VARSTVOSLOVJE,
letn. 18
št. 3
str. 288–302

Varnostno testiranje fizičnega kripto-modula za navidezna zasebna omrežja

Anže Zaletel, Jaka Žužek, Lavra Horvat, Katja Zupan, Sara Železnik, Nina Goršič, Maruša Lipušček

Namen prispevka:

Namen prispevka je predstaviti projekt[1] varnostnega testiranja v razvoju in produkciji fizičnega kripto-modula, ki je nujno potrebno pred lansiranjem izdelka na trg. Delo na projektu je bilo usmerjeno v izdelek Code 1 Secure (v nadaljevanju VPN kripto-modul C1S), za katerega je bila narejena primerjava s sorodnimi izdelki, predlagane različne ergonomične oblike ter opisani postopki potrebnih testiranj izdelka za pridobitev certifikatov oz. za doseganje standardov.

Metode:

Uporabljena je bila deskriptivna metoda s pomočjo študije primarnih in sekundarnih virov. Za potrebe opisa orodij za avtomatizirano testiranje smo delovanje orodij preizkusili in opravili vzorčna testiranja.

Ugotovitve:

Testiranje programske opreme in njene združljivosti s šifrirnimi algoritmi predstavlja najzahtevnejši del testiranj. Ključno stičišče projekta je predstavljal kolaboracijski portal, preko katerega se je evidentiral in spremljal napredek dela. S preizkušanjem orodij za avtomatizacijo opravil je bilo ugotovljeno, da avtomatizirano testiranje prihrani veliko časa in denarja.

Omejitve/uporabnost raziskave:

Projektno delo je bilo ciljno naravnano na izdelek VPN kripto-modula C1S, zato se tudi ugotovitve navezujejo nanj. Kljub temu lahko ugotovitve apliciramo na sorodne izdelke.

Praktična uporabnost:

S primerjavo sorodnih izdelkov se pokažejo konkurenčne prednosti VPN kripto-modula C1S pred podobnimi izdelki na trgu ter možnosti za izboljšave.

1 *Projekt »Varnostna testiranja v razvoju in produkciji kripto-modula« je potekal pod okriljem javnega razpisa »Po kreativni poti do praktičnega znanja«, ki so ga financirali Javni sklad Republike Slovenije za razvoj kadrov in štipendije, Ministrstvo za izobraževanje, znanost in šport ter Evropska unija iz Evropskega socialnega sklada.*

Pri projektu sta kot vodji sodelovala dr. Igor Bernik s Fakultete za varnostne vede in Milan Bunjevac s podjetja Miška, d. o. o., ter mag. Boštjan Knap in Blaž Malneršič kot strokovna mentorja s podjetja Miška, d. o. o.

Pri projektu so kot izbrani študenti dodiplomskih in podiplomskih študijskih programov na Fakulteti za varnostne vede sodelovali Anže Zaletel, Jaka Žužek, Lavra Horvat, Katja Zupan, Nina Goršič, Sara Železnik, Maruša Lipušček, Tina Slavec, Nina Gašparut in Matic Volk.

Predlagane so različne ergonomične oblike izdelka glede na ciljne skupine kupcev. Opis možnih testiranj, ki so potrebna za VPN kripto-modul C1S, poda okvirno predstavo o obsegu preizkušanj slehernega tehnološkega izdelka.

Izvirnost/pomembnost prispevka:

Glede na povišan trend zlorab v kibernetskem prostoru je področje kibernetske varnosti, v katerega spada tudi VPN kripto-modul C1S, izrednega pomena. Za ustrezno delovanje kripto-modulov in doseganje pričakovanj uporabnikov je te naprave pomembno dobro testirati.

UDK: 004.056

Ključne besede: informacijska varnost, šifriranje podatkov, kripto-modul, testiranje, analiza trga

Security Testing of a Hardware Virtual Private Network Crypto Module

Purpose:

The purpose of the paper is to present security testing approach in the phase of development and production of a hardware crypto-module, which is indispensable before the product goes on the market. The project work was focused on the product Code 1 Secure (from here on VPN crypto module C1S) for which a comparison with other similar products was made, different ergonomically designed shapes were proposed and product's necessary testing to gain certificates or/and achieve certain standards was described.

Methods:

A descriptive method with the study of primary and secondary sources was used. For the purposes of showing how the automated testing tools work, several testing activities were made.

Findings:

Testing the software and software's compatibility with encryption algorithms poses the most difficult part of all the testing activities needed to be done. The collaborative web portal had a major role in keeping track and progress of the project's work. Testing some of the automated tools showed that their usage saves time and consequently money.

Research Limitations/Implications:

Because the project work was focused on the product VPN crypto module C1S, all the findings are linked to it. However, most of them could be applied to related products.

Practical Implications:

Comparison of similar products shows competitive edge of VPN crypto module C1S and points out potentials for improvements. There were some ergonomically designed shapes presented with the intention of targeting certain costumers. Description of potential testing needed for the C1S, gives a rough estimate of testing's scope of every technological product.

Originality/Value:

VPN crypto-module is a subject of cyber security which has a great importance in everyday life, because of the increased trend of abuses in cyberspace. For the proper functioning of the crypto-modules and meet the expectations of the users, these devices must be appropriately tested.

UDC: 004.056

Keywords: information security, encryption, crypto-module, testing, market analysis

1 UVOD

Vse oblike varnostnih groženj, prisotnih v kibernetskem prostoru, so v porastu in predstavljajo vedno večjo nevarnost za različne vrste informacij in informacijskih sistemov, pomembnih tako za države, organizacije, podjetja kot posameznika (PwC, 2014). Ena izmed rešitev za zagotavljanje večje varnosti in zaščite informacij, ki se izmenjujejo preko kibernetskega prostora, predstavlja uporaba različnih metod šifriranja podatkov in uporaba navideznega zasebnega omrežja (angl. *Virtual private network – VPN*), ki s pomočjo tunelskih protokolov (npr. L2TP/IPSec ali PPTP) (Microsoft, 2003) omogoča vzpostavitev šifrirane povezave med dvema točkama izmenjevanja podatkov preko kibernetskega prostora. S šifriranjem na nižjih nivojih ISO/OSI in TCP/IP protokol prenosa podatkov se uporabnik kibernetskega prostora zaščiti pred grožnjami, ki so prisotne na višjih nivojih (predvsem na aplikacijskem nivoju), in s tem zagotovi zaščito informacij pred nepooblaščenim dostopom (Senetas, 2013) ter posledično večjo zaupnost, celovitost in razpoložljivost informacij, ki predstavljajo ključne elemente CIA triade. CIA triada (angl. *Confidentiality, Integrity in Availability triad*) predstavlja tri najpomembnejše principe informacijske varnosti, ki bi morali biti zagotovljeni v vsakem varnem informacijskem sistemu (Dimov, 2013).

