Anti tampering tehnike

Pandurić, Mario

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

ANTI TAMPERING TEHNIKE

Završni rad

Mario Pandurić

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 01.09.2022.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Mario Pandurić
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina	R4255, 26.07.2018.
OIB Pristupnika:	35750262452
Mentor:	Izv. prof. dr. sc. Davor Vinko
Sumentor:	,
Sumentor iz tvrtke:	
Naslov završnog rada:	Anti tampering tehnike
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rad:	Zadatak završnog rada je obraditi vrste i metode anti tampering tehnika za zaštitu uređaja od invazivnih napada. Analizirati mogućnosti primjene obrađenih anti tampering tehnika na IoT uređajima. Za više informacija javiti se mentoru: davor.vinko@ferit.hr
Prijedlog ocjene završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene od strane mentora:	01.09.2022.
Datum potvrde ocjene od strane Odbora:	07.09.2022.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

IZJAVA O ORIGINALNOSTI RADA

Osijek, 10.09.2022.

Ime i prezime studenta:	Mario Pandurić
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4255, 26.07.2018.
Turnitin podudaranje [%]:	6

Ovom izjavom izjavljujem da je rad pod nazivom**: Anti tampering tehnike**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Davor Vinko

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1. UVOD

Bilo da se radi o industriji, medicini ili samo zabavi, Internet objekata (IoT) uređaji su sve popularniji i korišteniji posljednjih godina. Iako nam svakodnevno olakšavaju posao, treba biti oprezan s korištenjem ovih uređaja zbog opasnosti u vidu krađe podataka, identiteta, gubljenje podataka, neovlaštenog pristupa pa čak i uništenja cijelog uređaja.

Kad govorimo o zlouporabi IoT uređaja i svih računala općenito, prvenstveno mislimo na zloćudni softver kao što su trojanski konj, računalni crvi i računalni virusi. Međutim jako malo se govori o fizičkoj zaštiti samog IoT uređaja. Podatke je moguće uništiti ili „izvući“ čak i iz samog čipa fizičkim pristupom što znači da uređaj sa slabom fizičkom zaštitom može biti laka meta hakerima.

U ovom završnom radu su predstavljeni IoT uređaji, njihova građa i njihova primjena. Opisan je pojam tamperinga, te su navedene i opisane tehnike za sprječavanje i otežavanje tamperinga i analizirano je nekoliko uređaja o mogućim primjenama anti tampering tehnika za pojedini uređaj. Za svaku tehniku je navedeno po par izvedbi kako se ona postiže i neke prednosti ili nedostaci istih.

1.1. Zadatak završnog rada

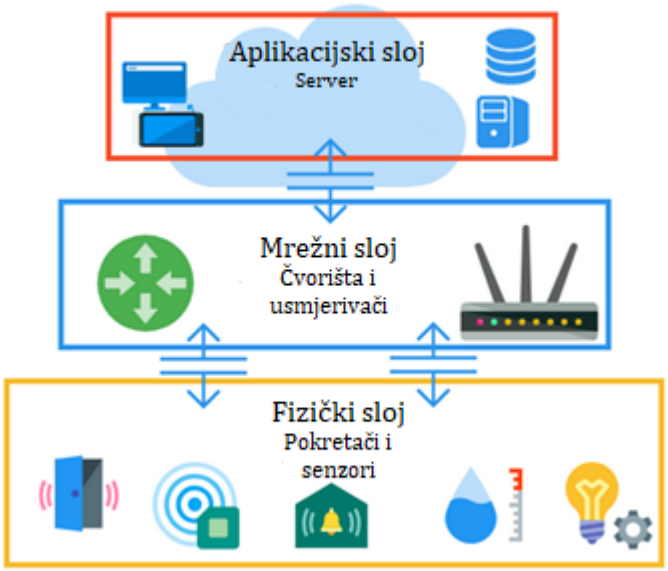
Zadatak završnog rada je obraditi vrste i metode anti tampering tehnika za zaštitu uređaja od invazivnih napada. Analizirati mogućnosti primjene obrađenih anti tampering tehnika na IoT uređajima.

2. INTERNET OBJEKATA

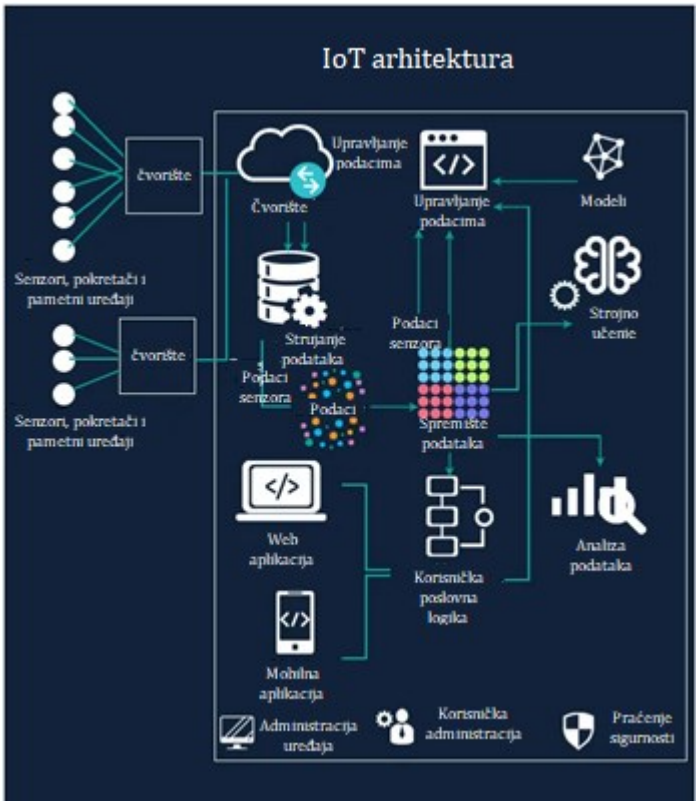
Pojam Internet objekata ili Internet stvari (IoT) se odnosi na skupinu međusobno povezanih uređaja koji razmjenjuju podatke putem Interneta ili neke druge komunikacijske mreže. U te uređaje spadaju razni senzori, pametni uređaji (pametni telefoni, pametni satovi, uređaji pametne kuće), moderna vozila, pa čak i životinje i ljudi (primjerice osoba sa srčanim implantatom). Uređaji prikupljaju podatke iz okoline i razmjenjuju ih s drugim IoT uređajima putem čvorišta ili nekog drugog rubnog uređaja gdje se podaci šalju u oblak ili se obrađuju lokalno. Uređaji većinu svog posla odrađuju bez posredovanja čovjeka, ali čovjek može komunicirat s njima, npr. za pristup podacima, za programiranje istih itd [1].

