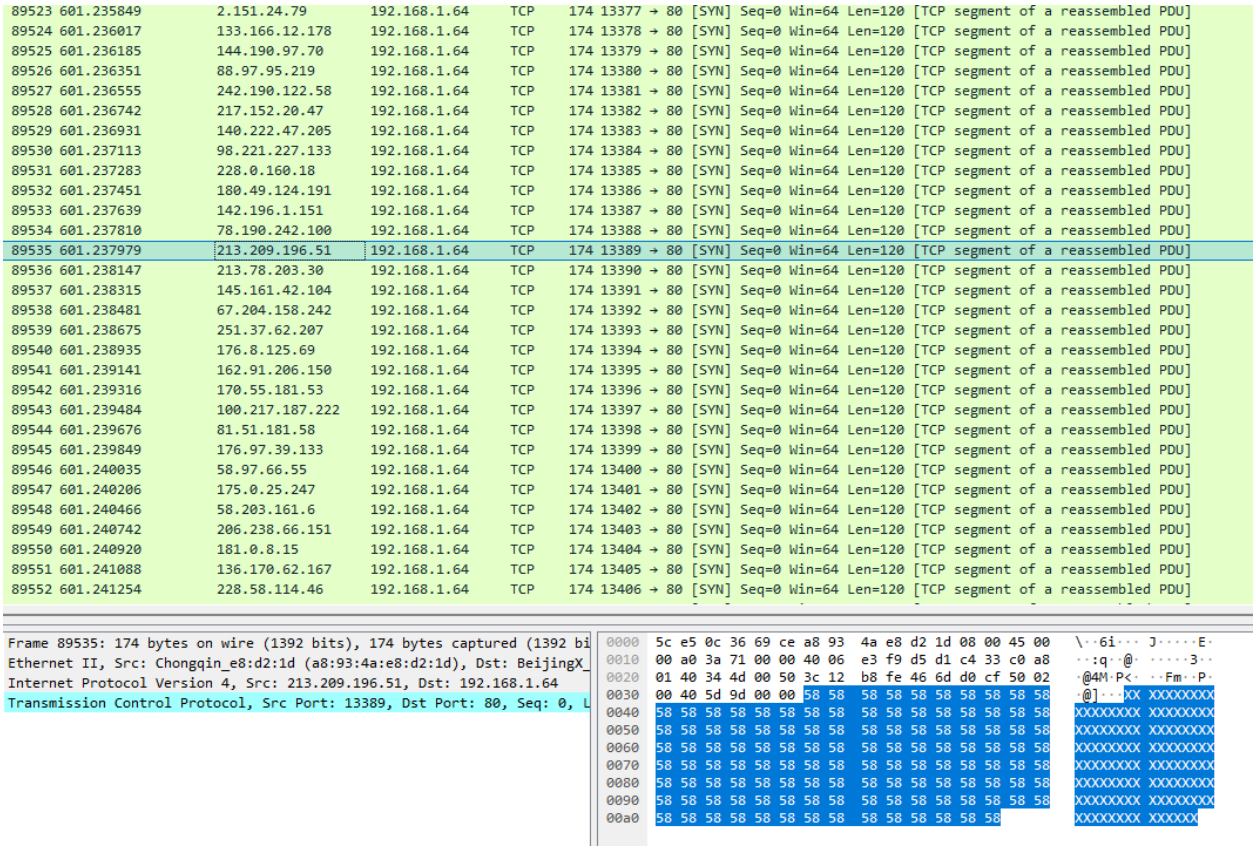
4.3 NAPAD S PONAVLJANJEM

Napad s ponavljanjem je pri napravah IoT zelo pogost – kar 75 % naprav IoT je ranljivih na tovrstne napade [21]. Napadalec v takem primeru prestreže, zajame, ali kako drugače pridobi pakete, ki bi sicer potovali od uporabnikove naprave (npr. mobilni telefoni ali nadzorna plošča) do pametnih naprav IoT. Včasih so vmes tudi strežniki, vendar so takrat napadi težje izvedljivi, saj večina internetnega prometa – kar 97,6 % – poteka prek protokola SSL/TLS [22], ki onemogoča ponovno uporabo zajetih paketov.