Kripto-moduli za navidezno zasebno omrežje predstavljajo visok nivo zaščite informacij, zaradi česar bi jih bilo smiselno uvajati tako v poslovno kot osebno okolje uporabnikov pri interakciji s kibernetskim prostorom. Kripto-moduli uporabljajo različne šifrirne algoritme za zaščito podatkov in informacij ter uporabniku nudijo možnost izbire med standardnimi šifrirnimi algoritmi (npr. AES, 3DES, RSA ...) ali namestitvijo manj standardnih šifrirnih načinov zaščite podatkov (npr. Blowfish, Serpent, ECC ...). Prednost uporabe fizičnih kripto-modulov za navidezno zasebno omrežje pred programskimi rešitvami je v njihovi zmožnosti zagotavljanja naključno izbranih šifrirnih ključev. Programske rešitve za šifriranje podatkov, uporabljajo psevdo naključno generiranje števil. To pomeni, da so naključno izbrana števila pravzaprav vnaprej določena z matematično formulo, medtem ko so resnično naključno generirana števila izbrana s pomočjo naključnih naravnih pojavov. Med omenjene naravne pojave sodijo fizični pojavi, kot so na primer atmosferski ali ostali šumi, ki se pojavijo ob vklopu kripto-modula (Haahr, 2015).

Kripto-moduli za navidezno zasebno omrežje predstavljajo varnostno rešitev za tako imenovano E2EE šifriranje (angl. *End to end encryption*). Ta uporabnikom

na preprost in transparenten način zagotovi varno prenašanje informacij v kibernetskem prostoru od izvora do prejemnika, tj. naprave, na katero je v tistem trenutku priklopljen kripto-modul za navidezno zasebno omrežje. Na takšen način se uporabniki zavarujejo pred izgubo informacij zaradi kibernetskih groženj, kot je na primer prisluškovanje na omrežju. Kripto-moduli za navidezno zasebno omrežje, ki dosledno upoštevajo standarde iz družine FIPS 140 ter pridobijo ustrezen certifikat, so primerni za uporabo tudi pri prenosu tajnih informacij. FIPS 140 so ameriški računalniški standardi, ki določajo zahteve za izdelavo fizičnih in programskih kripto-modulov (National Institute of Standards and Technology, 2016). Sledenje omenjenim standardom zagotavlja najvišjo stopnjo zaščite pred kibernetskimi grožnjami, zato so kripto-moduli za navidezno zasebno omrežje primerni za prenos vseh vrst zaupnih in tajnih podatkov preko kibernetskega prostora.

V nadaljevanju so predstavljene ključne ugotovitve skupnega študentskega projekta Fakultete za varnostne vede Univerze v Mariboru in podjetja Miška, d. o. o., z naslovom *Varnostna testiranja v razvoju in produkciji kripto-modula*. Ugotovitve se nanašajo tako na področje analize tveganj celotnega projekta, patentiranja in certificiranja kripto-modula, primerjave s sorodnimi kripto-moduli kot na testiranje programske in strojne opreme ter obrazložitve testnega scenarija primernega za poljuben kripto-modul za navidezno zasebno omrežje.

2 ANALIZA TVEGANJ

Za uspešno sodelovanje pri razvojnem projektu smo predhodno izvedli analizo tveganj njegove izvedbe. Zbrali smo številna možna tveganja in proučili načine zaščite. Izračun verjetnosti tveganj in težo posledic, če se tveganja uresničijo, prikazuje tabela 1.

Verjetnost/pogostost tveganj Teže posledic	A – Zelo pogosto	B – Pogosto	C – Redko	D – Izjemoma
1 – Zelo majhne posledice	A1-III.	B1-IV.	C1-IV.	D1-IV.
2 – Majhne posledice	A2-II.	B2-III.	C2-III.	D2-IV.
3 – Večje posledice	A3-I.	B3-II.	C3-II.	D3-III.
4 – Hude/težke posledice	A4-I.	B4-I.	C4-I.	D4-II.

Tabela 1: Metodologija ocenjevanja tveganj z nivoji tveganja (I. –IV.)

Po izbrani metodi (Slak, 2009) I. nivo tveganja zahteva – takojšnje ukrepanje, II. nivo – ukrepanje, III. nivo – spremljanje, IV. nivo – je sprejemljiv. Izračunali smo tudi verjetnost pregledanih tveganj ter težo posledic, če se ranljivosti uresničijo. Za specifična tveganja smo podali lastnike tveganj, tiste osebe, ki morajo poskrbeti, da se tveganja ne uresničijo, ter časovne roke, ki predstavljajo omejitev za dosego zaščite pred tveganji. Tveganja smo v nadaljevanju prve faze projekta razdelili na tri skupine:

- človeški viri,
- procesi in
- IT infrastruktura.

Zatem smo tveganja nadaljnje razvrstili na takšna področja, s katerimi smo lahko preverili verjetnost tveganj in njihovih posledic, obenem pa opredelili zaščito pred njimi na način, kot je razviden v tabeli 1. Za posamezna tveganja ugotavljamo, da zelo pogosto predstavljajo tveganje ob delu na projektu. Ta tveganja imajo v primeru uresničitve hude posledice, zato je bilo za njih treba predvideti takojšnje ukrepanje. Lastnika tveganj sta bila mentorja projekta, ki sta imela nadzor nad izvajanjem projekta, hkrati pa odgovornost, da ta poteka za vse sodelujoče ter po predvidenem načrtu. Postavili smo roke za vzpostavitev definiranih zaščit. Pogosto so bili roki že pred izvedbo prvih nalog, saj smo le preko zaščit, kot je spletni portal ali ustrezno delegiranje nalog na posamezne člane, lahko mirno in kakovostno izvajali projekt. Tak primer je izobraževanje študentov na področju testiranj izdelka in ostalih nalog, kjer je bilo izobraževanje potrebno. Rezultat analize tveganj je ugotovitev, da je komunikacija med udeleženci, najpomembnejši proces in hkrati zaščita za večji del tveganj. Do uresničitve konkretnih tveganj in groženj ni prišlo prav zaradi dobre priprave na projekt.