2.1. Građa i tehnologije Internet objekata

Za IoT uređaje ne postoji univerzalno definirana arhitektura, različiti istraživači su predlagali različite vrste arhitekture. Najjednostavnija arhitektura svakog IoT uređaja se može predstaviti s 3 različita sloja. On prikazuje glavnu ideju IoT uređaja. Prvi i najniži sloj je fizički sloj. Fizički sloj se odnosi na senzore i pokretače koji prikupljaju podatke iz okoline i pretvaraju ih u informacije koje se dalje koriste za analizu. Drugi sloj arhitekture IoT uređaja se odnosi na mrežni dio. On je odgovoran za spajanje IoT uređaja s drugim pametnim uređajima i serverima te za prijenos i obradu podataka dobivenih senzorom. Aplikacijski sloj je najviši sloj od ova dva navedena sloja. Odgovoran je za dostavljanje informacija korisniku. Podijeljen je na dva dijela, prvi dio se odnosi na usluge računarstva u oblaku. Drugi dio se odnosi na generirane aplikacije za IoT platforme. Te aplikacije su slične mobilnima i služe prikazu prikupljenih informacija i kontroli IoT uređaja [2].



Sl. 2.1.1. Troslojni prikaz arhitekture IoT uređaja [3]



Sl. 2.1.2. Detaljniji prikaz arhitekture IoT uređaja [4]

Kako bi IoT uređaj ispravno funkcionirao treba mu omogućiti i implementirati određene tehnologije. U početku su se za adresabilnost koristile RFID labele i identifikacija pomoću elektroničkog produkta koda (EPC). Današnji IoT se identificiraju pomoću IP adrese. Za adresiranje se koristi IPv6 protokol. Za bežično povezivanje i komunikaciju uređaja pri malim udaljenostima, koristi se Bluetooth Low Energy (BLE), ZigBee protokol, NFC protokol, RFID tehnologija, Wi-Fi. BLE je verzija Bluetooth-a s ciljem manje potrošnje energije i troškova namijenjena zdravstvenim ustanovama, kućnoj zabavi i sigurnosti. ZigBee je bežični mrežni protok sličan BLE-u, ali s većim dometom i sporijim prijenosom podataka u odnosu na BLE. NFC protokol se koristi za komunikaciju do 4 cm. Pogodan je kod sustava za plaćanje i kod prijave/odjave korisnika. RFID tehnologija je tehnologija koja služi za razmjenjivanje informacija između prijenosnih uređaja i host računala putem radio frekvencije. Sastoji se od labele ili taga koja sadrži podatke, antene i kontrolera. Wi-Fi je tehnologija za bežično lokalno umrežavanje bazirana na IEEE 802.11 standardu. Uređaji komuniciraju preko zajedničke točke ili izravno međusobno.

Za bežično povezivanje uređaja na srednjim udaljenostima, koriste se 5G i LTE Advanced tehnologija. LTE Advanced je mobilni komunikacijski standard i poboljšanje LTE standarda. 5G tehnologija omogućuje spajanje velikog broja IoT uređaja u pokretu pri brzini do 10 Gbit/s.

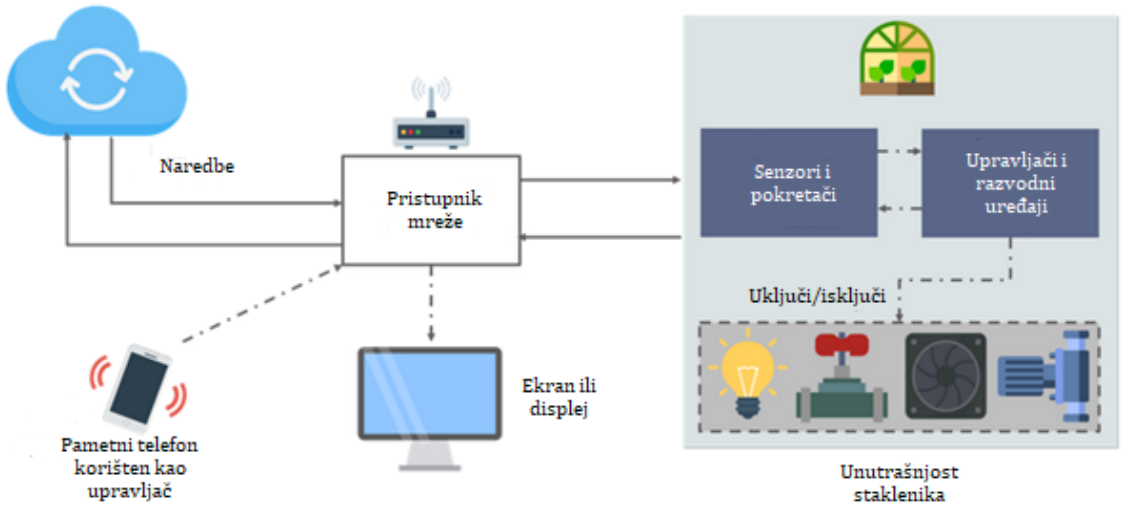
Za povezivanje pri velikim udaljenostima se koristi LPWAN i VSAT. LPWAN je bežična mreža s niskom brzinom prijenosa, ali i smanjenim troškovima. VSAT je satelitska komunikacijska tehnologija koja koristi male satelitske antene za uskopojasni i širokopojasni prijenos podataka.

Ethernet kabel se koristi za lokalno žično povezivanje. [2]

2.2. Primjena IoT uređaja

IoT ima vrlo široku primjenu od potrošačkih uređaja do proizvodnje i industrije. U nastavku su navedene najčešće primjene IoT uređaja.

Najpoznatiji IoT uređaji su uređaji za pametnu kuću. Neki od uređaja koji u njih spadaju su: pametna sigurnosna kamera, pametne utičnice, pametna rasvjeta, pametni termostat, pametna pećnica itd. Druga od najčešćih primjena s kojom se susrećemo su nosivi uređaji kao što su pametni satovi, senzor za mjerenje glukoze u krvi, senzori za mjerenje krvnog tlaka, pametni mobiteli. Još je bitno spomenuti primjenu IoT uređaja u poljoprivredi i industriji u svrhu automatizacije proizvodnje. Pametni sustavi omogućuju kontroliranje i praćenje klimatskih uvjeta pomoću pametnog uređaja (pametni telefon ili tablet) u staklenicima, vlažnosti tla na poljima, temperaturu i sl.