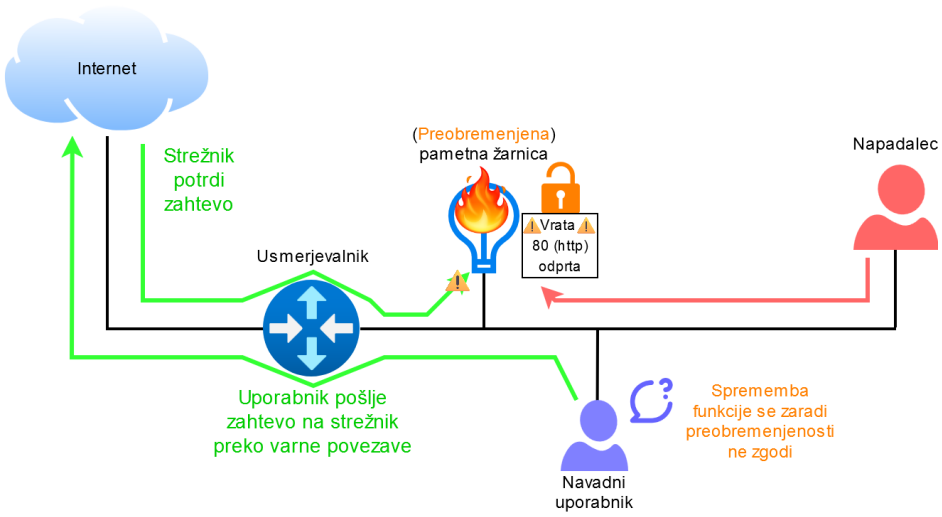
Za tarčo v naši reprodukciji napada smo izbrali pametno napravo za prezračevanje zraka, ki ima lastno aplikacijo za pametne telefone. Za razliko od pametne žarnice ta naprava komunicira le v lokalnem omrežju in zahtev ne pošilja na strežnik. Zaradi tega je napad s ponavljanjem bistveno lažje izvedljiv, saj podatki ob prenosu zelo verjetno niso šifrirani. Slednje je potrdil tudi naš eksperiment.

Ko smo iz mobilne naprave poslali ukaz (Slika 11), smo z orodjem Wireshark v omrežnem prometu opazili tri enake zaporedne pakete UDP, poslane z naslova pametne prezračevalne naprave na oddajni (angl. broadcast) naslov omrežja (Slika 12). Napravo je mogoče enostavno prepoznati že s prisluškovanjem, saj približno vsako sekundo pošlje enak paket UDP na oddajni naslov (Slika 13.

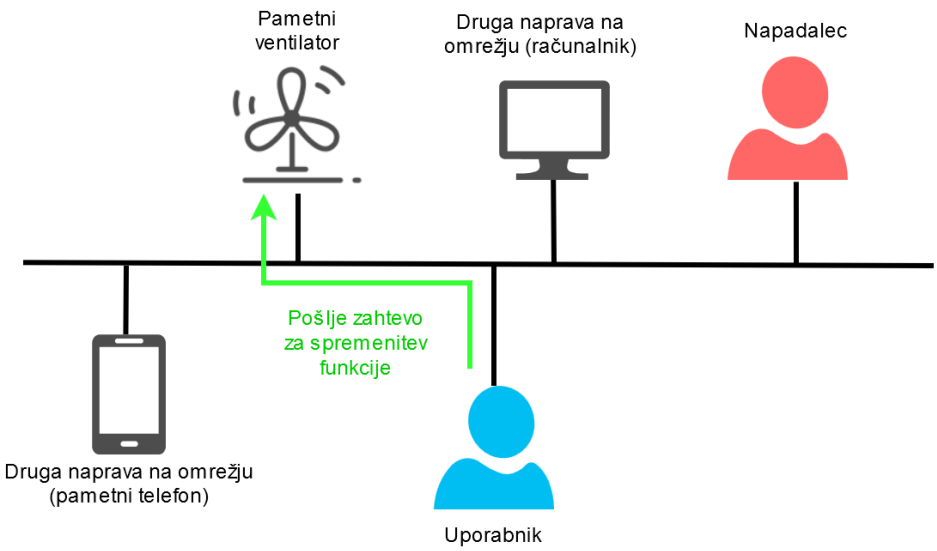
Iz vsebine paketov je bilo razvidno, da potujejo iz smeri pametne naprave na oddajni naslov omrežja. Poleg tega niso imeli nobenega mehanizma za prikrivanje, preverjanje integritete ali preverjanje enoličnosti.



Slika 9: Pregled prometa pri napadu DoS



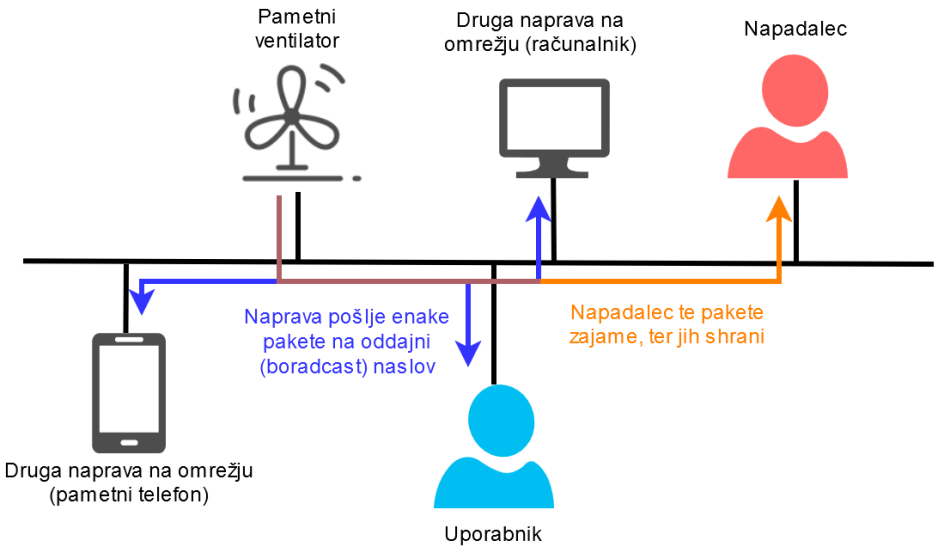
Slika 10: Vizualni prikaz omrežja pri napadu DoS



