UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Ocena tveganja informacijskega sistema za nadzor fizičnega dostopa prostorov podjetja RRC d.o.o. s sistemom kartice HID Indala FlexCard

Seminarska naloga pri predmetu Kriptografija in računalniška varnost na mag. podiplomskem študiju

Iztok Starc, univ. dipl. inž. el.

Mentor: prof. dr. Aleksandar Jurišić

Ljubljana, 15. januar 2011

Kazalo vsebine

Uvod

V okviru zadolžitve pri opravljanju predmeta Kriptografija in Računalniška Varnost smo dobili naročilo za oceno tveganja sistema kartice, ki se uporablja za nadzor fizičnega dostopa v prostore podjetja RRC.

Raziskava je poleg tehničnih znanj zahtevala še detektivskego delo, iznajdljivost in nekaj sreče, saj je razpoložljiva literatura o tem sistemu zelo skopa. Kot uporabnik prostorov RRC tudi sami posedujemo kartico in prva sled se je nahajala na sami kartici: »Indala – Špica«. Podjetje Špica se ukvarja s sistemi za nadzor dostopa. Uspelo nam je navezati stik s predstavnikom podjetja in pri poizvedbi glede delovanja sistema smo dobil prijazen odgovor:

»Naj povem, da od proizvajalcev običajno nimamo protokola ki ščiti informacije. Pogosto, so ti protokoli tajni zasebni ali pa patentirani. Za ostale (na primer tehnologija iClass, Legic Advant, Prime) pa smo podpisali NDA in smo zato pogodbeno zavezani molčečnosti. Uporabljamo tudi Mifare tehnologijo, katera pa je dostopna tudi širšemu krogu uporabnikov.«

»Pri vas od leta 2005 uporabljate kartice in čitalce Indala FlexCard, za katere je Chris Paget 2007 odkril pomanjkljivost in možnost kloniranja, vendar mu je objavo članka podjetje HID preprečilo. (sklicevanje na patente) http://www.schneier.com/blog/archives/2007/02/cloning_rfid_ch_1.html«

»Vaš čitalnik uporablja enosmerni protokol wiegand, kateri je vsesplošno sprejet na področju kontrole pristopa. Sam po sebi ni varen, nekoliko se ga da zaščititi pred dostopom s pravilno postavitvijo čitalca ter vgrajenim tamper switchem. http://en.wikipedia.org/wiki/Wiegand_interface«

»Na Špici damo velik povdarek na varnost. V vseh novih proizvodih uporabljamo iClass, ki je zaščiten s 3DES algoritmom, kjub vsemu pa se nekatere stranke še vedno odločijo za ugodnejši in manj varen system, ki ga skušamo opustiti.«[1]

Slika 1: Vzgled kartice HID Indala FlexCard

Od podizvajalca smo dobili iskren odgovor in koristne napotke za nadaljnjo preiskavo. Z zgornjega pisma je prav tako razvidno, da podjetje HID, ki razvija in prodaja sistem HID Indala FlexCard,

[1] Po [22] se izkaže, da je standardna postavitev sistema HID iClass »Standard Security« ranljiva, saj ključ za 3DES ni tajen in je »standarden« v vseh napravah. Ta napaka popolnoma razvrednoti pojem »Standard Security«. Žal, tudi protokol kartice ni brez napake, saj ne pozna overjanja sporočil. To ga izpostavi za napad z možem na sredini v vseh ti. »varnostnih načinih delovanja« HID iClass. V primerjavi je HID Indala FlexCard generacijo starejši produkt HID iClass.

podizvajalce zavezuje k zaupnosti o delovanju in arhitekture sistema s pogodbo o ne razkritju informacij.

Še več, strategija podjetja HID zmanjšanja tveganja razkritja teh dokumentov je uporaba vseh pravnih sredstev. Znan je javno odmeven primer iz leta 2007, ko je pravna služba HID onemogočila objavo ranljivosti in demonstracijo napada na ta sistem [11,25]. Podobne prakse za onemogočanje obveščanje javnosti in javnega interesa najdemo tudi drugod [5,18]. Dodatno, grožnje z visokimi odškodninami odvračajo objavo rezultatov drugih varnostnih raziskav. Le-to pa posledično pomeni, da je dostop do tovrstnih podatkov otežen do te mere, da je javnost o varnostno pomembnih vsebinah slabo obveščena.

Od te točke naprej bomo ta sistem imenovali »*Informacijski sistem za nadzor fizičnega dostopa prostorov podjetja RRC s sistemom kartice HID Indala FlexCard*«.

Namen seminarske naloge

Namen seminarske naloge je:

1. Zajem relevantnih **varnostnih podatkov** informacijskega sistema za nadzor fizičnega dostopa prostorov RRC s sistemom kartice HID Indala FlexCard.
2. Opraviti postopek **ocene tveganja** za določitev informacijske varnosti tega sistema. Proces in metode ocenjevanja tveganja skladno bodo skladne z družino mednarodno veljavnih standardov za načrtovanje, vzpostavitev in revidiranje *sistemov za upravljanje varovanja informacij* (SUVI) – ISO/IEC 2700X [14,15,16,17].

Uporabljen bo pristop preizkušanja črne škatle. Za tak pristop bi se običajno odločil zunanji napadalec ali pogodbeni varnostni strokovnjak, angažiran s strani vodstva podjetja. To posledično pomeni, da zaposleni v podjetju med procesom ocene tveganja ne bodo vedeli, da je preiskava v teku. O oceni tveganja bodo obveščeni po koncu preiskave.

Stopnja zaupnosti dokumenta

To poročilo lahko vsebuje informacije o izpostavljenih sredstvih s pripadajočimi ranljivosti in o postopkih napada za izkoriščanje ranljivosti. Potencialno ogroža vse pravne in fizične osebe, ki uporabljajo in/ali so odvisni od storitev, ki se nahajajo v prostorih podjetja RRC.

To je razlog, da je poročilu dodan znak zaupnosti. Uporaba in razširjanje poročila je zato dovoljena le s soglasjem avtorja in mentorja.