Sl. 2.2.1. Prikaz korištenje IoT uređaja u plastenicima [5]

3. TAMPERING

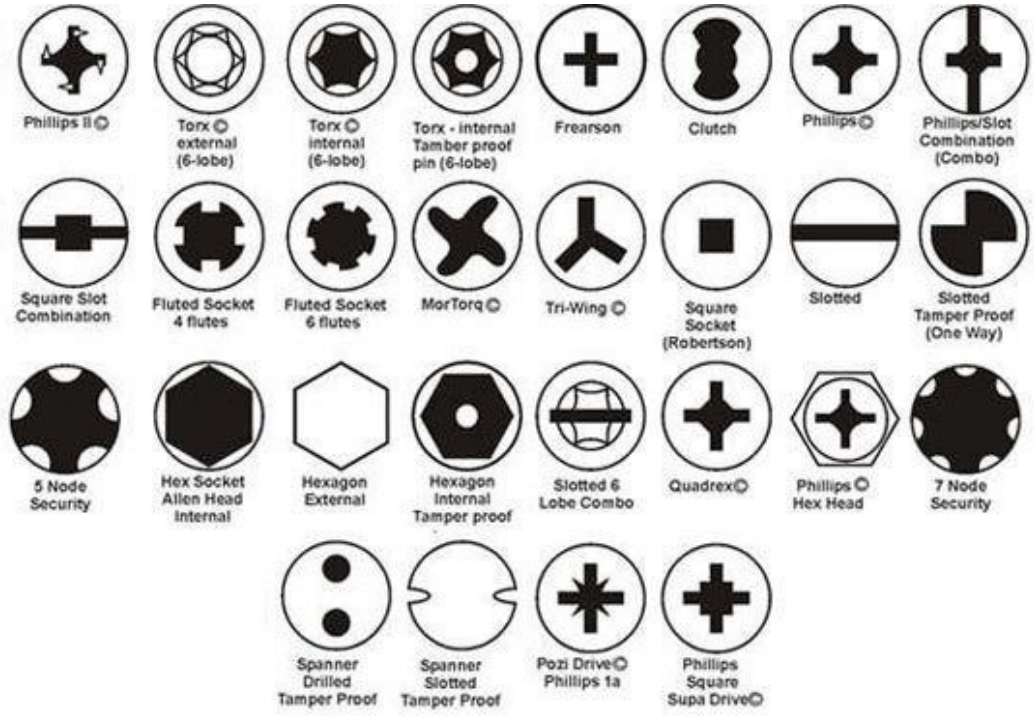
Pojam tampering općenito se odnosi na neku nedozvoljenu radnju s ciljem krađe podataka, mijenjanja podataka, prevare, sabotaže uređaja, odnosno općenito zbog zlouporabe. To se može odnositi na neovlašteno otvaranje uređaja ili na neovlašteno čitanje, mijenjanje i pisanje podataka koje taj uređaj prenosi ili čuva. Kako bi se rizik od tamperinga smanjio, poduzete su određene mjere pri proizvodnji uređaja. Te tehnike su podijeljene u 4 glavne kategorije : prevencija tamperinga, detekcija tamperinga, dokaz tamperinga i reakcija na tampering.

4. ANTI TAMPERING TEHNIKE

4.1. Prevencija tamperinga

4.1.1. Prevencija otvaranja kućišta uređaja

Kod zaštite sklopovlja prvi korak je što bolje osigurati kućište, odnosno otežati napadačima otvaranje istoga. To se postiže posebnim tehnikama i metodama spajanja dijelova kućišta. Prva mogućnost spajanja kućišta može se izvesti korištenjem vijaka s posebnim utorom na glavi vijka. Iako na neki način otežavaju otvaranje kućište uređaja, odvijače za njih je jednostavno nabaviti, jeftini su za kupiti i mogu se isprintati 3D printerom. Primjer ovoga su telefonski razvodni ormari gdje se koriste sigurnosni vijci s trokutastom glavom.



Sl. 4.1.1. Primjer vijaka s posebnim utorima [6]

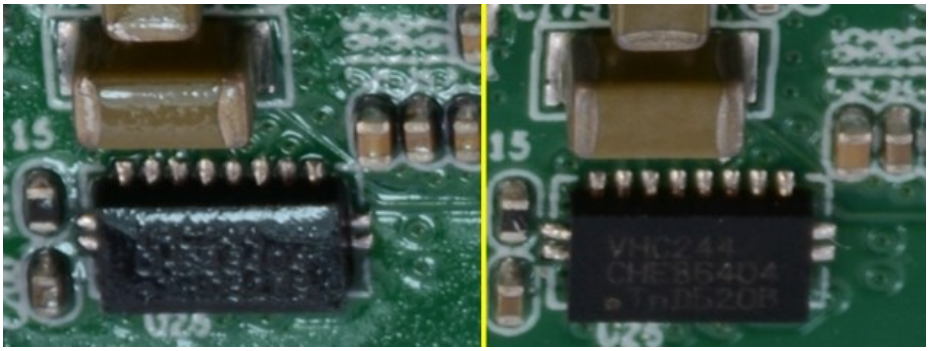
Još jedna često korištena tehnika spajanja kućišta je spajanje pomoću ultrazvučnog zavarivanja. Ultrazvučno zavarivanje je proces spajanja metalnih ili plastičnih dijelova gdje se dijelovi nalegnu jedan na drugi te zbog djelovanja ultrazvuka ti dijelovi počinju vibrirati i zagrijavati se zbog trenja, te uz djelovanja pritiska i hlađenja dolazi do spajanja tih dijelova. Ovaj način spajanja koristi se za spajanje čipova i elemenata u električnim mikro krugovima. Prednost ovog načina zavarivanja nad običnim je u tome što se mogu spajati različiti materijali. Također, uređaj je nemoguće otvoriti, a da se ne vidi nastalo oštećenje. Hlađenjem zavarenog dijela tekućim dušikom i ispunjavanjem s komprimiranim zrakom dolazi do napuknuća zavarenih dijelova [7].

Sl. 4.1.2. Primjer uređaja koje mu je kućište spojeno ultrazvučnim zavarivanjem [8]

4.1.2. Zaštita komponenata i tiskane pločice

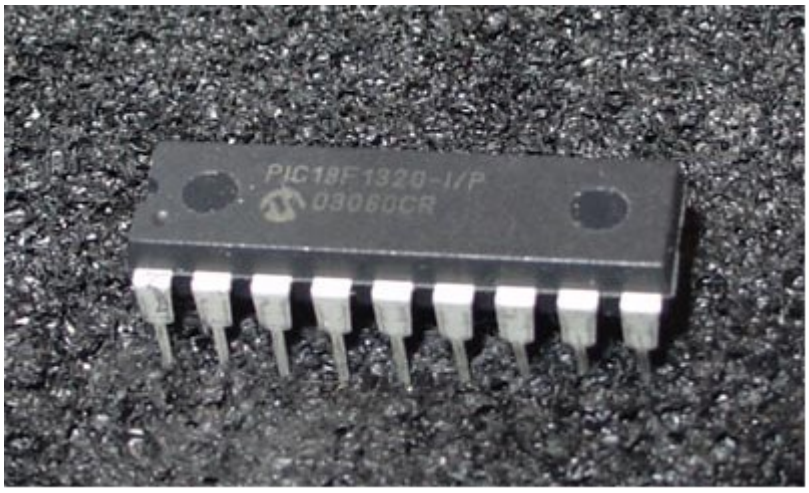
Za zaštitu pločice i elemenata na njoj, koristi se enkapsulacija elektroničkih komponenti i zaštita konformnim premaznim materijalom. Oni pločicu i elemente štite od vlage, prašine, korozije, vibracije, ali i od tamperinga, obrnutog inženjerstva i sl. Konformni premaz se odnosi na tanki polimerni sloj koji se nanosi na elektroničke komponente u svrhu zaštite. Debljina sloja je između 25 i 250 μm. Sloj se može nanijeti na mnogo načina: četkicom, sprejom ili raspršivačem. Ovisno o okolini i uvjetima, za konformni premaz se koriste različiti materijali: akrilno staklo (dobra otpornost na kemikalije i vlagu, temperatura taljenja je oko 150º C), epoksidne smole (ima slična svojstva kao i akrilno staklo, ali ima bolju otpornost na kemikalije) i silikon (odlična otpornost na vlagu i kemikalije, može izdržati temperaturu od oko 200º C, ali ga je mnogo lakše ukloniti od akrilnog stakla i epoksidnih smola) [9]. Za razliku od komformnog premaza, sloj enkapsulacije je deblji i čvršći. Enkapsulacija može biti potpuno zatvorena ili djelomično zatvorena. Kod djelomične enkapsulacije, komponente se enkapsuliraju samo na određenim mjestima.