3 ANALIZA TRGA

Namen primerjave na trgu dostopnih primerljivih kripto-modulov je analiza konkurence in spoznanj o trgu. To nam je v pomoč pri pridobivanju podatkov in kasnejšem odločanju za zmanjševanje tveganja in razvijanje novih, dodatnih idej, ki podjetju ohranjajo konkurenčnost na trgu (Mesojedec et al., 2015). Pri primerjavi primerljivih kripto-modulov je končna ugotovitev ključnega pomena za razvoj novega produkta, ki mora ob prihodu na trg imeti konkurenčne prednosti in s tem možnosti za ohranitev na trgu. Poznavanje lastnosti načrtovanega kripto-modula in njegovega namena je izhodišče primerjave. Pomembno je vedeti, kaj primerjamo; lastnosti, ki jih ima podjetje v načrtu vgraditi v produkt z namenom, da bi z ugotovitvami pri analizi trga predvideli, ali so načrtovane lastnosti konkurenčne in dejansko pomembne za končnega uporabnika – skladno s tem se lastnosti prilagaja ali spreminja. Nekatere od lastnosti, ki so v primeru prenosljivega kripto-modula za navidezno zasebno omrežje pomembne:

- Prenosljivost (teža in dimenzije) – manjši in lažji je kripto-modul, boljša je prenosljivost.
- Število in vrsta priključkov – povezava kripto-modula na druge naprave; koliko naprav lahko naenkrat povežemo in kateri priključki so najpogostejši ter najbolj uporabni pri povezljivosti.
- Izmenjava ključev in šifrirni algoritmi – zelo pomembno z vidika varnosti, predvsem za boljši nadzor nad kripto-modulom.
- Avtentikacija – potrditev, da kripto-modul uporablja samo pooblaščena oseba.
- Ergonomičnost – ravnovesje med kakovostjo izdelka, njegovo učinkovitostjo, zapletenostjo in uporabnostjo kripto-modula.
- Certificiranje – certifikacijski znak na proizvodu potrošnikom, trgovcem in pristojnim organom zagotavlja, da je izdelek skladen z zahtevami veljavnih harmoniziranih standardov.

Glede na omenjene lastnosti primerjave in cen sorodnih kripto-modulov na trgu se določijo potrebne, in za uporabnika koristne, lastnosti za optimalno

izdelavo in končno rabo izdelka. To je vodilo za nadaljnje raziskave in razvoj konkurenčnega ter uporabnega kripto-modula. Primerjava različnih produktov je razvidna v tabeli 2 (primer primerjave petih produktov), kjer smo med izvajanjem projekta primerjali 29 različnih produktov z lastnostmi, ki so zapisane zgoraj.

IME PRODUKTA	Država izvora	CENA	Max prepustnost VPN	Max število VPN tunelov	Podprti protokoli varnih VPN	Šifrirni algoritmi	Dimenzije D x Š x V (mm)	Teža (g)
Miška d. o. o. + Beyond Semiconductor d. o. o.								
Code 1 Secure	Slovenija	/	470 Mbps	32	IPSec	AES128/192/256, lahko dodaš svoje	/	/
TUTUS								
Färist Micro A300	Švedska	1200 EUR	10 Mbps	/	lasten mehanizem (modificiran SSL)	AES256, 3DES, lahko dodaš svoje	115 x 77 x 27	150
Tiny Hardware Firewall								
Belisarius	ZDA	48 EUR	7 Mbps	1	SSL (OpenVPN)	AES256	91 x 43 x 25,85	85
ZyXEL								
ZyXEL ZyWALL 310	Tajvan	570 EUR	500 Mbps	200 (IPsec), 50 (SSL)	IPSec in SSL	3DES	430 x 250 x 44	4626
BORDOTEK								
IP VPN ENCRYPTION HC-7825 10/20/100 MEGABIT VERSION	Švica	/	100 Mbps	250	/	HCA-480	444 x 260 x 44 mm	4200

Tabela 2: Primerjava sorodnih produktov (vir: Bordotek, n. d.; Tiny Hardware Firewall, n. d.; Tutus: Digital Gatekeepers, 2010; ZyXEL, 2016;).

Nekateri kripto-moduli so namenjeni (fizičnemu) prenosu, podobno kot VPN kripto-modul C1S, nekateri so narejeni v stacionarne namene za velike organizacije, nekateri so bolj »ceneni«. Vsi najdeni produkti opravljajo isto nalogo, vendar se razlikujejo po svojih lastnostih. Ugotavljamo, da je VPN kripto-modul C1S naprava, ki je konkurenčna ostalim, trenutno dostopnim produktom na trgu.

3.1 Ergonomski model kripto-modula za navidezno zasebno omrežje

Ergonomičnost pri kripto-modulu za navidezno zasebno omrežje razumemo kot optimalno ravnovesje med kakovostjo, učinkovitostjo, uporabnostjo ter zunanjim videzom izdelka, zato je ergonomičnost poleg osnovnih funkcionalnosti ena izmed ključnih lastnosti pri lansiranju produkta na trg. Kripto-modul je lahko po karakteristikah izjemen in cenovno konkurenčen, pa zaradi neustrezne ergonomije ni tržno uspešen. Iščemo pravo ravnovesje med kakovostjo, učinkovitostjo in uporabnostjo kripto-modula. Sestavni del kakovosti predstavljajo tudi standardi in certifikati. Le-ti so za mnoge organizacije velik finančni izziv. Glede na opravljeno analizo trga so si kripto-moduli na področju ergonomičnosti izredno podobni. Gre za tehnološko zahtevne izdelke, pri katerih je učinkovitost delovanja ter varnost

prenosa podatkov pomembnejša od samega zunanjega videza. Zagotovo pa ne smemo na račun »prijetnega« fizičnega oziroma vizualnega videza ter majhnosti in s tem prenosljivosti produkta žrtvovati zmogljivosti kripto-modula.