Pregled področja

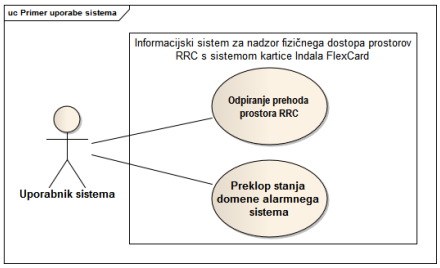
Informacijski sistem za nadzor fizičnega dostopa prostorov RRC s sistemom kartice Indala FlexCard

Opis funkcionalnih lastnosti sistema

Funkcionalnost informacijskega sistema za nadzor fizičnega dostopa prostorov RRC s sistemom kartice HID Indala FlexCard je naslednja:

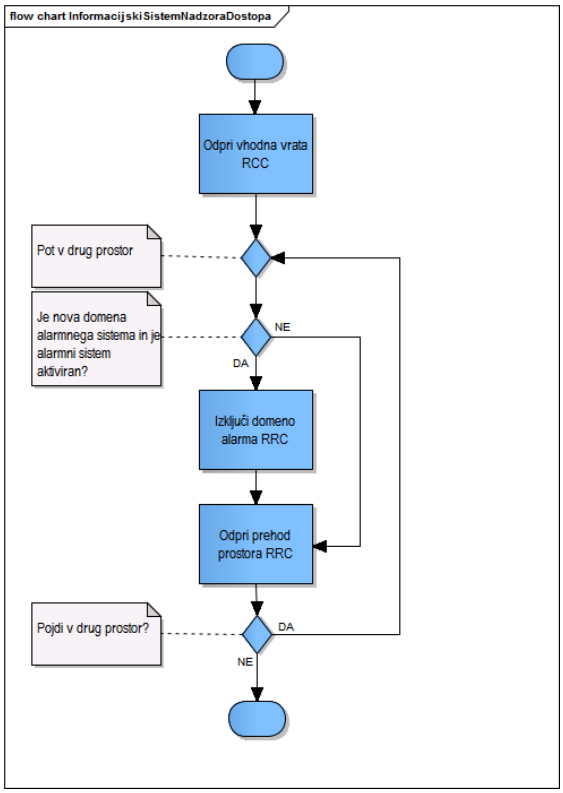
- Odpiranje vrat za prehod v različne prostore RRC.
- Preklapljanje stanja alarmnega sistema.

Za obe operaciji mora uporabnik imeti ustrezne privilegije, ki so zapisani v zalednemu delu sistema. Overjanje in avtorizacija uporabnika poteka na podlagi prenesenega identifikacijskega niza kartice.



Slika 2: Diagram primera uporabe – Primer uporabe informacijskega sistema za nadzor fizičnega dostopa

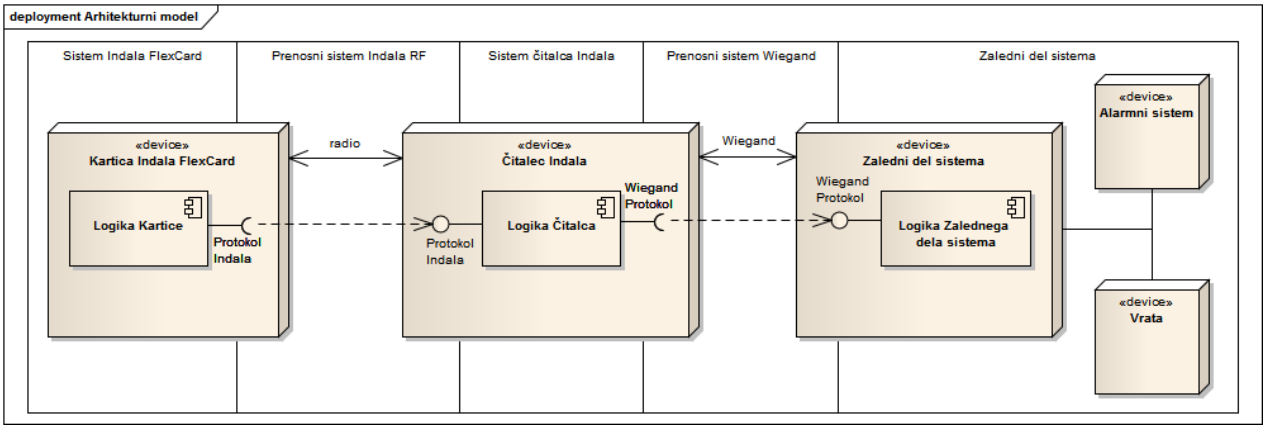
Uporabo funkcionalnosti sistema predstavimo s sledečim diagramom poteka.



Slika 3: Diagram poteka – model obnašanja sistema nadzora dostopa prostorov podjetja RRC d.o.o. s sistemom brezkontaktnih kartic

Arhitekturni model sistema z opisom elementov

Za sistem ne obstaja uradna objava arhitekturnega načrta, zato smo na podlagi naslednjih virov [8,12,20] rekonstruirali arhitekturni model sistem, ki je predstavljen s spodnjim diagramom postavitve. Model obnašanja sistema je predstavljen z diagramom sekvenc (glej Slika 5) in vsebuje obnašanje za oba primera uporabe (glej Slika 2).



Slika 4: Diagram postavitve – 3-tirni arhitekturni model informacijskega sistema za nadzor fizičnega dostopa prostorov RRC s sistemom kartice HID Indala FlexCard

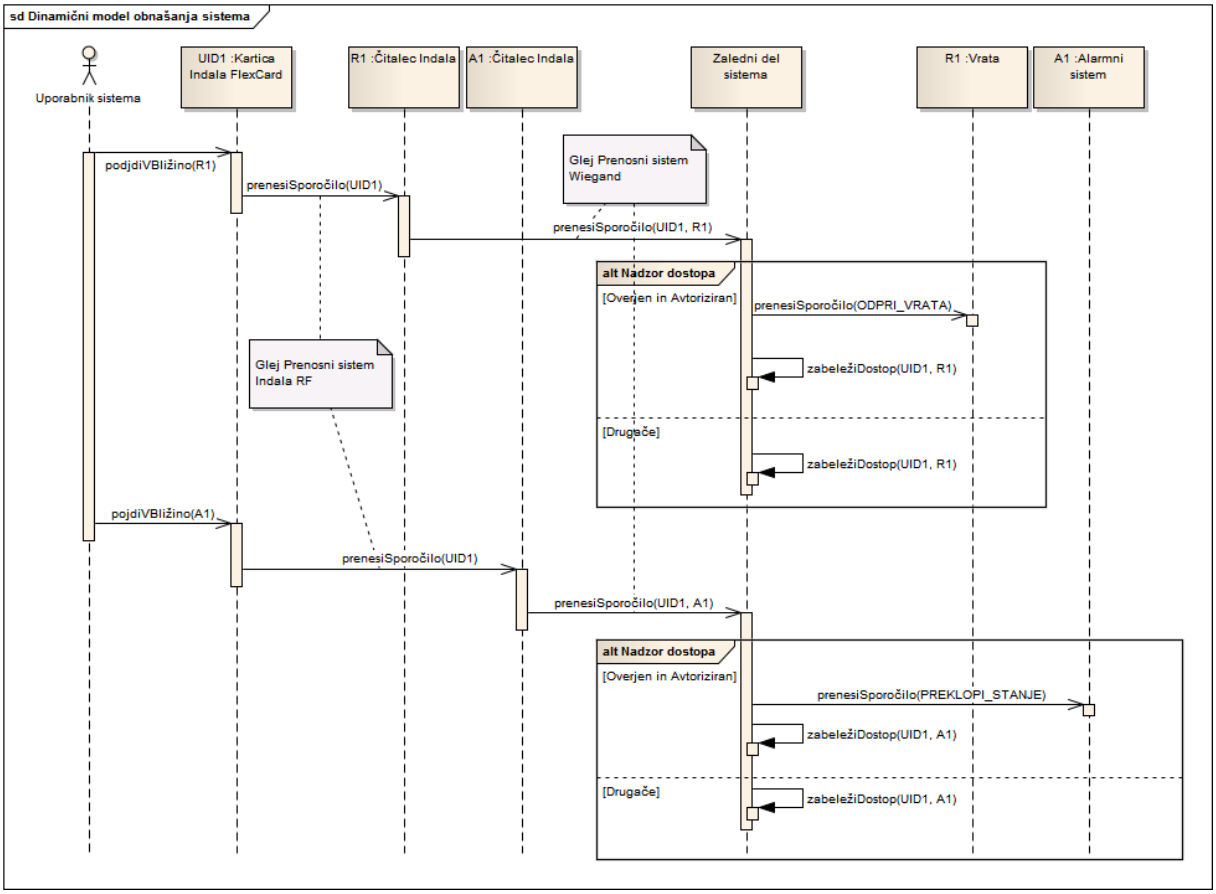
Arhitekturni model razdelimo na pet interesnih področij:

- Sistem kartice HID Indala FlexCard,
- Prenosni sistem Indala RF,
- Sistem čitalca Indala,
- Prenosni sistem Wiegand,
- Zaledni del sistema.

Spodnja tabela prikazuje umestitev porazdeljenega informacijsko-komunikacijskega sistema za nadzor dostopa v model ISO OSI [13]. Na tabelo se bomo sklicevali pri opisu interesnih področij.

Porazdeljeni sistem za nadzor dostopa	Kartica	Čitalec	Čitalec	Zaledni del sistema	Model ISO OSI
Informacijski sistem	Indala FlexCard	Indala FlexCard	Indala Reader	Indala Reader	Aplikacijska plast
	-	-	-	-	Predstavitvena plast
	-	-	-	-	Sejna plast
Transportni sistem	-	-	-	-	Transportna plast
	-	-	-	-	Omrežna plast
Prenosni sistem	N/A	N/A	Wiegand protokol	Weigand protokol	Prenosna plast
	125 kHz, FSK, radio	125 kHz, FSK, radio	Wiegand PHY	Weigand PHY	Fizična plast

Tabela 1: Umestitev informacijsko-komunikacijskega sistema Kartice, Čitalca in Zalednega dela sistem v model ISO OSI



Slika 5: Diagram zaporedja – Model obnašanja sistema glede na arhitekturni model (glej Slika 4) s primerom odpiranja prehoda prostora in preklopom alarmnega sistema

Sistem kartice HID Indala FlexCard

Naloga kartice je hraniti niz identifikacijskih bitov nosilca kartice in izvršiti prenos podatkov, kadar je to zahtevano. Kartico aktivira vzbujanje na frekvenci 125 kHz. Vzpostavi se induktivni sklop med kartico in fizično oddaljenim izvorom energije (navadno čitalcem). Vzbujena kartica periodično ponavlja prenos identifikacijskih bitov z uporabo prenosnega sistema.

Katalog HID [12] ali drugi zunanji viri ne poročajo o prisotnosti fizičnih in elektromagnetnih protiukrepih varovanja kartice, zato predpostavljamo, da ne obstajajo.

Slika 6: Slika kartice HID Indala FlexCard z odstranjeno zaščito (Vir: [8]). Slika prikazuje induktivno zanko (anteno kartice) povezano na integrirano vezje

Prenosni sistem Indala RF

Naloga prenosnega sistema Indala RF je prenos podatkov med kartico in čitalcem ter odkrivanje napak med prenosom.

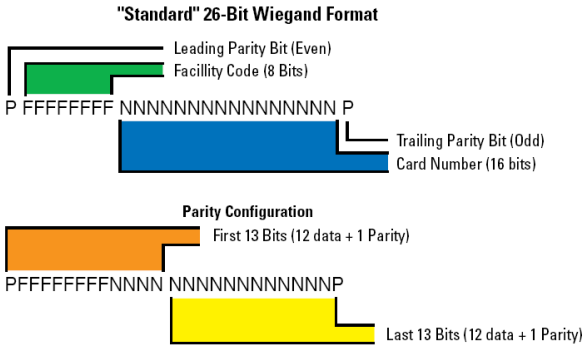
Storitev prenosa podatkov je nepovezana in nezanesljiva, saj ne vsebuje postopka vzpostavitve komunikacijskega kanala in ne vsebuje potrjevanja prejetih sporočil.

Karakteristike prenosnega sistema glede na lastnosti kanala so:

- izmenično dvosmeren (*angl.* »half-duplex«) skupinsko prenosni kanal z možnostjo kolizije,
- zaporedni kanal (radio),
- sinhronizacija je na nivoju paketa in je dosežena s tvorjenjem okvirjev.

O načinu tvorjenja okvirjev na prenosni plasti ni razpoložljivih podatkov, vendar smo prepričani, da je proizvajalec HID izbral lastniško shemo. Tvorjenje okvirjev je pomembna naloga prenosnega sistema , saj rešuje težavo sprejemnika, kako iz sekvence bitov odkriti začetek in konec okvirja.

Identifikacijski niz se nahaja v formatu zapisa Wiegand [10,22]. To je 26-bitni format zapisa, ki vsebuje dva paritetna bita za odkrivanje napak pri prenosu. Preostalih 24-bitov se deli naprej na dva dela: 8-bitni identifikator zgradbe in 16-bitni identifikator kartice. Uporaba dveh paritetnih bitov za odkrivanje napak pomeni, da prenosni sistem prepozna največ dve napaki.



Slika 7: Format zapisa Wiegand in postopek računanja paritete za odkrivanje napak med prenosom (Vir [10]**)**

Delovanje fizične plasti prenosnega sistema opišemo na naslednji način. Ko se kartica nahaja v delovnem področju čitalca, jo ta vzbuja s frekvenco 125 kHz. Kartica in čitalec sta sklopljena induktivno. Kartica prenese niz bitov z uporabo modulacijske sheme s frekvenčnim skokom FSK (*angl.* Frequency Shift Keying). Pri tem je nosilni signal moduliran z diskretnimi spremembami frekvence, ki oznanjajo logično '0' in '1'.

Implementacija prenosnega sistema Indala RF je lastniška in nestandardizirana.