Slika 11: Pošiljanje ukaza pametni napravi

```
2 1.025… 192.168.0.236  192.168.0.255  UDP    92 1028 → 1028 Len=50
3 1.029… 192.168.0.236  192.168.0.255  UDP    92 1028 → 1028 Len=50
4 1.034… 192.168.0.236  192.168.0.255  UDP    92 1028 → 1028 Len=50
```

Slika 12: Trije zaporedni paketi UDP prezračevalne naprave



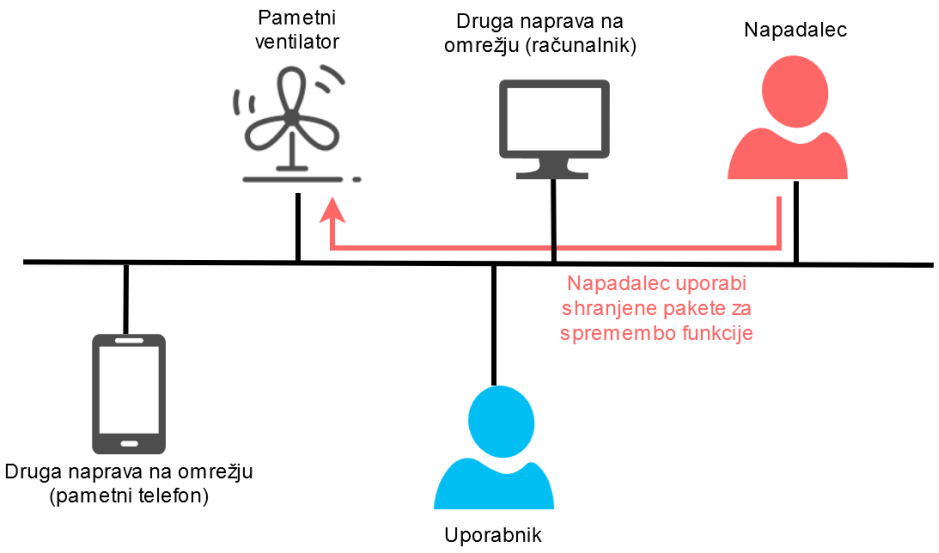
Slika 13: Prezračevalna naprava pošlje pakete na oddajni naslov

Z uporabo orodja Wireshark smo pakete shranili in izvozili, s pomočjo orodja *tcpreplay* pa smo jih nato ponovno poslali po omrežju in tako uspešno izvedli napad s ponavljanjem.

```
tcpreplay --intf1=enp0s3 speed_fast.pcapn
```

Slika 14: Ponovno pošiljanje paketov s tcpreplay

V ukazu na Sliki 14 smo parametru `--intf1` podali ime mrežnega vmesnika (enp0s3), s katerega smo želeli poslati pakete, ter ime datoteke (speed_fast.papn), ki smo jo izvozili z orodjem Wireshark. Komunikacija na nivoju omrežja je predstavljena na Sliki 15



Slika 15: Napadalec uporabi zajete pakete za spremembo funkcije

Po uspešni izvedbi ukaza nas program obvesti o poslanih paketih. Ker so bili ti paketi zajeti ob pošiljanju ukaza za hitrejše delovanje z mobilne naprave, se ob njihovi ponovni uporabi funkcija zopet aktivira.

5 OBRAMBA PRED NAPADI

Obrambo pred opisanimi napadi lahko deloma izvajajo uporabniki sami, v večini primerov pa gre za programske ranljivosti, ki jih morajo nasloviti proizvajalci. To odpira glavno vprašanje, ali je nujno, da je vsaka naprava pametna. Tudi če so uporabniki seznanjeni s tveganji, so zaradi napak ali malomarnosti proizvajalcev pogosto izpostavljeni ranljivostim, pred katerimi se ne morejo učinkovito zaščititi.