Po analizi sorodnih izdelkov na trgu sledi oblikovanje ergonomskega modela kripto-modula za navidezno zasebno omrežje. Poglaviten in osrednji cilj pri oblikovanju predlogov je ustvariti takšen kripto-modul za navidezno zasebno omrežje, ki omogoča šifriranje in zaščito podatkov ter ima zanimiv in eventualno drugačen dizajn. Namen je dati obliko izdelku, z upoštevanjem skladnosti med funkcionalnostjo, estetiko in tehnološkim procesom (Slovar slovenskega knjižnega jezika, 2014). Zato smo želeli z lastnim oblikovanjem predlogov za kripto-modul za navidezno zasebno omrežje in pripadajoče dodatne opreme prikazati, da se pri razvoju izdelka VPN kripto-modula C1S lahko z različnimi oblikami približamo široki množici ljudi – tako domačim kot poslovnim uporabnikom, ki varnost in morebitno tajnost podatkov postavljajo na prvo mesto.

Pripravili smo šest predlogov oblik VPN kripto-modula C1S:

- **C1S Mouse** zadošča potrebam o prenosljivosti, majhnosti in nizki teži samega produkta. Oblika miške je inovativen in hkrati zelo uporaben, saj za vnašanje kode PIN ne potrebujemo dodatne tipkovnice.
- **Premični C1S** je zasnovan z več različnimi vhodi (mrežni UTP priključek, direktni USB in dodatni vhodi za mikro USB).
- **C1S Multi** omogoča priklop več računalnikov oziroma uporabnikov na en kripto-modul za navidezno zasebno omrežje, ki ga upravlja ena oseba. Omenjeni produkt je odlična izbira za podjetja in organizacije, saj med drugimi prednostmi predstavlja tudi nižji strošek.
- **C1S USB Edition** predstavlja najmanjšo različico kripto-modula, ki v celoti ustreza kriterijem o prenosljivosti.
- **C1S Kids** je inovativna oblika kripto-modula, ki smo si ga zamislili za potrebe ozaveščanja mladih o varnosti na internetu ter seznanjanja mlajših otrok (vrtec, prva triada osnovne šole) o pomembnosti šifriranja.
- Pod dodatno opremo smo umestili še silikonske pokrovčke, tako imenovane **C1S Fashion**, ki s svojo barvitostjo in modnim (barve, razni junaki ...) videzom ciljajo na najširšo populacijo končnih uporabnikov. Pokrovčki nimajo zgolj estetske funkcije, temveč kripto-modulu za navidezno zasebno omrežje nudijo tudi dodatno zaščito.

Produkt VPN kripto-modul C1S je v osnovi namenjen zagotavljanju varnosti posredovanih in prejetih podatkov in je po vseh lastnostih konkurenčen trenutno dostopnim produktom na trgu, kot je razvidno iz tabele 2 v prejšnjem odstavku.

4 TESTIRANJE VPN KRIPTO-MODULA C1S

Testiranje izdelka, kot je VPN kripto-modul C1S, je zahteven proces, ki ga sestavlja več vrst testiranj. Ta se zgodijo na različnih ravneh delovanja izdelka in na različnih stopnjah razvoja. Večino testnih procesov je treba ponavljati v vseh fazah razvoja izdelka, saj je le tako mogoče preprečiti napake in zmanjšati stroške razvoja produkta.

4.1 Programsko testiranje

Programsko testiranje je proces, s katerim poskušamo prikazati, da v programski opremi, ki jo programiramo, ni napak (Mayers, 2004). Gre za izvajanje oziroma vrednotenje programa ali zgolj komponent z namenom, da se preveri, ali program ustreza zahtevam oziroma, da se prikaže razlika med pričakovanimi in dejanskimi izhodnimi vrednostmi (Dogša, 1993). S testiranjem tako lahko prikažemo zgolj prisotnost posameznih napak, nikakor pa ne moremo dokazati njihove odsotnosti. Pri testiranju se tako izvajajo testni scenariji, s katerimi se preverja specifične funkcionalnosti izdelka. Dejstvo pa je, da ni mogoče v celoti trditi, da je izbrani izdelek popolnoma brez napak. Nobenega sistema se ne da testirati v popolnosti, saj za to obstajajo teoretične omejitve. Ne omejujejo pa nas zgolj teoretične, temveč tudi praktične omejitve, saj se pri testiranju srečujemo z omejenim časom in omejenimi stroški. Zaradi omejenosti je tako potrebno razumno ravnanje z napakami (Lončarić et al., 2015). Najprimernejši metodi testiranja programske opreme VPN kripto-modula C1S sta se po analizi izkazali metodi črne in bele škatle (angl. *White and black box testing*). Pri testiranju po metodi črne škatle nimamo vpogleda v interno strukturo produkta, testiramo le funkcionalnosti produkta – ali se vneseni podatki skladajo s pričakovanimi izhodnimi podatki. Pri testiranju po metodi bele škatle poznamo notranjo strukturo in vse algoritme, po katerih deluje izdelek. Pri testiranju po metodi bele škatle torej določimo vhodne podatke ter tudi pričakovane, pravilne izhodne podatke (British Computer Society Specialist Interest Group in Software Testing (BCS SIGIST), 2001). Poleg omenjenega pa smo kot primerno, a nekoliko manj ključno ocenili tudi dinamično testiranje in testiranje po metodi sive škatle (angl. Gray box testing), kar pomeni, da mora oseba, ki opravlja test, vsaj delno poznati delovanje notranje strukture in algoritmov (Khan in Khan, 2012).

Testiranja, ki jih je treba izvajati v posameznih komponentah kripto-modula, predstavljajo osnovo oziroma stopenjsko testiranje programske opreme, ki je razvidno v tabeli 3.