Sistem čitalca Indala

Naloga čitalca je vzbujanje medija s signalom frekvence 125 kHz. V primeru, da se v delovnem območju čitalca nahaja kartica, čitalec zazna moduliran signal, ki se manifestira kot napetostno nihanje na anteni čitalca. Ta napetostna nihanja čitalec ojači, demodulira in vzorči signal. V prejeti sekvenci bitov se nahaja okvir, v njem pa identifikacijski niz oddajnika.

Če čitalec v okvirju ne odkrije napake, je naloga čitalca posredovati prejeti identifikaciji niz zalednemu delu sistema z uporabo prenosnega sistema Wiegand.

Po korespondenci s Špico obstaja za varovanje čitalca protiukrep z vgrajenim stikalom proti vtikanju (*angl.* tamper switch), ki je povezano na alarmno napravo.

Katalog HID [12] ali drugi zunanji viri ne poročajo o prisotnosti fizičnih in elektromagnetnih protiukrepih varovanja čitalca, zato predpostavljamo, da ne obstajajo.

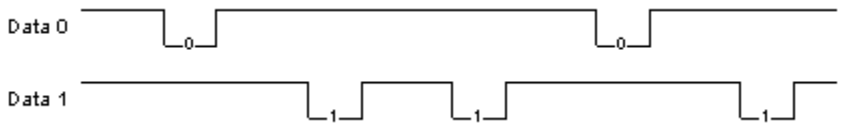
Prenosni sistem Wiegand

Naloga prenosnega sistema Wiegand je prenos podatkov med čitalcem in zalednim delom sistema ter odkrivanje napak med prenosom.

Storitev prenosa podatkov je nepovezana in nezanesljiva, saj ne vsebuje postopka vzpostavitve komunikacijskega kanala in ne vsebuje potrjevanja prejetih sporočil.

Karakteristike prenosnega sistema glede na lastnosti kanala so:

- enosmeren (*angl.* »simplex«) dvotočkovni kanal,
- paralelni kanal (trije bakreni vodniki: skupna masa, kanal za pošiljanje logične '0' in kanal za pošiljanje logične '1'),
- sinhronizacija je na nivoju paketa in je dosežena s tvorjenjem okvirjev.



Slika 8: Časovni diagram protokola Wiegand

O načinu tvorjenja okvirjev na prenosni plasti ni razpoložljivih podatkov, vendar smo prepričani, da se proizvajalec HID drži standarda zaradi združljivosti povezljivosti z zalednim delom sistema. Tvorjenje okvirjev je pomembna naloga prenosnega sistema, saj rešuje težavo sprejemnika, kako iz sekvence bitov odkriti začetek in konec okvirja.

Delovanje fizične plasti Wiegand opišemo na naslednji način. Čitalec in zaledni del sistema sta z vhodno/izhodno napravo povezana na medij, katerega sestavljajo trije bakreni vodniki. Naloga prvega vodnika je izenačitev ničelnega potenciala. Prenos podatkov poteka paralelno po drugih dveh vodnikih. Prenos logične ničle in enice poteka na ločenih vodnikih, kot je prikazano na zgornjem diagramu. V nasprotju s prenosnim sistemom kartice, ta prenosni sistem ne uporablja modulacije signala.

Protokol, aparaturni vmesnik in format zapisa Wiegand sestavljajo industrijski standard povezovanja elementov sistema za nadzor dostopa in prepričani smo, da je implementacija čitalca Indala zaradi združljivosti naprav skladna s temi standardi.

Zaledni del sistema

Naloga zalednega dela sistema je overjanje identifikacijskih nizov in avtorizacija zahtevane storitve. Za vsak čitalec obstaja seznam nadzora dostopa, v katerem se nahaja trojica identifikacijski niz – čitalec–pristojnost.

Postopek overjanja in avtorizacije se zaključi uspešno, če se oddajnik identifikacijskega niza preko čitalca nahaja v tej trojici. V tem primeru se proži izvedba zahtevane storitve. Informacijski sistem za nadzor dostopa ponuja dve storitvi:

- odklep vrat in
- preklapljanja stanja alarmnega sistema.

Metode znanih napadov na sistem za nadzor dostopa prostorov s sistemom kartice Indala FlexCard

V poglavju »Arhitekturni model sistema z opisom elementov« smo definirali arhitekturo in opisali delovanje sistema. V tem poglavju se bomo osredotočili na opis ranljivosti in na metode znanih napadov na ta sistem.

O nameščenih protiukrepih za zmanjšanje tveganja napada na celovitost fizičnih naprav ni podatkov v katalogu HID ali na Internetu. Če bi sami želeli opraviti tovrstna preizkušanja, bi potrebovali posebno opremo in dostop do podobnega sistema.

Po drugi strani pa nam je uspelo proučiti delovanje protokolov kartice in čitalca. Medij katice in čitalca sta zrak in vodnik. S pomočjo modela za določanje lastnosti protokolov Dolev-Yao [6] bomo postavili zahteve za varno uporabo tega sistema. V modelu Dolev-Yao privzemamo, da je nosilec podatkov po mediju napadalec, katerega omejujejo le kriptografske metode. Napadalec na ta način lahko prisluškuje, prestreže ali vnese sporočilo.

Za vsak informacijski sistem za nadzor fizičnega dostopa se zahteva zagotavljanje naslednjih dveh varnostnih kriterijev: celovitost in zaupnost sistema.

Del informacijskega sistema kartica-čitalec na predstavitveni plasti ne vsebuje protokola za medsebojno overjanje entitet, overjanje in zagotavljanje tajnosti sporočil, zato je ta porazdeljeni informacijski sistem po modelu Dolev-Yao varen samo, če je varen medij.

Podoben problem predstavlja predstavitvena plast v delu informacijskega sistema čitalec-zaledni del sistema.

Medij zavarujemo z uporabo različnih protiukrepov. Primera teh protiukrepov sta:

- namestitev Faradayeve kletke v področje kartice in v delovno področje čitalca. Fizično varovanje prostora bi zagotavljal lastnik kartice, ki je hkrati tudi uporabnik storitev čitalca.
- Oklopljen vodnik med čitalcem in zalednim delom sistema, katerega notranji vodniki so zaščiteni s prevodno folijo (Faradayovo kletko). Idealno bi tak kabel še imel stikalo proti vtikanju (*angl.* tamper switch). Fizično varnost bi zagotavljala vgradnja kabla v betonsko steno.

Informacijski sistem za nadzor fizičnega dostopa v prostore podjetja RRC d.o.o. s sistemom kartic HID Indala FlexCard teh dveh ali podobnih protiukrepov nima nameščenih, zato je izpostavljen **vsaj** na napade na protokol kartice in čitalca, ki ju bomo opisali v nadaljevanju.