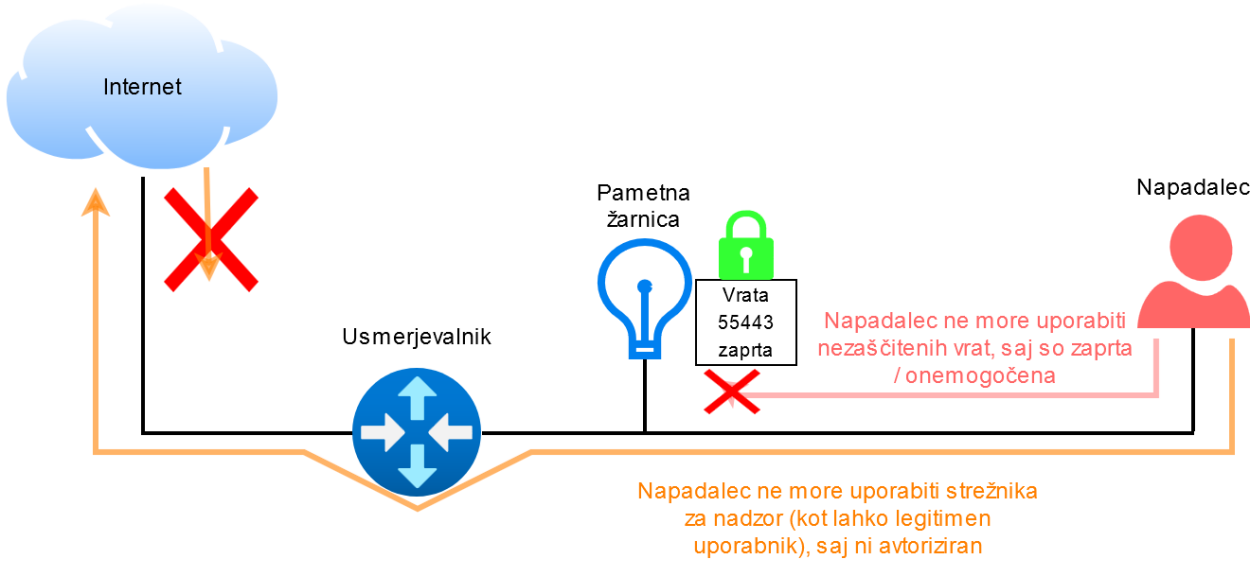
5.1 PREPREČEVANJE NAPADA ZARADI SLABE AVTENTIKACIJE

V splošnem je preprečevanje takšnih napadov dokaj enostavno. Uporabniki morajo spremeniti privzeto geslo in upoštevati dobre prakse ustvarjanja močnih gesel.

Toda v obravnavanem primeru napad izhaja iz pomanjkanja implementacije osnovne avtentikacije iz strani proizvajalca nasploh. Takšne dobre prakse tako niso dovolj, če proizvajalec njihovo pomembnost zanemari. V tem primeru to predstavlja, da uporabniki pustijo omogočeno privzeto možnost lokalnega nadzora, kar odpre varnostno luknjo. Odgovornost proizvajalcev je, da uporabnike o nevarnosti ustrezno opozorijo.

Z zaprtjem vrat 55433 napadalci izgubijo možnost nedovoljenega dostopa do upravljanja pametne žarnice, saj je po tem edini način spreminjanja nastavitev žarnice mogoč le preko uradnega strežnika. Ta povezava je povsem varna in zaščitena, za legitimno uporabo pa je potrebna ustrezna avtorizacija (Slika 16).

Kot proizvajalci naprav lahko takšne napade preprečimo z boljšim informiranjem uporabnikov o delovanju omenjene funkcije lokalnega nadzora. Še učinkovitejša rešitev je uvedba avtentikacije ob pošiljanju podatkov.



Slika 16: Napadalec nima več dostopa do upravljanja

Ker je ob prvi nastavitvi pametne žarnice v vsakem primeru potrebno ustvariti oz. se prijaviti v uporabniški račun, bi lahko ta proces, ki poteka preko strežnika z zaščitenim protokolom TLS 1.2, uporabili tudi za izmenjavo javnega in zasebnega ključa. Ta ključ bi se nato uporabljal za zaščito komunikacije znotraj lokalnega omrežja, s čimer bi bili podatki prikriti. Hkrati bi bila sama izmenjava ključev varno izvedena preko zaščitenega protokola.

5.2 PREPREČITEV NAPADA DOS

Tudi pred napadi DoS se končni uporabniki težko zavarujejo, saj preprečevanje zahteva programsko implementacijo s strani proizvajalcev.

Uporabniki lahko napravo zgolj umestijo v ločen, zaščiten segment omrežja (VLAN), kjer je omejen dostop do vrat 80. Vhodni in izhodni paketi so tako nastavljeni na zavrnitev, kot je prikazano na Sliki 17. Analiza z orodjem Wireshark potrjuje, da se vrata 80 oziroma protokol HTTP sploh ne uporabljajo.

Proizvajalci lahko težavo odpravijo tako, da vrata 80 oziroma spletno stran, ki ni uporabi, preprosto zaprejo. Če je uporaba teh še vedno potrebna, pa morajo vzpostaviti ustrezne mehanizme za preprečevanje DoS napadov. Ker večina povezav, razen lokalnega nadzora na vratih 55443 z uporabo ključev, poteka prek zunanjega strežnika, lahko proizvajalci uporabijo zaščito DDoS, kot je Cloudfare.