Sl. 4.1.3. Primjer enkapsulacije [10]

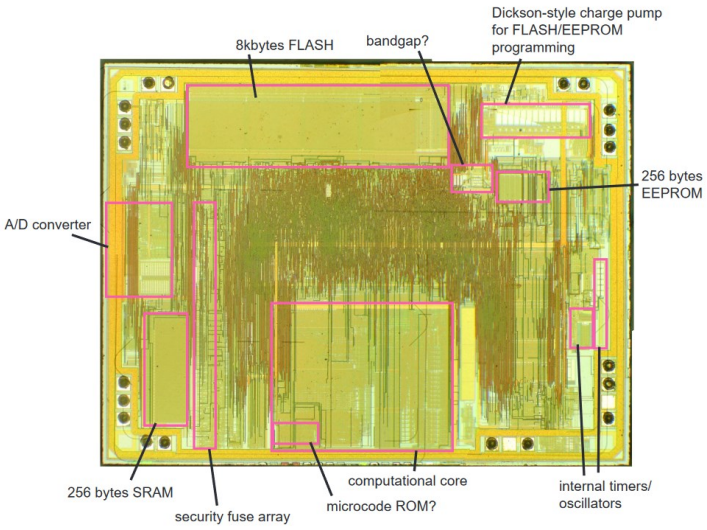


Sl. 4.1.4. Prikaz zaštite komponente komfornim premazom (lijevo) i bez zaštite (desno) [11]

Postoje čipovi koji u sebi imaju ugrađene mehanizme za zaštitu od tamperinga kao što je čip PIC 18F1320. On u sebi ima ugrađene sigurnosne osigurače koji onemogućuju čitanje i mijenjanje memorije. Resetiranjem tih osigurača bi se obrisali svi podaci s čipa. Međutim, FLASH memorija ovog čipa koristi tehnologiju sličnu UV-EEPROM memoriji. Zbog toga izlaganjem UV svjetlu određenih dijelova čipa, moguće je onesposobiti zaštitne osigurače i pročitati podatke spremljene u memoriji. Kao zaštita od toga na čip se može zalijepiti tamna ljepljiva traka [12].



Sl. 4.1.5. PIC 18F1320 čip [12]



Sl. 4.1.6. Struktura PIC 18F1320 čipa [12]

4.2. Detekcija tamperinga

Detekcija tamperinga je svojstvo uređaja da osjeti da je uređaj pod napadom, odnosno da reagira na napad i pokrene odgovarajuću obrambenu radnju. Dizajnira se s obzirom na vrstu prijetnje i rizika. Uglavnom se implementira pomoću senzora, sklopki i anti-tampering strujnih krugova.

4.2.1. Anti-tampering sklopke

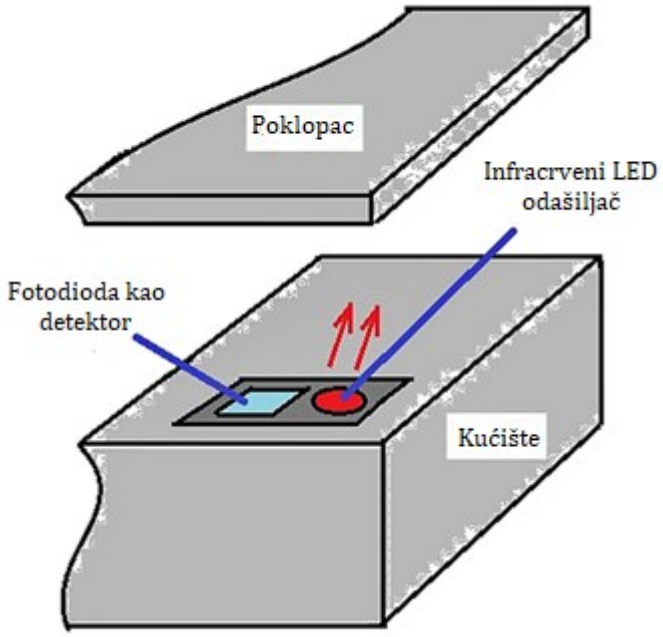
Elektromehaničke sklopke se mogu koristiti kao detektori tamperinga. Upravljački sklop prati napon na analogno-digitalnom pretvaraču (ADC) ili GPIO-u koji je spojen na sklopku, otvaranjem uređaja, sklopka se okida te upravljački sklop reagira. Prednost ove metode je mogućnost vraćanja sklopke u početno stanje nakon tamperinga tj. nije destruktivna kao kod nekih metoda sa strujnim krugovima. Nedostatak je osjetljivost kontakata na koroziju i oksidaciju što može izazvati zaglavljenje kontakata. Zbog toga ove metoda nije preporučljiva za uređaje namijenjene za dužu vremensku uporabu.

Osim elektromehaničkih sklopki postoje još i magnetske sklopke. Na kućište uređaja se ugrađuje permanentni magnet koji stvara magnetsko polje unutar uređaja. Uklanjanjem poklopca uređaja magnetsko polje oslabi na što reagira ugrađena magnetska sklopka. Prednost ovoga je što nema mehaničkih kontakata, ali problem može nastati zbog smetnji uzrokovanim stranim magnetskim poljima [13].

4.2.2. Anti-tampering senzori

Postoje mnogo različitih vrsta senzora za detekciju tamperinga kao što su senzori za temperature, napona, zračenja itd. Senzori napona služe za detekciju promjene napona pri radu uređaja. Slično kao i senzori napona, senzori temperature reagiraju na promjenu radne temperature uređaja. Senzori zračenja reagiraju na X-zrake i na ionizirajuća zračenja. Za primjer je prikazan rad jednog senzora koji reagira na infracrveno (IR) zračenje.