Medtem ko napad na protokol čitalca zahteva fizični dostop do vodnika, napad na protokol kartice ne zahteva fizičnega dostopa, zaradi vzpostavitve »brezžičnega« induktivnega sklopa med čitalcem in kartico. Predpostavljamo lahko, da bo kvaliteta antene in jakost signala napadalca boljša od

navadnega čitalca, zato bomo podali taksonomijo razdalj odčitavanja pasivnih kartic po [19], ki obravnava možnosti oddaljenosti napadalca od kartice:

1. **Nominalna razdalja čitalca** je delovno področje čitalca in navadno dosega razdaljo odčitavanja do 10 cm. Pri tem pripomnimo, da je najmočnejši čitalec Indala zmožen odčitavati na razdalji do 60 cm [12].

2. **Razdalja čitalca napadalca** je delovno področje čitalca napadalca, ki presega nominalno razdaljo čitalca, saj ima nameščen močnejši in nestandardni ojačevalec signala. Razdalja čitalca napadalca definirana največjo razdaljo pri kateri katerikoli čitalec lahko še vzbudi kartico.

3. **Razdalja prisluškovanja prenosa v smeri kartica-čitalec** presega razdaljo čitalca napadalca. Največja razdalja pri kateri čitalec lahko še vzbudi kartico je presežena, zaradi obstoja drugega vira vzbujanja, katerega na primer predstavlja legitimni čitalec.

4. **Razdalja prisluškovanje prenosa v smeri čitalec-kartica** presega razdaljo prisluškovanja prenosa v smeri kartica-čitalec, saj je jakost signala v smeri čitalec-kartica za nekaj magnitud večja.

Napad na protokol kartice

Zaradi zgoraj navedenih pomanjkljivost lahko v namen napada na protokol kartice uporabimo orodja za prisluškovanje, ki po zgornji taksonomiji oddaljenosti napadalca sodijo v kategorijo 1, 2 in 3. Kategorija 4 za ta sistem ne prinaša koristi razen za identifikacijo izvora čitalca, npr. z metodo triangulacije signala. Prejeti signal se uporabi za dekodiranje identifikacijskega niza, katerega se posname na kartico ali pa se ga z uporabo antene in ojačevalnika ponovno predvaja legitimnemu čitalcu.

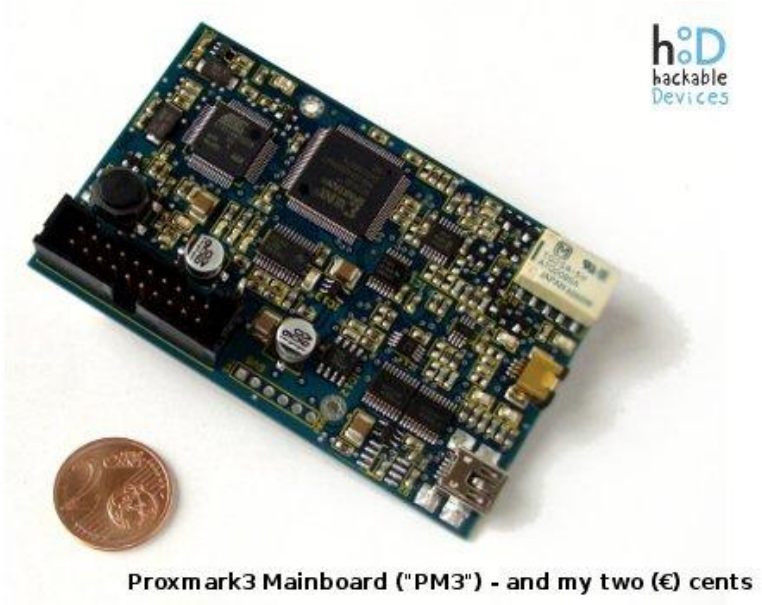
- Prvemu napadu rečemo napad s kloniranjem kartice (*angl.* »tag cloning attack«),
- drugemu pa napad s ponovnim predvajanjem (*angl.* »replay attack«).

Za oba napada obstajata implementaciji, kateri je mogoče kupiti preko spleta. Prav tako obstajajo načrti za lastno gradnjo orodja skupaj s programsko opremo. Orodja za napad na različne tipe kartic različnih proizvajalcev so navedena na spletni strani [1].

Naša naloga je identifikacija orodja za napad na kartico HID Indala FlexCard. Kreator orodja za napad na to vrsto kartice je Jonatan Westhues, ki je svoja orodja poimenoval »Prox mark-I.«, »Prox mark-II.« in »Prox mark-III.« [28]. Zadnja različica orodja Proxmark 3 je nastala leta 2006. Uporabo orodja je Westhues demonstriral na informacijskem sistemu za nadzor fizičnega dostopa sedeža zvezne vlade države Kalifornije ZDA [27]. Načrt za gradnjo in navodila za uporabo orodja je objavil na javno dostopno spletno stran [2].

Po drugi strani pa hekerjem ni potrebno lastnoročno izdelovati orodja za napad na kartico HID Indala FlexCard, ampak je za ceno manj kot 200 EUR na voljo v spletni trgovini [3,4]. Ko je heker Chris Paget ponovno demonstriral ranljivost kartice na konferenci RSA [23], je požel vso slavo, kateri so sledile grožnje s strani proizvajalca kartice HID [25]. Tretja znana demonstracija napada na to kartico izvira s

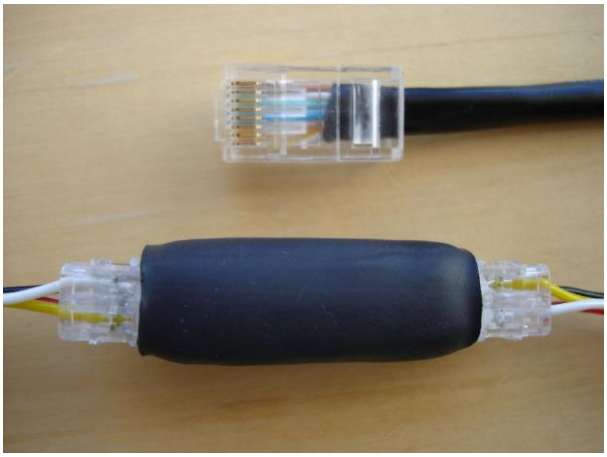
prestižne univerze MIT, kjer so sami razvili orodje za napad za manj kot 50 EUR [21]. Zadnja različica orodja Proxmark 3 je narejena v velikosti nekaj evrocentov in je (brez antene) prikazana na spodnji sliki.