Vrsta testiranja	Opis
Testiranje enot in modulov	*Test enot je metoda testiranja programske opreme, pri kateri se osredotočamo na posamezno enoto ali posamezen del programske kode.*
Integracijsko testiranje	*Z integracijskim testom želimo preveriti funkcionalnosti, zmogljivosti in zanesljivosti ključnih delov programske opreme.*
Sistemsko testiranje	*Sistemsko testiranje je metoda testiranja programske opreme, kjer se osredotočamo na celoten integriran sistem. Namen sistemskega testiranja je preveriti skladnost sistema z zahtevami, ki so bile predhodno določene v dokumentaciji.*
Testiranje sprejemljivosti	*Testiranje sprejemljivosti je metoda testiranja programske opreme, ki predstavlja zadnje testiranje pred predajo programske opreme v uporabo naročniku. Programska oprema, ki uspešno prestane test sprejemljivosti, naj bi ustrezala skoraj vsem zahtevam, ki jih je izpostavil naročnik oziroma razvijalec programa.*
Testiranje komponent vmesnika	*Testiranje komponent vmesnika je metoda testiranja programske opreme, ki se uporablja za preverjanje ravnanj s podatki med različnimi enotami ali komponentami. Namen te vrste testiranja je najti napake vmesnikov in napake v predpostavkah, povezanih z vmesniki.*

Tabela 3: Osnovna oziroma stopenjska testiranja programske opreme (vir: Kuzem, 2011).

Tabela 3: Nadaljevanje

Vrsta testiranja	Opis
Sistemsko integracijsko testiranje	*Pri omenjenem testiranju se pod drobnogled vzame več integriranih sistemov, ki so prestali sistemsko testiranje, hkrati pa se preveri tudi, kako delujejo zahtevane interakcije med samimi sistemi.*
Regresijsko testiranje	*Regresijsko testiranje je metoda testiranja programske opreme, ki se uporablja v primerih, ko se programska koda večkrat spremeni. Z omenjenim testiranjem tako preverjamo, ali so uvedene spremembe botrovale k nastanku novih napak, prav tako pa se s testiranjem iščejo napake, ki so bile v prvotni fazi odpravljene, a so se zaradi spremenjene kode zopet pojavile.*

V široki paleti testiranj, ki jih lahko izvajamo na končnem produktu, smo izbrali testiranja, prikazana v tabeli 4.

Tabela 4: Testiranja, ki jih izvajamo na končnem produktu (vir: Software testing, 2015).

Vrsta testiranja	Opis
»Smoke and sanity« testiranje	*»Smoke« testing pomeni predhodno testiranje, s katerim iščemo preproste napake, ki bi lahko bile tako hude, da bi onemogočile izdajo programske opreme. »Sanity« test je osnovni test za hitro ugotavljanje, ali so rezultati izračunov resnični. Pri tem testu se preverja programska koda in njena funkcionalnost.*
Testiranje povezljivosti	*Testiranje povezljivosti je sistemsko testiranje, ki preverja skladnost aplikacijske rešitve z njenimi nefunkcionalnimi zahtevami. Preverjamo torej, kako se je aplikacija zmožna povezati z računalniškim okoljem.*
Namestitveno testiranje	*Pri namestitvenem testiranju ugotavljamo, kaj bodo uporabniki morali storiti za pravilno namestitev in vzpostavitev delovanja programske opreme. Proces testiranja vključuje polno ali delno nadgrajevanje oziroma odstranjevanje programske opreme.*
Varnostno testiranje	*Varnostno testiranje je proces, s katerim se odkrivajo pomanjkljivosti v varnostnem mehanizmu informacijskega sistema, ki varuje podatke.*
Destruktivno testiranje	*Destruktivno testiranje se izvaja z namenom razumevanja strukturne zmogljivosti in vedenja materiala. Destruktivni testi pokažejo, v kakšnih razmerah in ob katerih dogodkih izdelek še deluje in kje pride do okvare ali napake v programski kodi.*
Beta testiranje	*Uporabniki, ki prejmejo beta različico programske opreme, poročajo razvijalcem o prisotnosti hroščev, na katere so naleteli, kar omogoča programskim razvijalcem lažje in hitrejše odpravljanje teh težav.*
Test uporabnosti	*Test uporabnosti se navezuje na testiranje sprejemljivosti, in sicer s testom uporabnosti preverimo, ali je uporabniški vmesnik lahek za uporabo ter razumljiv.*

Testiranja, ki bi jih bilo prav tako smiselno izvesti, vendar niso primarnega pomena, so prikazana v tabeli 5.

Tabela 5: Testiranja, ki bi jih bilo smiselno izvesti za VPN kripto-modul C1S (vir: Software testing, 2015).

Vrsta testiranja	Opis
Razvojno testiranje	*Razvojno testiranje je programsko-razvojni proces, ki vključuje sinhronizirano dodajanje širokega spektra procesov za preprečevanje napak in strategij za odkrivanje napak z namenom zmanjšanja tveganj, časa in stroškov pri razvoju programske opreme.*
A/B testiranje	*Princip delovanja A/B testiranja je preprost in temelji na tem, da imamo identična programa (A in B), pri katerih tekom testiranja spreminjamo različne spremenljivke in nato spremljamo odziv programov na nove (različne) spremenljivke.*
Testiranje delovanja programske opreme	*Testiranje delovanja programske opreme predstavlja testiranje, ki odgovori na vprašanje, kako sistem ali podsistem deluje v odzivnosti in stabilnosti, kadar je pod določeno delovno obremenitvijo.*
Testiranje po specifikacijah	*Testiranje po specifikacijah je testiranje, s katerim se ugotavlja skladnost izdelka z zahtevami specifikacij, pogodbe ali uredbe.*
Hkratno testiranje	*Hkratno testiranje predstavlja testiranje, ki določa stabilnost sistema ali aplikacije, kadar je izpostavljena normalnemu delovanju.*
Alfa testiranje	*Alfa testiranje je metoda testiranja programske opreme, kjer gre za simulirane oziroma dejanske operativne teste, ki so izvajani s strani potencialnih uporabnikov oziroma neodvisnih testnih skupin s strani razvijalca.*

Pri programskem testiranju so pomembni tudi procesi testiranja, ki so nekakšna osnova nadaljnjega razvoja produkta. Od obstoječih tipov tovrstnega testiranja so za izdelek VPN kripto-modul C1S najprimernejše agilne metoda (angl. *Agile software development*), čeprav je za testiranje primerna tudi uporaba tradicionalnih metod (npr. slapovni razvoj programske opreme). Ekstremno programiranje, kot ena izmed agilnih metod, je zaradi svojega načina delovanja na prvi pogled neprimerno za testiranje VPN kripto-modula C1S, vendar je ob sledenju modelom za prepoznavanje groženj (npr. Microsoft STRIDE) primerno tudi za testiranje in razvoj varne programske opreme (Bolboaca in Bolboaca, 2014; Microsoft, 2016). Pri delu s programsko kodo je uporabno tudi avtomatizirano testiranje, ki preverja predvsem delovanje osnovnih in manj zahtevnih funkcij. Pri VPN kripto-modulu C1S bi se za to vrsto testiranja lahko odločili pri testiranju grafičnega uporabniškega vmesnika ter pri testiranju programske kode in vmesnika za programiranje (Software testing, 2015). Vsi tipi programskega testiranja, primernih za VPN kripto-modul C1S, so predstavljeni v tabelah 3, 4 in 5.