U uređaj je ugrađena fotodioda koja služi kao detektor i IR LED koja služi kao odašiljač. S unutarnje strane poklopca uređaja se nalazi reflektirajuća ploča koja prekriva fotodiodu. IR LED odašilje svjetlost koja se reflektira od reflektirajuće ploče na fotodiodu. Ako je jakost reflektirajuće svijetlosti iznad određenog praga jakosti, poklopac uređaja je na mjestu. U slučaju da je poklopac pomaknut, jakost reflektirajućeg svijetla će dramatično opasti što znači da poklopac nije na prvobitnom mjestu, odnosno da netko pokušava otvoriti uređaj. Prednost ove metode je otpornost na koroziju i nije destruktivna (neće se uništiti i radit će ponovo nakon tamperinga) [12].



Sl. 4.2.1. Prikaz IR senzora [13]

4.2.3. Anti-tampering strujni krugovi

Ovo je jedna od najjednostavnijih metoda detekcije tamperinga. Svodi se na mjerenje električnih veličina (struje, napona, otpora, kapaciteta i sl.) te reakciju na promjenu istih. Jedan od načina na koji se ova metoda može izvesti je tako da se komad žice ili nekog drugog vodljivog materijala ugradi s unutarnje strane kućišta. Dok se ne dira, ta žica normalno zatvara strujni krug. Kod pokušaja tamperinga ili otvaranja uređaja, taj zaštitni dio se slomi te strujni krug postaje otvoren. Ova metoda je jednostavna i jeftina, ali je destruktivna (nakon što se poklopac vrati, žica i dalje ostaje slomljena) [13].

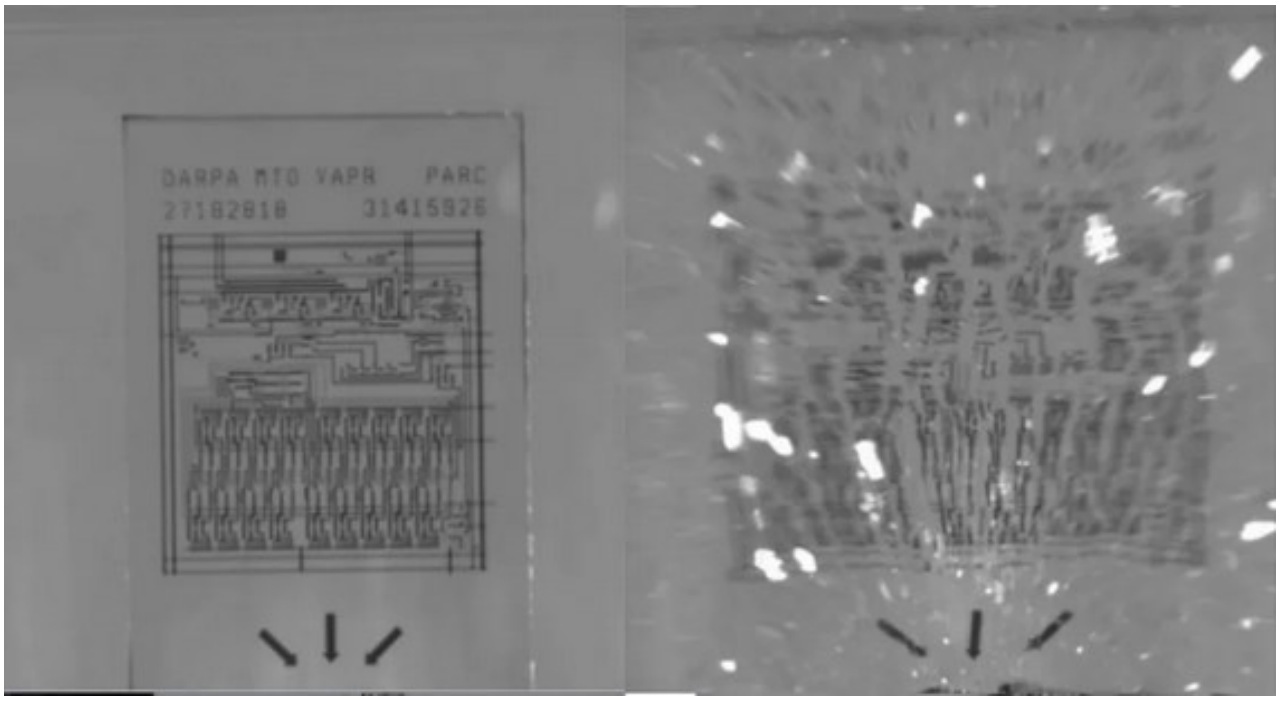
Drugi način na koji se ova metoda može izvesti je pomoću mreža za otkrivanje upada. To mogu biti optička vlakna, obične žice i piezoelektrični limovi. Oni se mogu obložiti oko kritičnih dijelova koje želimo zaštiti te pomoću raznih mjernih uređaja možemo pratiti njihov otpor ili kapacitet.

4.3. Odgovor na tampering

Pod pojmom odgovor na tampering misli se na radnju koja se izvodi prilikom tamperinga. Cilj joj je izbrisati sve dijelove memorije koji sadrže lozinke, kriptografske ključeve, PIN-ove ili neke druge bitne podatke. Mehanizam je obično pokrenut signalom senzora (senzori za detekciju tamperinga) ili naredbom operatora.

4.3.1. Samouništive komponente

Postoje komponente i čipovi koji se u slučaju tamperinga same uništavaju. Silikonske pločice su spojene sa djelićem zaštitnog stakla koje se zagrijavanjem razbija u komadiće. Zagrijavanje se uključuje daljinski preko Wi-Fi-a ili radiovalovima. Ovaj način zaštite prikazan je na slici 4.3.1 [14].



Sl. 4.3.1. Prikaz čipa prije samouništenja (lijevo) i nakon samouništenja (desno) [14]

Također, postoji izvedba gdje se za samouništenje čipa koriste različite kemikalije umjesto stakla kao u prethodnom primjeru. Čip je ugrađen u polikarbonatnu ljusku unutar koje se nalaze malene šupljine ispunjene s metalima rubidijem i cezijem. Metali su zatvoreni iza membrane načinjene od grafena i silicijevog nitrida. Kako bi ih se ispustilo, potrebno je poslati radio signal čipu. Tada čip provede električnu struju iz baterije do membrane. Dolazi do zagrijavanja i širenja grafena sve dok ne razbije silicijev nitrid. Nakon toga dolazi do kemijske reakcije metala i zraka. Kemijskom reakcijom nastaje toplina koja uništava polikarbonatnu ljusku i samim time i čip u njoj [15].

Sl.4.3.2. Čip nakon uništenja kemijskom reakcijom [15]

4.3.2. Nulizacija podataka

Nulizacija (eng. zeroization) je naziv za mehanizam brisanja osjetljivih podataka s čipova kao odgovor na tampering. Nulizacijom se može obrisati glavna memorija, cache memorija, NVRAM i FLASH memorije. Pokrenuta je poduzimanjem akcije, primjerice pritiskom gumba na ploči.

Nedostatak ove metode je što zahtijeva neprekidno napajanje. Također može doći i do remanencije (zaostatak) podataka.