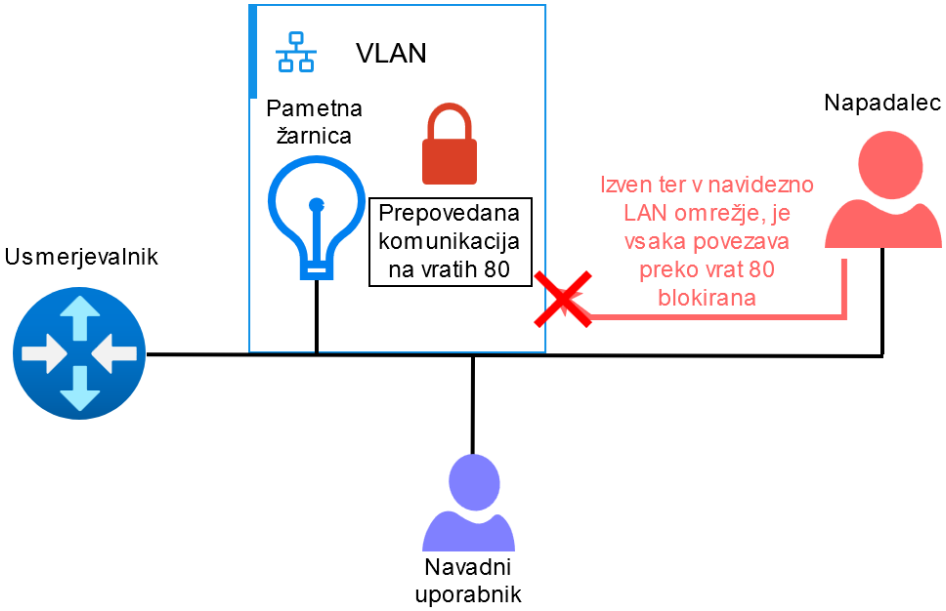
5.3 PREPREČITEV NAPADA S PONAVLJANJEM

Napad je mogoče najenostavneje preprečiti z dobro programsko kodo, za kar so odgovorni proizvajalci. S strani uporabnikov je preprečevanje takšnih napadov bistveno težje, saj je izogibanje napadom skoraj nemogoče, če so napadalci že znotraj lokalnega omrežja in komunikacija poteka brez kakršnekoli zaščite.

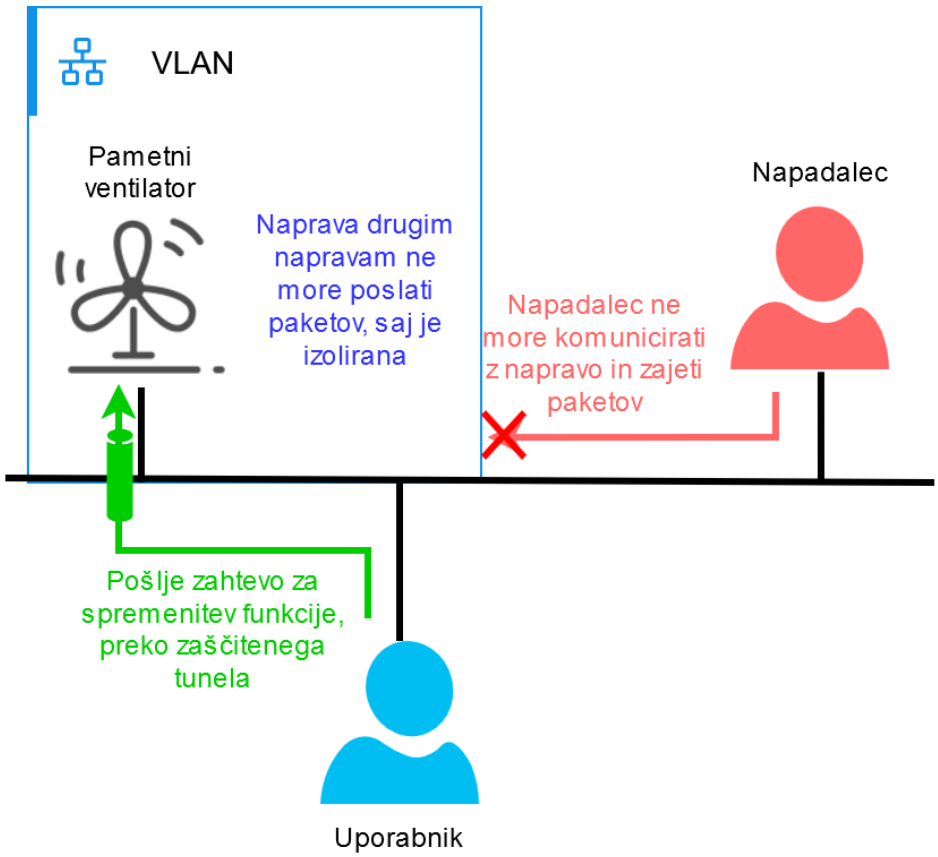
Največ, kar lahko naredi uporabnik, je vzpostavitev ločenega zaščitenega omrežja VLAN, v katerega so povezane ranljive naprave. Za komunikacijo med mobilno napravo za nadzor funkcij in samo napravo IoT na omrežju VLAN moramo postaviti tudi zaščitni tunel, preko katerega se pošiljajo prekriti paketi, kar preprečuje prisluškovanje napadalcev, kot je prikazano na Sliki 18.