Slika 9: Reklamna slika za napravo Proxmark3 za hekanje naprav HID (vključno z HID Indala FlexCard) brez priključene antene in izvora električne energije ter primerjava velikosti naprave z dvema stotinoma (Vir slike [4])

Napad na protokol čitalca

Raziskovalec Zac Franken je implementiral orodje Gecko [4,7], ki izkorišča ranljivost protokola za komunikacijo med čitalcem in zalednim delom sistema – Wiegand. Na konferenci LayerOne je leta 2007 ta napad tudi demonstriral. Za izkoriščanje te ranljivosti je nujno, da se napravo Gecko priključi na kabel med čitalcem in zalednim delom sistema.



Slika 10: Orodje Gecko (Vir slike [8]) in primerjava velikosti naprave s priključkom RJ45 (priključek za Ethernet)

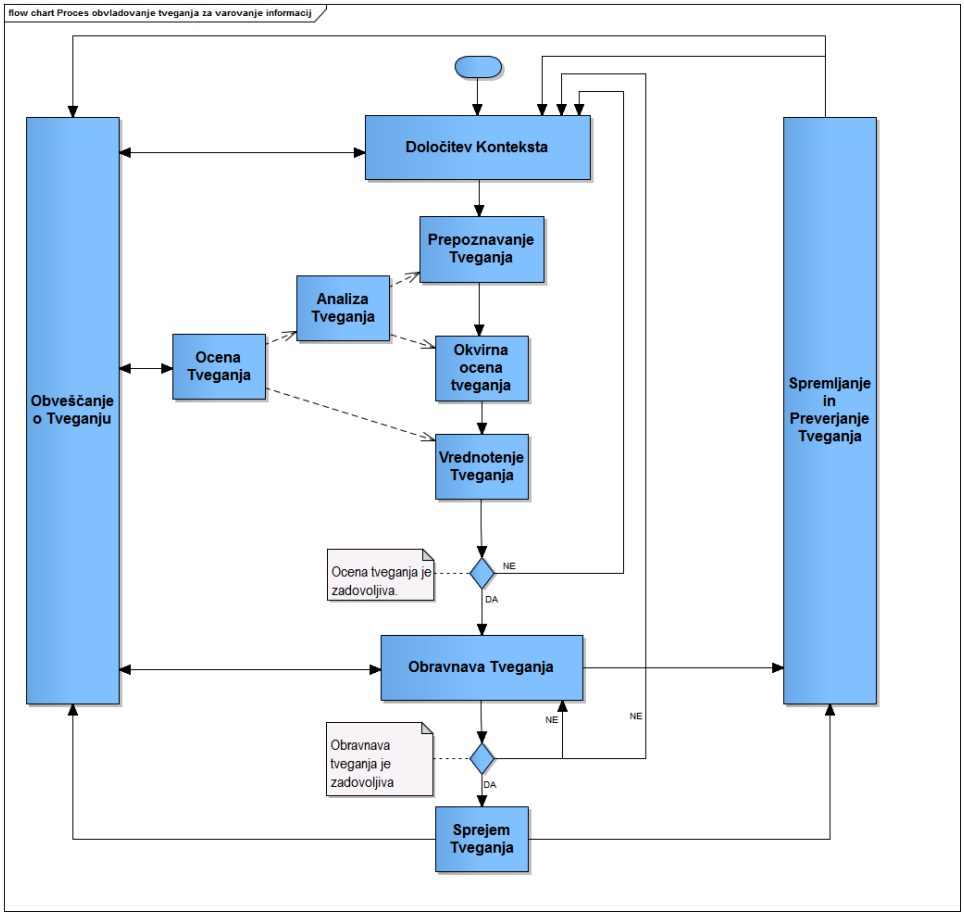
Proces obvladovanja tveganja za varovanje informacij

Sistem za upravljanje varovanja informacij (SUVI) je del celotnega sistema vodenja, ki temelji na pristopu obvladovanja poslovnega tveganja, za vzpostavitev, implementacijo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje informacijske varnosti [14].

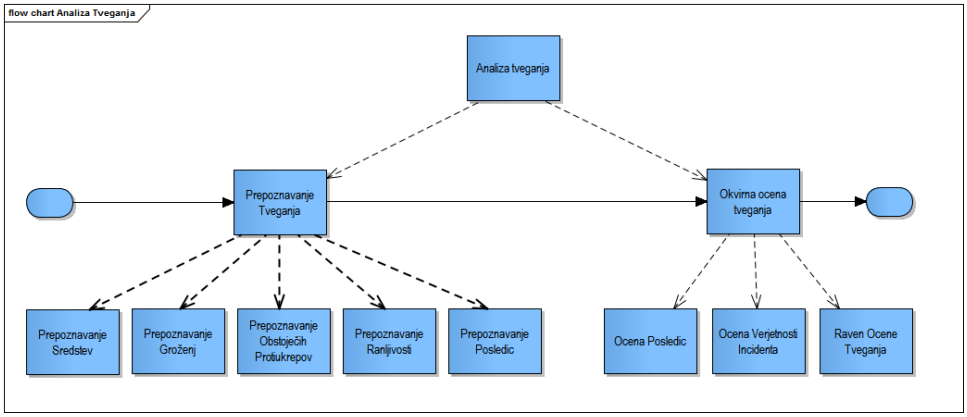
Da se opredelijo potrebe organizacije glede varovanja informacij in se oblikuje učinkovit sistem SUVI, je potreben sistematičen pristop k obvladovanju tveganja pri varovanju informacij. Iz ISO/IEC 27005 [16] sledi, da obvladovanje tveganja pri varovanju informacij mora prispevati k:

- prepoznavanju tveganja,
- oceni tveganja v smislu posledic za poslovanje in verjetnosti njihovega dogodka,
- razumevanju in komunikaciji posledic tveganja,
- določitvi prednostnega vrstnega reda za obravnavo tveganja,
- o sodelovanju interesnih skupin pri sprejemu odločitve o obvladovanju tveganja
- spremljanju učinkovitosti obravnave tveganja,
- spremljanju tveganj in rednemu pregledovanju procesa obvladovanja tveganja,
- zbiranju informacij za izboljšanje pristopa k obvladovanju tveganja in
- o neprekinjenem procesu izobraževanja o tveganjih in ukrepih za njihovo blaženje.

Spodnja diagrama predstavljata opisan proces obvladovanja tveganja za varovanje informacij.