Remanencija podataka je pojam koji se odnosi na pojavu ostataka podataka nakon što su se podaci prethodno pokušali izbrisati ili promijeniti. Kao posljedica toga može doći do povratka i otkrivanja podataka. Ostaci podataka su zabilježeni i kod privremenih memorija kao što su SRAM I DRAM, i to pri sobnoj temperaturi. Snižavanjem temperature memorije vrijeme zadržavanja memorije je duže, primjerice na hlađenje SRAM-a na -20 ºC, vrijeme zadržavanje može biti i do 17 minuta, a hlađenjem SRAM-a na -50 ºC i do 10 sati [16].

Ovisno o vrsti memorije, mjere koje se mogu poduzeti za sprječavanje povratka podataka na ovaj način su: prepisivanje memorije sa svim 0 ili svim 1, demagnetizacija, samouništenje čipa.

4.4. Dokaz tamperinga

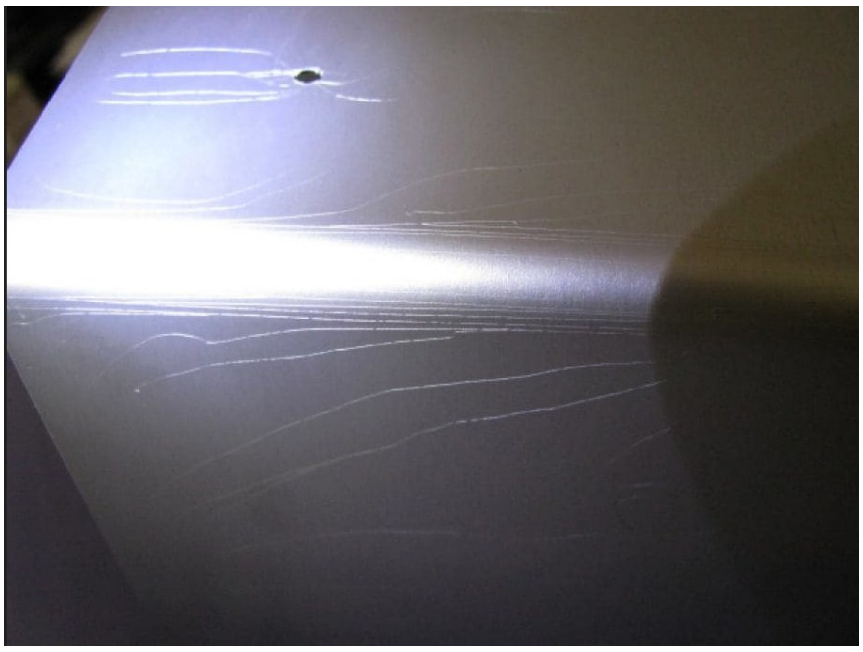
Dokaz tamperinga se odnosi na mjere kojima je svrha da u slučaju da dođe do tamperinga uređaja, ostane vidljivi dokaz. Njihov zadatak nije zaštita od napada ili reakcija dok je napad u tijeku, nego zabilježiti da se napad dogodio. Kako bi ovo imalo smisla, vrlo je bitno često provjeravati sustav i uređaje Ove metode su jako osjetljive i na najmanja oštećenja. Postižu se mehaničkim i kemijskim svojstvima materijala.

4.4.1. Pakiranje uređaja u krhke i lomljive materijale

Uređaji su zatvoreni u lomljivom materijalu kao što su primjerice staklo i keramika. U slučaju pokušaja otvaranja i dolaska do uređaja, dolazi do pucanja stakla ili keramike ostavljajući dokaz o tamperingu [16].

4.4.2. Pukotine na paketu uređaja

Slično kao i prošla izvedba, samo umjesto keramike i stakla, ovdje se uređaji nalaze u aluminiju ili nekom sličnom materijalu. U slučaju zagrijavanja i naglog hlađenja, dolazi do vidljive pojave plitkih udubljenja i pukotina na površini materijala. Također kod tamperinga uređaja kojem je kućište spojeno ultrazvučnim zavarivanjem, moguće je vidjeti ovakve pukotine [17].



Sl. 4.4.1. Prikaz oštećenja aluminija gore opisanom metodom [18]

4.4.3. Dokaz pomoću boje

U boji kućišta uređaja se nalaze mikro baloni suprotne boje. Oštećenjem uređaja dolazi do razlijevanja boje u balonima što ostavlja vidljivi trag [17].

4.4.4. Holografske ljepljive trake i naljepnice

Na površini trake ili naljepnice se nalazi holografska slika koja, kad se traka ili naljepnica odlijepi s površine uređaja (kako bi se uređaj pokušao otvoriti) ostaje na površini uređaja [17].

Sl. 4.4.2. Primjer anti-tampering naljepnice [19]

5. ANALIZA PRIMJENE ANTI TAMPERING TEHNIKA ODREĐENIH IOT UREĐAJA

Za analizu primjene navedenih anti tampering tehnika, za primjer je uzeto nekoliko IoT uređaja, za koje će se navesti koje bi tehnike bile pogodne za određeni uređaj te koje su tehnike već primijenjene.

5.1. Primjer primijenjenih anti tampering tehnika na IoT uređaje

5.1.1. Primijenjene anti tampering tehnike pametnih telefona

Pametni telefoni su najpopularniji i najkorišteniji IoT uređaji. Pozivi, pristup internetu, slanje poruka i e-mailova, igranje igara su samo neke usluge koje ovi uređaji pružaju. Zbog toga su nam vrijedni podaci koje oni čuvaju te su uzeti kao jedan od primjera analize. Ovaj primjer se najviše bazira na Xiaomi Redmi Note 7 Pro uređaju, ali slično je i kod ostalih pametnih telefona.

Do prije nekoliko godina, poklopac pametnih telefona se mogao skinuti bez nekih većih problema. Razlog tome je bila potreba za ubacivanjem memorijskih i SIM kartica. Kod današnjih uređaja to nije slučaj, već je poklopac zalijepljen za uređaj te ga je zbog toga teže otvoriti. Jednom odvojen poklopac više se ne može vratiti bez ponovnog lijepljenja. Ovo je dobra stvar jer može poslužiti kao dokaz tamperinga. Čipovi su zaštićeni plastikom koja je pričvršćena običnim vijcima te ju je lako otkloniti. Na poleđini poklopca se nalazi anti tampering naljepnica kao upozorenje i dokaz otvaranja uređaja.

Sl. 5.1.1. Unutrašnjost Xiaomi Redmi Note 7 pametnog telefona [20]

5.1.3. Analiza primjene anti tampering tehnika za senzore pokreta

Senzori pokreta su također vrlo korišteni uređaji za pametne kuće. Oni za detekciju tamperinga koriste mehaničku sklopku koja se u slučaju tamperinga aktivira te na displeju se prikazuje poruka upozorenja.