Pomembno je, da uporabimo najnovejše protokole za varovanje brezžičnega omrežja, kot sta WPA3 ali WPA2. V nasprotnem primeru je omrežje lahko popolnoma odprto in potencialnim napadalcem omogoča dostop do enostavno ponovljivih paketov, saj protokol UDP sam po sebi ne zagotavlja zaščite.

Implementacija ustrezne zaščite je torej nujna in mogoča predvsem na strani proizvajalcev že ob razvoju programske opreme. Eden od učinkovitih pristopov je uporaba enkratnih vrednosti (angl. nonce) za



Slika 17: Napadalec nima več dostopa do vrat 80



Slika 18: Napadalec ne more prisluškovati paketom

označevanje posameznih paketov. Ta preprečuje ponovno uporabo že poslanih paketov, saj bi bili neveljavni paketi zavrnjeni. Podobno pristop uporablja protokol TCP z zaščito proti ponavljanju.

Ker v našem primeru zaščita samih podatkov ni bistvena, šifriranje podatkov ni nujno, zato lahko še vedno uporabljamo protokol UDP. Na primer, dejstva, da smo spremenili moč naprave na najvišjo vrednost nam ni treba prikrivati, saj to sporočilo ne vsebuje zaupnih ali osebnih podatkov. V primerih, kjer pa bi bilo potrebno prikriti poslane podatke, bi pa bil potreben drugačen, varnostno okrepljen pristop.

6 DISKUSIJA

Naprave IoT izpostavljajo ključno vprašanje, kako zagotoviti varnost naprav, ki so vse bolj prisotne v vsakdanjem življenju, a zaradi neinformiranosti uporabnikov pogosto zapostavljene, kar nato privede do varnostnih incidentov. Čeprav je ozaveščenost uporabnikov ključnega pomena za varovanje lastnih naprav z zgoraj opisanimi metodami (uporaba močnih gesel, preverjanje stanja naprav, redne posodobitve), osrednja odgovornost za varnost še vedno leži na proizvajalcih pametnih naprav.

Dandanes lahko katerokoli podjetje, tudi nekvalificirano, začne proizvajati pametne naprave. To vodi v preplavljen trg, na katerem se pogosto znajdejo izdelki z varnostnimi pomanjkljivostmi in brez ustrezne regulacije. Medtem ko v Evropski uniji za naprave veljajo strogi varnostni standardi, so ti na nekaterih drugih trgih pogosto spregledani ali neobstoječi. Potrošniki, ki stremijo k znižanju stroškov, se zato pogosto odločajo za cenejše izdelke s tujih trgov, kar pa povečuje tveganje za uporabo nevarnih naprav.

Zaradi pomanjkanja nadzora proizvajalci pogosto tudi zanemarijo testiranje varnosti programske opreme naprav, posledice te odločitve pa nosijo končni uporabniki, ki morajo za varnost poskrbeti sami.

Optimalna rešitev za opisano težavo bi bila uvedba strožjih zakonodaj in regulacij, ki bi veljale tudi za uvoz naprav IoT s tujih trgov. Te bi morale določati minimalne varnostne zahteve za programsko kodo, kot je obvezna enkripcija podatkov med komunikacijo, ter jasno opredeljevati odgovornost proizvajalcev za posledice varnostnih pomanjkljivosti.

Zaradi obsežnosti globalnih trgov je uveljavitev takšnih ukrepov na globalni ravni izjemno zahtevna, zato za končne uporabnike še vedno predstavlja najboljšo prakso nakup naprav priznanih kvalificiranih proizvajalcev z dokazanimi varnostnimi standardi.

7 ZAKLJUČEK

Pomembnost rednega posodabljanja naprav in kakovostno zasnovane programske kode je pri napravah IoT, ki so povezane na splet, ključna. Že najmanjša napaka v kodi lahko privede do velikih varnostnih ranljivosti, ki omogočajo izvajanje napadov – od zbiranja podatkov do onemogočanja naprave ter zlorabe računske moči naprave.

V članku smo obravnavali tri ključne napade na programsko opremo.

Napadi zaradi slabe avtentikacije so pogosto posledica šibkih gesel ali celo popolne odsotnosti avtentikacije. Napadalcem omogočijo popoln dostop do naprave brez iskanja drugih ranljivosti in so enostavni za izvedbo. Za preprečevanje je nujno upoštevanje dobrih varnostnih praks ustvarjanja uporabniških računov.

Napadi DoS ohromijo delovanje pametnih sistemov. Preprečevanje tovrstnih napadov mora biti vključeno že v zasnovo programske opreme, saj lahko uporabniki sami zgolj izolirajo napravo v ločeno omrežje (VLAN). S tem tako preprečijo omrežno komunikacijo med takšno ranljivo napravo in ostalimi napravami v omrežju, ter preprečijo izvedbo napada DoS.