Slika 11: Diagram poteka – Proces obvladovanja tveganja za varovanje informacij (povzeto po ISO 27005 [16])

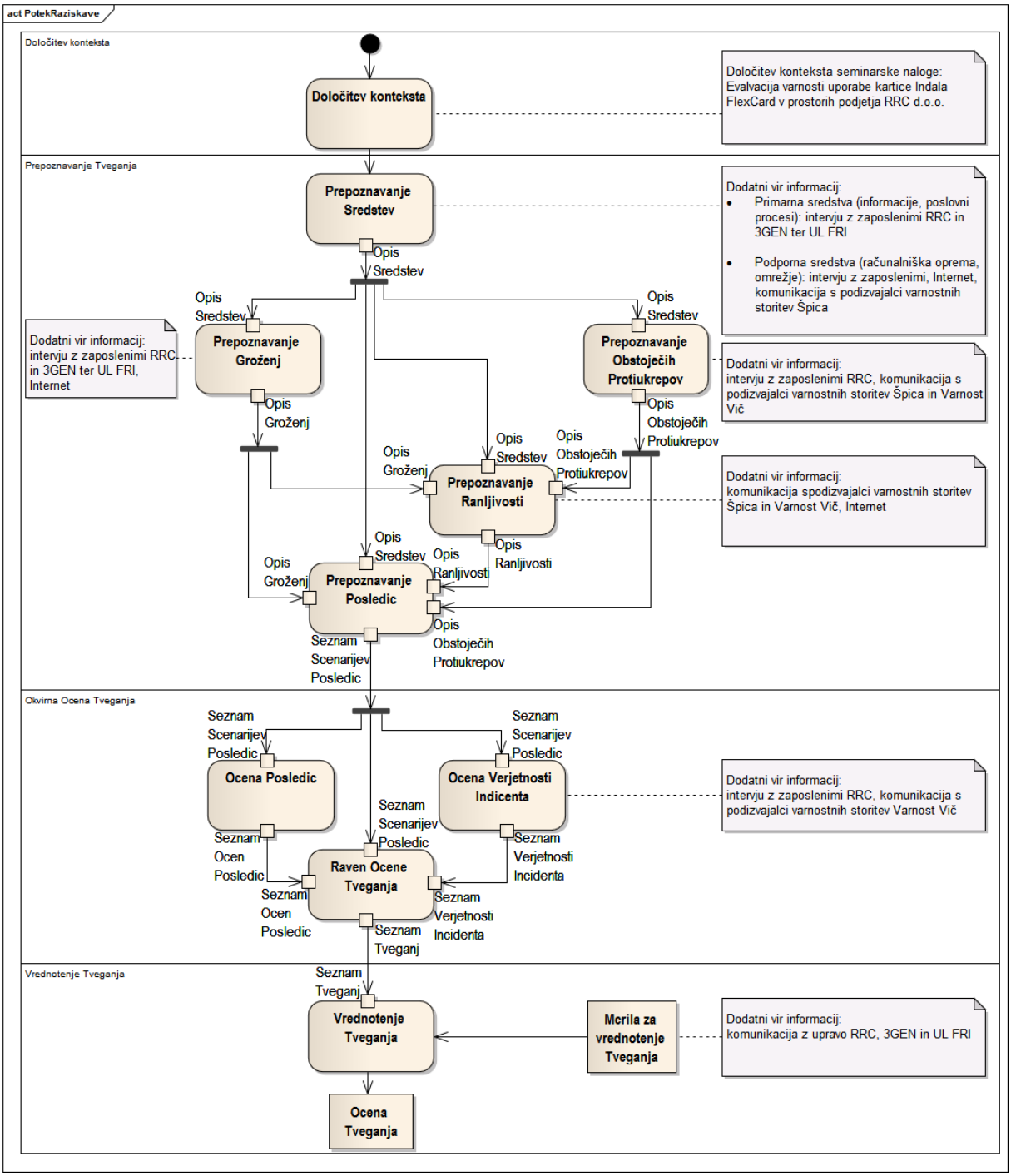


Slika 12: Diagram poteka – Proces analize tveganja

Ocena tveganja informacijskega sistema za nadzor fizičnega dostopa prostorov podjetja RRC d.o.o.s sistemom kartice HID Indala FlexCard

Potek raziskave

Potek opravljene raziskave je podan s spodnjim diagramom aktivnosti in je vezan na proces ocene tveganja v okviru procesa obvladovanja tveganja [16] (glej Slika 11 in Slika 12).



Slika 13: Diagram aktivnosti – Postopek ocene tveganja informacijskega sistema za nadzor fizičnega dostopa prostorov podjetja RRC d.o.o. s sistemom Indala FlexCard

Potek opravljene raziskave opišemo na naslednji način:

1. Začetek raziskave oznanja črni krog. V tržnem primeru je to naročilo storitve ocene tveganja, v našem primeru pa zadolžitev pri opravljanju predmeta.

2. V naslednjem koraku se stranki pogodita glede konteksta raziskave. V našem primeru je bil kontekst podan z nalogo zadolžitve, tj. proučitev varnosti uporabe kartice Indala FlexCard v prostorih podjetja RRC d.o.o.

3. Ko se stranki dogovorita za kontekst raziskave, sledi proces ocene tveganja, ki vsebuje tri aktivnosti: prepoznavanje tveganja, okvirna ocena tveganja in vrednotenje tveganja. Izvajanje teh aktivnosti in podaktivnosti pojasnimo na naslednji način:

   Standard ISO/IEC 27005 [16] ne definira vrstnega reda izvajanja podaktivnosti prepoznavanja tveganja in ocene tveganja. Po drugi strani pa za vsako podaktivnost definira prispevek, ukrep, navodila za vpeljavo in rezultat. Odraz tega opišemo z objektnim tokom zgornjega diagrama. Posamezna podaktivnost se proži:

   a. v trenutku ko so na voljo vsi vhodni (podatkovni) žetoni oz.

   b. ob spremembi vhodnega (podatkovnega) žetona, če je izpolnjena prejšnja predpostavka.

   Črna palica v diagramu predstavlja delitev žetonov na več sočasnih tokov.

Proces ocene tveganja na ta način poteka tako dolgo, dokler raziskava več ne daje novih rezultatov, kar potem predstavlja dokončni rezultat ocene tveganja. Po drugi strani pa se bomo v tej raziskavi omejili zgolj na prvo iteracijo. To pomeni, da v okviru zgornjega diagrama dodamo omejitev, da posamezna aktivnost lahko generira le en sam izhodni žeton.

Določitev konteksta

Kontekst raziskave je bil določen z naročilom za oceno tveganja sistema kartice, ki se uporablja za nadzor fizičnega dostopa v prostore podjetja RRC. Namen raziskave je:

1. Zajem relevantnih **varnostnih podatkov** informacijskega sistema za nadzor fizičnega dostopa prostorov RRC s sistemom kartice HID Indala FlexCard.

2. Opraviti postopek **ocene tveganja** za določitev informacijske varnosti tega sistema. Proces in metode ocenjevanja tveganja skladno bodo skladne z družino mednarodno veljavnih standardov za načrtovanje, vzpostavitev in revidiranje *sistemov za upravljanje varovanja informacij* (SUVI) – ISO/IEC 2700X [14,15,16,17].