Ko združimo skupaj različne stopnje in tipe testiranj, vidimo, da je celoten proces testiranja, od začetkov pisanja programske kode do uporabe končnega produkta, kompleksen in zahteven. V samem procesu testiranja programske opreme morajo sodelovati tako razvijalci opreme, testni inženirji kot končni uporabniki, saj le s sodelovanjem vseh akterjev izdelamo program ali izdelek, ki je primeren za uporabo na trgu.

Pri testiranju programske opreme je treba omeniti še samotestiranje, ki ga kripto-modul izvaja po priporočilih standarda FIPS 140-2. Kripto-modul opravi samotestiranje ob vsakem vklopu (angl. *Power-up self-test*) oziroma v primerih, kadar se zažene varnostna funkcija ali operacija, ki zahteva samotestiranje (angl. *Conditional self-test*). V primeru, kadar kripto-modul ne uspe zagnati samotestiranja oziroma je samotestiranje neuspešno, sporoči napako preko vmesnika za javljanje statusa naprave (angl. *Status output interface*). Če je kripto-modul v stanju napake, ne sme izvajati nobenih funkcij ali operacij (National Institute of Standards and Technology, 2001). Samotestiranje je pomemben del testiranja, ki omogoča nemoteno delovanje kripto-modula. Samotestiranje uvrstimo med vse tri tipe testiranj, ker zajema tako testiranje programske, strojne opreme ter kode nameščene na strojni opremi.

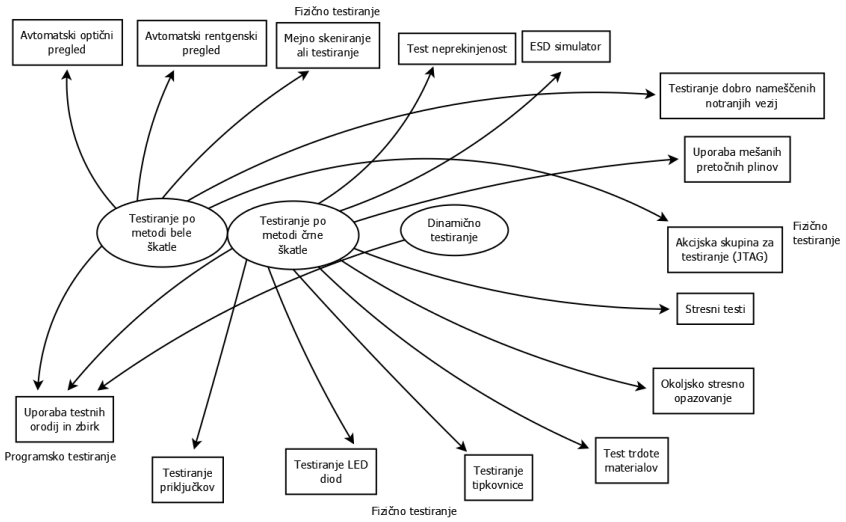
4.2 Testiranje strojne opreme

Za zagotavljanje celovitosti pri delovanju VPN kripto-modula C1S pred končnim lansiranjem izdelka na trg je treba poleg programskega testiranja opraviti tako imenovano testiranje strojne opreme. Testiranje strojne opreme poteka podobno kot ostale vrste testiranj, le s to razliko, da so testiranja osredotočena primarno na fizično delovanje strojne opreme. Kot je razvidno iz slike 1, sta za potrebe VPN kripto-modula C1S primerni metodi testiranja po metodi bele in črne škatle, ki omogočata:

1. Preverjanje delovanja priključkov – preverimo, ali mikro USB in UTP priključki delujejo tako, kot to zagotavlja njihov proizvajalec (Global Sources, n. d.).

2. Testiranje LED diod – s programom ali s pomočjo digitalnega multimetra testiramo delovanje diod.
3. Testiranje tipkovnice – za fizično testiranje pritiskov na tipkovnici se uporabljajo avtomatizirani testni roboti (TRICOR Systems, n. d.).
4. Stresne teste – testiranje v pogojih izven zmogljivosti produkta, pogosto blizu točke zloma (angl. *breaking point*) (Stress testing, 2015).
5. Akcijska skupina za testiranje (JTAG) ali IEEE 1149.1 standard – testiranje pinov na tiskanih vezjih (Altera Corporation, 2007).
6. Uporaba testnih orodij in zbirk – uporaba programov za testiranje strojne opreme.

Slika 1: Metode testiranja strojne opreme



Na sliki 1 je s puščicami ponazorjena primernost uporabe posameznih tipov testiranj, ki niso omenjeni v zgornjih alinejah. Zadnji tip testiranja, ki prav tako pripomore k celovitosti delovanja kripto-modula, predstavlja testiranje kode, nameščene na strojni opremi (angl. *Firmware*). Kot je znano, nam VPN kripto-modul C1S omogoča šifriranje s šifrirnimi standardi AES128/192/256 ter možnostjo dodajanja lastnih šifrirnih algoritmov. To pomeni, da lahko uporabnik kripto-modulu dodaja poljubne šifrirne algoritme, ki nadomestijo AES. Zaradi teh dveh vrst kode na strojni opremi kripto-modula je treba opraviti določena testiranja, ki zagotavljajo, da koda in same komponente delujejo tako, kot od njih pričakujeta proizvajalec in uporabnik. Najboljša možnost testiranja takega tipa opreme je z uporabo testiranja po metodi bele škatle, in sicer z uporabo programskega testiranja, pri katerem uporabljamo uporabo testnih orodij in/ali zbirk s KAT, MMT in MCT testi, ki se uporabljajo predvsem za testiranje šifrirnih algoritmov (Bassham III, 2002).