Napadi s ponavljanjem omogočajo ponovno uporabo poslanih podatkov, ki so bili zajeti med prenosom. Proizvajalci naprav jih lahko preprečijo z uporabo varnostnih mehanizmov, kot sta uporaba enkratnih vrednosti v paketu, in/ali šifriranje podatkov v paketu. Uporabniki se lahko zavarujejo zgolj z vzpostavitvijo izoliranega omrežja in uporabo t. i. tunelskega načina za prenos šifriranih podatkov.

Poleg omenjenih napadov obstajajo tudi drugi varnostni izzivi, ki so povezani z veliko rastjo popularnosti naprav IoT.

Uporaba umetne inteligence za varnost v napravah IoT

Z vse bolj razširjeno uporabo umetne inteligence v varnostnih sistemih nastajajo tudi nova orodja za zaznavanje in preprečevanje vdorov v pametne naprave. Napredni modeli so zmožni obdelati velike količine podatkov in z uporabo nevronskih mrež enostavneje prepoznajo vzorce, ki lahko opozorijo na oz. preprečijo napade [23].

Raziskava [24] predlaga nov sistem za zaznavanje vdorov (angl. Intrusion Detection System - IDS) v naprave IoT z uporabo integriranih konvolucijskih nevronskih mrež (CNN) in mrež z dolgotrajnim spominom (LSTM), ki z 99,52 % natančnostjo zaznajo zlonameren promet. Razvijajo se tudi prilagojene limanice (angl. honeypots), [25] ki z uporabo strojnega učenja omogočajo avtomatizirano interakcijo z napadalci. Ker je razvoj posebnih limanic za vsako napravo IoT neizvedljiv, uporabimo takšne metode, da nato napadalci porabijo več časa na prilagojenih limanicah, kot bi sicer na klasičnih. Hkrati pa je potrebno pomniti, da zaradi izjemne rasti uporabe naprav IoT in vedno večje integracije z našim vsakdanjim življenjem dosedanji protinapadi postajajo prešibki. Za učinkovito obrambo se bo tako potrebno tudi poslužiti naprednih pristopov, kot so strojno in globoko učenje[26].

Prihodnje raziskave se bi lahko osredotočale v smeri uporabe umetne inteligence in strojnega učenja v domačih okoljih za varovanje vsakodnevnih naprav IoT uporabnikov. Z razširitvijo domačega usmerjevalnika, kateremu bi bila dodana omenjena funkcionalnost, bi lahko izboljšali varnost celotnega obstoječega omrežja, saj se bi ta učila na podlagi delovanja omrežja, ter bi takoj ukrepala ob zaznavi nenormalnih anomalij.

Nevarnost predstavljajo tudi **napadi na osebne podatke**, saj naprave IoT zbirajo velike količine zaupnih osebnih podatkov. Ob pomanjkljivi zaščiti lahko to vodi do kršitev zasebnosti in zlorab, vključno s krajo ali preprodajo podatkov na črnem trgu [27].

LITERATURA

[1] Gregory Kipper. “Chapter 6 - Visions of the Future”. V: *Augmented Reality*. Ur. Gregory Kipper. Boston: Syngress, 2013, str. 129–142. ISBN: 978-1-59749-733-6. DOI: 10.1016/B978-1-59-749733-6.00006-1.

[2] Martin McMaker. *Smart, self-watering plant pot planter ‘Flaura’*. https://www.thingiverse.com/thing:4921885. [Online]. Dostopano: 26. november 2024. 2021.

[3] Geir M Køien. “Aspects of security update handling for IoT-devices”. V: *Int. J. Adv. Security* 10.1 (2017).

[4] Constantinos Kolias in sod. “DDoS in the IoT: Mirai and Other Botnets”. V: *Computer* 50.7 (2017), str. 80–84. DOI: 10.1109/MC.2017.201.

[5] Taimur Bakhshi, Bogdan Ghita in Ievgeniia Kuzminykh. “A Review of IoT Firmware Vulnerabilities and Auditing Techniques”. V: *Sensors* 24.2 (2024). ISSN: 1424-8220. DOI: 10.3390/s24020708.

[6] Saman Taghavi Zargar, James Joshi in David Tipper. “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”. V: *IEEE Communications Surveys & Tutorials* 15.4 (2013), str. 2046–2069. DOI: 10.1109/SURV.2013.031413.00127.

[7] Jyoti Deogirikar in Amarsinh Vidhate. “Security attacks in IoT: A survey”. V: *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. 2017, str. 32–37. DOI: 10.1109/I-SMAC.2017.8058363.

[8] Ismail Butun, Patrik Österberg in Houbing Song. “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures”. V: *IEEE Communications Surveys & Tutorials* 22.1 (jan. 2020), str. 616–644. DOI: 10.1109/COMST.2019.2953364.

[9] Omar Alrawi in sod. “SoK: Security Evaluation of Home-Based IoT Deployments”. V: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, maj 2019, str. 1362–1380. DOI: 10.1109/SP.2019.00013.