Sl. 5.1.2. Prikaz sklopke koja se nalazi u unutrašnjosti senzora pokreta [21]

5.2. Mogućnost primjene anti tampering tehnika na IoT uređaje

5.2.1. Analiza primjene anti tampering tehnika sigurnosnih kamera

Sigurnosne kamere su jedan od često korištenih uređaja pametnih kuća. Osim u privatnim i oko privatnih kućanstava, može ih se pronaći u poslovnim okruženjima. Jedan su od najbitnijih uređaja za praćenje i nadzor nekog sustava i prostorija. Često su postavljene vani na otvorenom i zato su ranjive na oštećenja, krađu ili vandalizam.

Prva razina zaštite koju korisnik može izvesti jest onemogućiti lak pristup kamere, odnosno postaviti kamera na teško pristupačnom mjestu, primjerice na velikoj visini. Kao zaštitu prevencije tamperinga, moguće je koristiti vijke sa „zvjezdastom“ glavom [22]. Za zaštitu podataka kamere u slučaju tamperinga, podaci bi se mogli uništiti nulizacijom podataka. Kao detekcija tamperinga, za ovaj uređaj bi se mogao koristiti opisani infracrveni senzor.

Sl. 5.2.1. WBox WBC0E CLIB5R4VM nadzorna kamera [23]

5.2.2. Analiza primjene anti tampering tehnika senzora za mjerenje temperature

Senzori za mjerenje temperature su često korišteni IoT uređaji, bilo da se radi o industrijskoj, proizvodnji, poljoprivredi ili za osobnu upotrebu. Za analizu kao opisan je Auriol IAN 375672 senzor.

Uređaj se sastoji od senzora koji se postavlja u prostoriju kojoj se želi mjeriti temperatura i prijamnika s displejom.

Kao prevencija za tampering kućišta moguće je koristiti vijke sa specijalnim glavama. Ultrazvučno zavarivanje nije opcija jer je potrebno mijenjati baterije u uređajima. Konformni premaz se može koristiti kao dodatna zaštita za električne komponente. Za detekciju bi bilo prikladno koristiti magnetske sklopke zbog mogućnosti mjerenja vanjske temperature. Korištenjem običnih elektromagnetskih sklopki vani na otvorenom, postoji mogućnost od korozije. Ljepljive trake i naljepnice se mogu koristiti za dokaz tamperinga.

Sl. 5.2.2. Auriol IAN 375672 senzor za mjerenje temperature [24]

5.2.3. Analiza primjene anti tampering tehnika bežični zvučnika

U zadnje vrijeme bežični zvučnici su popularniji od običnih „žičnih“ zvučnika. Oni primaju zvučne signale pomoću radiovalova, najčešće pomoću Wi-Fi-a i Bluetooth-a.

U uređaj ne idu baterije nego se puni preko USB porta što znači da je spajanje kućišta uređaja moguće izvesti ultrazvučnim zavarivanjem. Samim time prisilnom otvaranjem kućišta, ostali bi tragovi koji nam mogu ukazivati na dokaz tamperinga. Za detekciju tamperinga moguće je koristiti elektromehaničke ili magnetske sklopke.

Sl. 5.2.3. COOCHEER 24W Bluetooth zvučnik [25]

5.2.4. Analiza primjene anti tampering tehnika senzora kvalitete zraka

Senzori za određivanje kvalitete zraka su IoT uređaji koji mjere čestice koje onečišćuju zrak kao što su PM2.5 čestice, VOC čestice, CO2, formaldehid itd.

Uređaj se sastoji samo od senzora s displejom, baterija uređaja se puni preko USB priključka. Zbog toga, kao i kod bežičnih zvučnika, spajanje dijelova kućišta je moguće izvesti ultrazvučnim zavarivanjem. Komponente je moguće zaštiti konformnim premazom ili enkapsulacijom. Za detekciju moguće je koristiti elektromehaničke ili magnetske sklopke.

Sl. 5.2.4. Temtop M10 senzor za određivanje kvalitete zraka [26]

5.2.5. Analiza primjene anti tampering tehnika pametnog aparata za kavu

Pametni aparati za kavu su aparati za kavu koji se putem Wi-Fi-a ili Bluetootha bežično spajaju na pametni telefon pomoću kojih ih je moguće kontrolirati.

Spajanje kućišta uređaja bi bilo pogodno izvesti ultrazvučnim zavarivanjem. Kao i svaki uređaj do sada spomenut elektroničke komponente je moguće dodatno zaštiti konformnim premazom. Sve navedene metode za detekciju moguće je primijeniti na ovaj uređaj, ali najbolje je koristiti navedeni infracrveni senzor. S obzirom da je ovaj uređaj dovoljno velik, uz naljepnice za dokaz tamperinga moguće je koristiti mikro-balone s bojama.

Sl. 5.2.5. Atomi Smart Coffee Maker aparat za kavu [27]

6. ZAKLJUČAK

Zaštita uređaja od napada i zlouporabe nam je jako bitna. Uređaj nije dovoljno samo zaštititi od zloćudnog softvera, nego i od fizičkog pristupa odnosno tamperinga. Zato su u tu svrhu razvijene posebne tehnike zaštite. Najbitnija tehnika je prevencija tamperinga, cilj joj je onemogućiti ili barem otežati otvaranje samog uređaja. Za detekciju tamperinga najbolje je koristiti različite senzore. Odgovor na tampering se ne čini kao uvijek kao dobra praksa jer se podaci, (ponekad i sam čip s podacima) uništavaju. Izvedbe dokaza tamperinga se svode na vidljivi trag ili oštećenje na kućištu uređaja. Uređaj je zbog toga potrebo redovito pregledavati kako bi se utvrdio je li došlo do tamperinga ili pokušaja tamperinga. Svaka od pojedinih izvedbi tehnika ima svoje prednosti i nedostatke, i svaka je pogodna za određenu vrstu uređaja. Spajanje kućišta pomoću ultrazvučnog zavarivanja je bolje rješenje nego specijalnim vijcima jer ga je teže otvoriti te nasilnim otvaranjem kućišta ostavlja udubine i ogrebotine koje služe kao dokaz tamperinga. Međutim ovo nije izvedivo za sve uređaje, primjerice uređaji u koji se stavljaju baterije. Senzori za detekciju tamperinga su bolja opcija nego sklopke ili strujni krugovi. Većina IoT uređaja, posebice senzori su slično građeni pa zbog toga kod analize za zaštitu od tamperinga, tehnike za anti tampering su slične.

Nije se dobro oslanjati samo na jednu tehniku i izvedbu pojedine, nego je potrebno kombinirati više pojedinih radi bolje zaštite i pouzdanosti, primjerice ako jedan senzor za detekciju zakaže, možda drugi reagira.

LITERATURA

[1] A. S. Gillis, TechTarget, What is the Internet of things (IoT)?, dostupno: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT, pristup: 13. 5. 2022.

[2] M.Anantha Guptha, Internet of things and it's applications, Malla Reddy College of Engineering & Technology, dostupno na: https://www.mrcet.com/downloads/digital_notes/EEE/IoT%20&%20Applications%20Digital%20Notes.pdf, pristup: 10. 5. 2022.