5 TESTNE METODE ZA EN MODUL

S pomočjo testiranja lahko pravočasno popravimo napake tako na strojni (mehanske oziroma tehnične nepravilnosti) kot na programski (»hrošči«) opremi. Za uspešno izvedbo samega testiranja moramo natančno opredeliti in predvideti testne scenarije. Zaradi obsežnosti naloge in omejenosti s časom smo se osredotočili na pisanje testnih scenarijev za spreminjanje imena naprave oziroma »Hostname«. V okviru projekta smo pripravili 24 testnih scenarijev. Iz tabele 6 je razviden primer enega testnega scenarija.

Tabela 6: Primer enega testnega scenarija

Testni scenarij	Element	Cilj testnega scenarija	Podrobna razlaga	Visokonivojski opis	Pričakovan rezultat
TC_GUI_ HostName_V-01	Hostname	Vnos veljavnega »hostname«	V vnosno polje zapišemo veljavno ime za »hostname« in shranimo spremembe	1. Določi nov »hostname«; omejitve 1 ≤ N ≤ 24, znaki: velike in male črke ASCII ter številke 2. Shrani spremembe	**OK** »Hostname« mora biti spremenjen in shranjen

Ker je testnih scenarijev veliko, je priročno, če testiranje avtomatiziramo. Izvedli smo postopek vizualnega testiranja z orodjem SikuliX. SikuliX je orodje, s katerim avtomatiziramo vse, kar vidimo na zaslonu računalnika. Za identificiranje in upravljanje komponent grafičnega vmesnika se uporablja orodje za prepoznavo slike (Sikuli, n. d.). Preizkusili smo delovanje Robot Framework, ki je generično testno avtomatizirano ogrodje za preskušanje sprejemljivosti ter razvoj na podlagi preskusa sprejemljivosti (Robot Framework, 2014). Ugotovili smo, da je prišlo do razlik med orodjema. Na eni strani je SikuliX, preprost za uporabo, na drugi pa Robot Framework, za katerega je potrebno napredno znanje in izkušnje s področja programiranja.

Pri vseh testih moramo stvari tudi ustrezno beležiti. To lahko uredimo s pomočjo sistema za beleženje hroščev (angl. *Bug tracking system*) v programski opremi. Gre za orodje, ki skrbi za beleženje napak testiranj programske opreme, ki je v procesu razvijanja in nadgrajevanja. Lahko gre za odprt sistem, v katerega poročila o napakah beležijo in poročajo tudi končni uporabniki, ali pa gre za zaprt sistem, ki ga uporabljajo samo razvijalci v fazi razvijanja in testiranja programske opreme. Glavna prednost sistema je centraliziran vpogled na zahteve po razvoju in izboljšavah, kot tudi na stanje napredka in dela na teh zahtevah. Na podlagi tega se lahko generirajo poročila o produktivnosti programerjev pri popravljanju in odpravljanju hroščev (Techopedia, 2016). Testni proces je nekaj, kar se uporablja skozi celotno življenjsko dobo izdelka.

6 UGOTOVITVE IN ZAKLJUČKI

Za izvedbo večmesečnega projekta in ustrezno testiranja VPN kripto-modula C1S je potrebno dobro usklajevanje sodelujočih. Ta se kaže v ustreznem delegiranju nalog in sprotnem izobraževanju tistih, ki testiranja izvajajo in pripravljajo ter urejajo vmesna in končna poročila. Pomembno stično točko celotnega dela na

projektu predstavlja uporaba skupnega spletnega portala, ki omogoča nemoteno komunikacijo med vsemi sodelujočimi in sprotno beleženje dela ter napredka na projektu. Poleg ustrezne izvedbe analize tveganj je za testiranje pomembno poznavanje sorodnih izdelkov ter primernih testnih metod za konkreten izdelek. S poznavanjem in podrobno analizo sorodnih izdelkov je lažje določiti testne scenarije in testne metode. S tem korakom pri testiranju poskrbimo za optimalno izrabo časa in sredstev. Poleg primerjave s sorodnimi izdelki je testerjem omogočen prihranek časa in sredstev s preverjanjem testnih specifikacij, ki jih za vgrajene komponente opravijo proizvajalci. Kot primer vzamemo USB priključke, LED svetila in tipkovnico kripto-modula za navidezno zasebno omrežje, ki so testirana s strani proizvajalca, zaradi česar testiranje teh komponent, kot del testiranja strojne opreme, ni potrebno. Seveda je v teh primerih obvezna izbira zanesljivega in preverljivega proizvajalca posameznih komponent.

Najzahtevnejši del celovitega testiranja predstavlja testiranje programske opreme in šifrirnih algoritmov, posebno tistih, ki jih uporabnik sam namesti na kripto-modul. Testiranje šifrirnih algoritmov, ki spadajo pod kodo, nameščeno na strojni opremi, poteka po standardu FIPS 140-2. To pomeni, da mora kripto-modul zadovoljiti vse potrebe standarda pred lansiranjem na trg. Sledi testiranje programske opreme, ki predstavlja unikaten prispevek posameznih programerjev k delovanju, predvsem uporabniškega vmesnika kripto-modula za navidezno zasebno omrežje. Prav testiranje uporabniškega vmesnika je ena izmed vrst testiranja, ki je lahko avtomatizirano s pomočjo programov npr. SikuliX in Robot Framework. Ugotavljamo, da se s pravilnim postopkom izpeljave avtomatizacije testnih procesov prihranita čas in finančna sredstva, ki bi jih tester oziroma programer porabil ob neavtomatiziranem testnem procesu. Za pravilno delovanje ostale programske opreme, ki je z avtomatiziranim testiranjem ne morem optimalno vključiti v testni proces, je treba uporabiti primerne testne metode. Metodo črne škatle, kadar nas zanimajo le končni rezultati vhodnih in izhodnih podatkov, ali metodo bele škatle, kadar nas zanima celoten cikel potovanja vhodno-izhodnih podatkov.