[10] Suman Sankar Bhunia in Mohan Gurusamy. “Dynamic attack detection and mitigation in IoT using SDN”. V: *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, nov. 2017, str. 1–6. DOI: 10.1109/ATNAC.2017.8215418.

[11] Ioan Tudosa in sod. “Hardware Security in IoT era: the Role of Measurements and Instrumentation”. V: *2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)*. 2019, str. 285–290. DOI: 10.1109/METROI4.2019.8792895.

[12] Marie Baezner in Patrice Robin. *Stuxnet*. Teh. poročilo 4. Center for Security Studies (CSS), ETH Zürich, okt. 2017. DOI: 10.3929/ethz-b-000200661.

[13] Petar Kochovski in sod. “An Architecture and Stochastic Method for Database Container Placement in the Edge-Fog-Cloud Continuum”. V: *Proceedings of the 33rd IEEE International Parallel & Distributed Processing Symposium (IPDPS 2019)*. IEEE, 2019, str. 396–405. DOI: 10.1109/IPDPS.2019.00050.

[14] Pouriya Miri in Vlado Stankovski. “Blockchain-powered IoT for Smarter Infrastructure: Structural Health Monitoring Use-case”. V: *Proceedings of the 2024 IEEE International Conference on Computer Communication and the Internet (ICCCI)*. IEEE, 2024, str. 145–149. DOI: 10.1109/ICCCI62159.2024.10674173.

[15] Zawar Shah in sod. “Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey”. V: *Sensors* 22.3 (2022), str. 1094. DOI: 10.3390/s22031094.

[16] Sandeep Singh, A. S. M. Sanwar Hosen in Byung-Gon Yoon. “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network”. V: *IEEE Access* 9 (2021), str. 13938–13959. DOI: 10.1109/ACCESS.2021.3051602.

[17] IOTA Foundation. *Trinity Attack Incident Part 1: Summary and Next Steps*. https://blog.iota.org/trinity-attack-incident-part-1-summary-and-next-steps-8c7ccc4d81e8/. [Online]. Dostopno: 22. december 2024. 2020.

[18] Silviu Stahie. *Common Credentials Criminals Use in IoT Dictionary Attacks Revealed*. https://www.bitdefender.com/en-au/blog/hotforsecurity/common-credentials-criminals-use-in-iot-dictionary-attacks-revealed. [Online]. Dostopno: 31. marec 2025. 2021.

[19] Caroline Cakebread. *You’re not alone, no one reads terms of service agreements*. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11. [Online]. Dostopno: 8. december 2024. 2017.

[20] Ltd Qingdao Yeelink Information Technology Co. *Yeelight WiFi Light Inter-Operation Specification*. https://www.yeelight.com/download/Yeelight_Inter-Operation_Spec.pdf. [Online]. Dostopno: 8. december 2024. 2015.

[21] Sara Lazzaro in sod. “Is Your Kettle Smarter Than a Hacker? A Scalable Tool for Assessing Replay Attack Vulnerabilities on Consumer IoT Devices”. V: *Proceedings of the 2024 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2024, str. 114–124. DOI: 10.1109/PerCom59722.2024.10494466.

[22] W3Techs. *Usage statistics and market shares of SSL certificate authorities for websites*. https://w3techs.com/technologies/overview/ssl_certificate. [Online]. Dostopno: 10. december 2024. 2025.

[23] Tehseen Mazhar in sod. “Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence”. V: *Brain Sciences* 13.4 (2023), str. 683. DOI: 10.3390/brainsci13040683.

[24] Nadia Ansar in sod. “A Cutting-Edge Deep Learning Method For Enhancing IoT Security”. V: *arXiv preprint arXiv:2406.12400* (jun. 2024). DOI: 10.48550/arXiv.2406.12400.

[25] Volviane Saphir Mfogo in sod. “AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices”. V: *arXiv preprint arXiv:2303.12367* (mar. 2023). DOI: 10.48550/arXiv.2303.12367.

[26] Fatima Hussain in sod. “Machine Learning in IoT Security: Current Solutions and Future Challenges”. V: *arXiv preprint arXiv:1904.05735* (mar. 2019). DOI: 10.48550/arXiv.1904.05735.

[27] Hamed Taherdoost. “Security and Internet of Things: Benefits, Challenges, and Future Perspectives”. V: *Electronics* 12.8 (2023), str. 1901. DOI: 10.3390/electronics12081901.

Kristjan Bratašević je študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zanima se za področje kibernetske varnosti in razvoja programske opreme, še posebej za vsakodnevno uporabo. Posveča se ustvarjanju varnih celovitih aplikacijskih sistemov, tako z vidika programske kode, kot s sistemskega in omrežnega vidika.

Matevž Pesek je izredni profesor in raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je diplomiral (2012) in doktoriral (2018). Od leta 2009 je član Laboratorija za računalniško grafiko in multimedije. Od leta 2024 izvaja predmeta Varnost programov in Varnost sistemov, kjer se raziskovalno ukvarja s poučevanjem konceptov in organizacijo dogodkov s področja računalniške varnosti.