[3] Internet of Things, mPython, dostupno na: https://mpython.readthedocs.io/en/master/tutorials/advance/iot/, pristup: 11. 5. 2022.

[4] IoT arhitektura, dostupno na: https://hr.education-wiki.com/7028347-iot-architecture, pristup: 11.5.2022.

[5] Real World IoT Applications in Different Domains, edureka, dostupno na: https://www.edureka.co/blog/iot-applications/, pristup: 12. 5 .2022.

[6] J. Paulin, Security Screw Identification Chart, 19. 8. 2013., dostupno na: https://justinpaulin.com/2013/08/19/security-screw-identification-chart/, pristup: 22. 5. 2022.

[7] Ultrasonic welding, Wikipedia, dostupno na: https://en.wikipedia.org/wiki/Ultrasonic_welding, pristup: 24. 5. 2022.

[8] Rps-sonic, U disk ultrasonic plastic seamless welding technology, 23. 8. 2019., dostupno na: https://www.rps-sonic.com/U-disk-ultrasonic-plastic-seamless-welding-technology-id3224864.html, pristup: 26. 5. 2022.

[9] Conformal coating, Wikipedia, dostupno na: https://en.wikipedia.org/wiki/Conformal_coating, pristup: 26. 5. 2022.

[10] Caplinq, Encapsulants for electrical insulation and mechanical protection, Liquid Encapsulants, dostupno na: https://www.caplinq.com/liquid-encapsulants.html?ENU&tag_id=1248, pristup: 20. 6. 2022.

[11] Teledyne Lumenera, Protecting Aerial Imaging Equipment with Conformal Coating, 24. 1. 2018. dostupno na: https://www.lumenera.com/blog/protecting-aerial-imaging-equipment-with-conformal-coating, pristup: 26. 6. 2022.

[12] Bunnie: studios, Hacking the PIC 18F1320, dostupno na: https://www.bunniestudios.com/blog/?page_id=40, pristup: 28. 6. 2022.

[13] J. Archibald, FIERCE Electronics, How To Implement Reliable Tampering Detection With A Standard Proximity Sensor Module, 27. 7. 2017., dostupno na: https://www.fierceelectronics.com/components/how-to-implement-reliable-tampering-detection-a-standard-proximity-sensor-module, pristup 10.7. 2022.

[14] T. Ghose, This Computer Chip Will Self-Destruct in 5 Seconds, Live Science, 6. 8. 2015., dostupno na: https://www.livescience.com/52397-self-destructing-chip-secures-data.html, pristup: 15. 7. 2022.

[15] K. Baggaley, PopSci+, These self-destructing electronics can turn your data to dust on command, 6. 2. 2018., dostupno na: https://www.popsci.com/vaporize-electronics-radio-signal/, pristup: 20. 7. 2022.

[16] Elena Dubrova, Anti-Tampering Techniques, Royal Institute of Technology, Stockholm, Sweden, dostupno na:

https://people.kth.se/~msmith/is2500_pdf/AntiTamper%20Techniques_elena.pdf, pristup: 20. 7. 2022.

[17] S. H. Weingart, Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses, Secure Systems and Smart Card Group IBM Thomas J. Watson Research Center, Hawthorne, NY

[18] Finishing, Crazing/cracking problem in anodizing, dostupno na: https://www.finishing.com/328/30.shtml, pristup: 25. 7. 2022.

[19] Indiamart, Tampering Evident Labels - "warranty Void If Removed" Labels, dostupno na: https://www.indiamart.com/proddetail/tampering-evident-labels-warranty-void-if-removed-labels-13069328673.html, pristup: 26 .7. 2022.

[20] iFixit, Xiaomi Redmi Note 7 Screen and Metal case Replacement, 7. 5. 2021., dostupno na: https://www.ifixit.com/Guide/Xiaomi+Redmi+Note+7+Screen+and+Metal+case+Replacement/144548, pristup: 29. 7. 2022.

[21] Boundary, One of my sensors is tampered, how can I resolve this?, dostupno na: https://support.boundary.co.uk/hc/en-gb/articles/360018662517-One-of-my-sensors-is-tampered-how-can-I-resolve-this-, pristup 1. 8. 2022.

[22] Verkada, Protecting Your Security Camera Hardware, dostupno na: https://info.verkada.com/security/camera-hardware/, pristup: 2. 8. 2022.

[23] Indiamart, https://www.indiamart.com/proddetail/wbox-wbc0e-clib5r4vm-ir-bullet-camera-23153582673.html, pristup: 4.8. 2022.

[24] Kernelreoladed: http://kernelreloaded.com/reading-temperature-data-from-auriol-temperature-station-via-rtl_433/, pristup: 5.8. 2022.

[25] Amazon: https://www.amazon.com/Wireless-Bluetooth-COOCHEER-Waterproof-Dustproof/dp/B07Y382CL2, pristup: 7. 8. 2022.

[26] Amazon: https://www.amazon.com/Temtop-M10-Professional-Electrochemical-Rechargeable/dp/B07DHXQXGK?th=1&linkCode=ll1&tag=leafscore-20&linkId=8234cdd1409d50b8cb77e6b5cc8cd983&language=en_US&ref_=as_li_ss_tl, pristup: 9. 8. 2022.

[27] Amazon: https://www.amazon.com/Atomi-Smart-WiFi-Coffee-Maker/dp/B08PHBJXLY, pristup: 10. 8. 2022.

SAŽETAK

Cilj ovog završnog rada je predstaviti pojam tampering, navesti i opisati anti-tampering tehnike za IoT uređaje. Za svaku tehniku je opisano po nekoliko njihovih izvedbi. Za prevenciju tamperinga, navedeni su načini kako se može zaštiti kućište posebnim metodama spajanja i na koje načine se mogu zaštititi komponente. Navedene su i opisane vrste sklopki i vrste senzora koje koristimo za detekciju tamperinga. Za primjer navedenog je opisan senzor koji pomoću infracrvenog zračenja detektira tampering. Prikazani su načini kako se podaci mogu uništiti u slučaju tamperinga, također su prikazani načini kako možemo dokazati tampering. Na kraju je navedeno nekoliko IoT uređaja i navedene su pogodne tehnike za zaštitu svakog uređaja.

Ključne riječi: anti-tampering, IoT, detekcija tamperinga, prevencija tamperinga, odgovor na tampering, dokaz tamperinga

ABSTRACT

The goal of this final paper is to present meaning of tampering, to state and describe anti-tampering tecniques for IoT devices. It is described several methods how they can be implemented for each techique.For tampering prevention, it is stated how housing can be protected and it is described how components can be protected. Types of swithces and sensors are stated and described for tampering detection. For example of tampering detection sensor, it is described sensor which with infrared radiation can detect tampering. It is explained how data can destroy itself in case of tampering, also it is described how can we make device tampering evident. At the end, it is stated and described few IoT devices and appropriate techniques for each stated device.

Key words: anti-tampering, IoT, tampering detection, tampering prevention, tampering response, tampering evident