Ugotavljamo, da je testiranje kripto-modula za navidezno zasebno omrežje kompleksen, vendar nujno potreben proces, ki zagotavlja optimalno delovanje izdelka, kot je VPN kripto-modul C1S. S testiranjem smo odpravili večino napak, kar pomeni, da je na trg lansirani izdelek VPN kripto-modul C1S konkurenčen in zagotavlja izjemno stopnjo varnosti pred grožnjami, prisotnimi v kibernetskem prostoru.

UPORABLJENI VIRI

Altera Corporation. (2007). *IEEE 1149.1 (JTAG) boundary-scan testing for cyclone II devices.* Pridobljeno na http://www.altera.com/literature/hb/cyc2/cyc2_cii51014.pdf

Bassham III, L. E. (2002). *The advanced encryption standard algorithm validation suite (AESAVS).* National Institute of Standards and Technology Information Technology Laboratory Computer Security Division. Pridobljeno na http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

Bolboaca, A. in Bolboaca A. (6. 3. 2014). *Briefly on architecture, extreme programming and security testing.* Agile Record. Pridobljeno na http://www.agilerecord.com/architecture-extreme-programming-security-testing/

Bordotek. (n. d.). *HC-7825m.* Pridobljeno na http://www.bordotek.net/en/brands-listing/product/57-hc-7825-10-20-100-mb-version.html

British Computer Society Specialist Interest Group in Software Testing [BCS SIGIST]. (2001). *Standard for software component testing*. Pridobljeno na http://www.testingstandards.co.uk/Component%20Testing.pdf

Dimov, I. (20. 6. 2013). *Guiding principles in information security*. Infosec Institute. Pridobljeno na http://resources.infosecinstitute.com/guiding-principles-in-information-security/

Dogša, T. (1993). *Verifikacija in validacija programske opreme*. Maribor: Tehniška fakulteta.

Global Sources. (n. d.). *Micro USB connector manufacturer*. Pridobljeno na http://www.globalsources.com/gsol/I/Micro-USB/p/sm/1066479043.htm#1066479043

Haahr, M. (12. 4. 2015). *Introduction to randomness and random numbers*. Dublin: Random.org. Pridobljeno na https://www.random.org/randomness/

Khan, M. E. in Khan, F. (2012). A comparative study of white box, black box and grey box testing techniques. *International Journal of Advanced Computer Science and Applications, 3*(6), 12–15. Pridobljeno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.261.1758&rep=rep1&type=pdf

Kuzem, R. (2011). *Načrtovanje testiranja pri razvoju IS v manjših razvojnih skupinah* (Diplomsko delo). Ljubljana: Fakulteta za računalništvo in informatiko. Pridobljeno na http://eprints.fri.uni-lj.si/1266/1/Kuzem_R._-_diplomsko_delo.pdf

Lončarić, T., Vehovec, A., Kastelic, M., Drofenik, D., Divjak, S., Kavčič, A. et al. (31. 3. 2015). *Upravljanje s programljivimi napravami.* Pridobljeno na http://www.egradiva.net/moduli/programirljive_naprave/01_datoteka.html

Mayers, G. J. (2004). *The art of sotfware testing* (2nd ed.). New Jersey: John Wiley & Sons.

Mesojedec, T., Šporar P., Strojan, K., Valentinčič, T., Bačar, F., Sakovič, G. et al. (2015). *Socialno podjetništvo.* Pridobljeno na http://www.socialni-inovatorji.si/knjiga/socialno-podjetnistvo/44-trzne-raziskave-analiza-trga

Microsoft. (2003). *What is VPN?* Pridobljeno na https://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx

Microsoft. (2016). *The STRIDE threat model*. Pridobljeno na https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

National Institute of Standards and Technology. (2001). *Security requirements for cryptographic modules.* Pridobljeno na http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

National Institute of Standards and Technology. (1. 2. 2016). *Standards.* Pridobljeno na http://csrc.nist.gov/groups/STM/cmvp/standards.html

PwC. (2014). *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015*. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Robot Framework. (2014). *Robot Framework introduction*. Pridobljeno na http://robotframework.org/#introduction

Senetas. (2013). *Understanding senetas layer 2 encryption: Technical paper*. Pridobljeno na http://www.senetas.com/_uploads/files/Technical-Paper_Understanding_Senetas_Layer_2_Encryption.pdf

Sikuli. (n. d.). *Sikuli script*. Pridobljeno na http://www.sikuli.org/

Slak, L. (2009). *Analiza operativnih tveganj OE banke.* Maribor: Nova KBM. Pridobljeno na http://www.isaca.si/datoteke/Analiza_operativnih_tveganj.ppt

Slovar slovenskega knjižnega jezika. (2014). Ljubljana: Založba ZRC; Znanstveno raziskovalni center SAZU. Pridobljeno na http://www.fran.si/130/sskj-slovar-slovenskega-knjiznega-jezika

Software testing. (2015). V *Wikipedia: The free encyclopedia*. Pridobljeno na https://en.wikipedia.org/wiki/Software_testing

Stress testing. (2015). V *Wikipedia: The free encyclopedia*. Pridobljeno na http://en.wikipedia.org/wiki/Stress_testing

Techopedia. (2016). *Bug tracking*. Pridobljeno na http://www.techopedia.com/definition/25910/bug-tracking

Tiny Hardware Firewall. (n. d.). *Tiny Hardware Firewall VPN client*. Pridobljeno na http://tinyhardwarefirewall.com/

TRICOR Systems. (n. d.). *Automated keyboard test system – 921 xy.* Pridobljeno na http://www.tricor-systems.com/products/switch-testers/switch-tester-921xy.htm

Tutus: Digital Gatekeepers. (2010). *Färist Micro.* Pridobljeno na http://www.tutus.se/products/farist-micro.html

ZyXEL. (2016). *VPN firewall: ZyWALL 1100/310/110*. Pridobljeno na http://www.zyxel.com/products_services/zywall_1100_310_110.shtml?t=p

O avtorjih:

Anže Zaletel, diplomirani varstvoslovec, magistrski študent Fakultete za varnostne vede Univerze v Mariboru.

Jaka Žužek, diplomirani varstvoslovec informacijske varnosti.

Lavra Horvat, diplomantka upravnih ved, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Katja Zupan, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Sara Železnik, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Nina Goršič, diplomantka upravnih ved, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.

Maruša Lipušček, diplomirana varstvoslovka, magistrska študentka Fakultete za varnostne vede Univerze v Mariboru.