V prostorih podjetja RRC delujejo tri podjetja:

Podjetje RRC d.o.o. nudi računalniške storitve za vzpostavitev informacijskih sistemov za učinkovito upravljanje z energijo, javna naročanja, kadrovske sisteme in razvoj poslovnih rešitev po meri naročnika. Njihovi poslovni partnerji so:

- Ministrstvo RS za Finance,
- Davčni Urad RS,
- Ministrstvo RS za Obrambo,
- Ministrstvo RS za Šolstvo in šport,
- Uprava RS za zaščito in reševanje,
- Uprava RS za izvrševanje kazenskih sankcij,
- Banka Slovenije,
- Casino Lev,
- Podjetja Kemofarmacija d.d., DDC d.o.o. in
- Zavod za varstvo pri delu d.d. in zavod za šport RS Planica.

Podjetje 3GEN d.o.o. se ukvarja s sitemsko in operativno podporo velikih IBM mainframe sistemov in UNIX orientiranih sistemov ter baz podatov. Njihovi naročniki so različni organi javne uprave.

UL Fakulteta za računalništvo in informatiko je visokošolska inštitucija, ki se ukvarja z izobraževanjem in raziskavami ter aplikativnimi projekti, ki so podprti s strani ARRS, Ministrstva RS za visoko šolstvo, znanost in tehnologijo, Ministrstva RS za šolstvo in šport, Evropske komisije ter industrije in individualnih naročnikov.

Za vsa podjetja je skupno, da

- razpolagajo z dragoceno računalniško opremo in/ali
- upravljajo z informacijami zaupne narave, za katere regulator nalaga obvezno varovanje v 102. členu (zaščitni ukrepi) Zakonu o elektronskih komunikacijah (ZEKom) RS [24]. Za kršitev alineje 4 tega člena zakonodajalec nalaga prevzem odgovornosti in stroškov, ki nastanejo kot dokazana posledica zlorab.

Analiza tveganja

Prepoznavanje sredstev

V naslednji tabeli so prikazana prepoznana sredstva s pripadajočimi viri informacij.

Org.	Sredstvo	Tip Vrednotenja	Vrednotenje Sredstva	Kolicnik	Vrednotenje v EUR	Vir
UL FRI	Strojna oprema	Trenutna vrednost	~100.000 EUR	1	~100.000 EUR	Računovodstvo FRI, g. Maher Kaddoura
		Nabavna vrednost	~300.000 EUR	1	~300.000 EUR	Računovodstvo FRI, g. Maher Kaddoura
UL FRI	Izpad pedagoškega procesa	Čas izpada	~1 teden predavanj, ~3 tedne vaj	20EUR/h	~10.000 EUR	Prodekanja za pedagoško dejavnost – prof.dr. Neža Mramor Kosta, Podpora IKT ga. Tadeja Saje, urnik FRI
3GEN	Strojna oprema	Trenutna vrednost	~5.000 EUR	1	~5.000 EUR	Vir: Uslužbenka podjetja 3GEN
3GEN	Izpad kritičnih poslovnih procesov	Čas izpada	~1 mesec (20 delovnih dni)	100EUR/dan/delavec, 3 delavci	~6000 EUR	Vir: Uslužbenka podjetja 3GEN
3GEN	Kršenje zaupnosti podatkov	Potencialna škoda	5 (Kvalitativno na lestivici od 1 do 5)	-	-	Vir: Uslužbenka podjetja 3GEN

Tabela 2: Tabela prepoznanih primarnih in podpornih sredstev

Podjetje RRC zaradi lastne politike varovanja informacij zavrača sodelovanje pri raziskavi, zato njihova sredstva niso bila popisana. Neuradno pa ocenjujemo, da so sredstva računalniške opreme RRC primerljiva z vrednostjo sredstev računalniške opreme UL FRI v teh prostorih. Potencialna škoda, ki bi nastala zaradi izgube informacij pa ocenjena s oceno 5 na kvalitativni lestvici od 1 do 5. Do tega sklepa smo prišli na podlagi pregleda njihovih poslovnih partnerjev, ki upravljajo z zaupnimi informacijami in fizičnega pregleda prostorov RRC.

V popisu sredstev manjka še popis sredstev – poslovnih procesov laboratorijev ViCOS in LKRV UL FRI.

Prepoznavanje groženj

V naslednji tabeli je prikazan seznam prepoznanih groženj, ki pretijo podjetjem RRC, 3GEN in UL FRI.

Grožnja	Motiv	Možne posledice grožnje
Vdiralec	Denar	Kraja opreme
Industrijsko vohunjenje	Konkurenčna prednost	Kraja informacij Obrambna prednost Politična prednost Gospodarsko izkoriščanje Vdor v zasebnost

Tabela 3: Tabela prepoznanih groženj

Prepoznavanje obstoječih protiukrepov

V okviru konteksta raziskave sta bila prepozna dva protiukrepa:

1. Sistem za nadzor fizičnega dostopa prostorov s sistemom HID Indala FlexCard ima vgrajeno stikalo proti vtikanju (*angl.* tamper switch), kar izvedbo kraje čitalca.
2. Podjetje 3GEN ima vzpostavljen sistem neprekinjenega poslovanja za nadaljevanje kritičnih procesov ob morebitnih prekinitvah. Pri posledicah se le-ta upošteva v krajšem času za ponovno vzpostavitev kritičnih poslovnih procesov.

Podatke o tipičnih protiukrepih za obravnavanje tveganja kraje nam ni uspelo pridobiti, ker intervjuvanci niso vedeli odgovoriti na to vprašanje ali ker niso hoteli sodelovati pri raziskavi. To so navadno sklenjene zavarovalne police za zavarovanje računalniške opreme proti kraji. Zaradi tega razloga bomo v nadaljevanju le-to črnogledo upoštevali tako, kot če nobeno podjetje ne bi imelo vzpostavljenega protiukrepa za prenos tveganja z zavarovanjem proti kraji.

Prepoznavanje ranljivosti

V naslednji tabeli sta prikazani prepoznani ranljivosti, ki sta povezani z možnimi grožnjami.

Vrsta ranljivosti	Ranljivost	Opis ranljivosti	Grožnja
Prostor organizacije UL FRI, 3GEN, RRC	Pomanjkanje fizične zaščite zgradbe, vrat in oken.	Ranljivost protokola kartice porazdeljenega informacijske sistema nadzora fizičnega dostopa v prostore RRC s sistemom Indala FlexCard (glej odsek Napad na protokol kartice)	Vdiralec
			Industrijsko vohunjenje
		Ranljivost protokola čitalca porazdeljenega informacijske sistema nadzora fizičnega dostopa v prostore RRC s sistemom Indala FlexCard (glej odsek Napad na protokol čitalca)	Vdiralec
			Industrijsko vohunjenje

Tabela 4: Tabela prepoznanih ranljivosti

Prepoznavanje posledic

Prisotnost ranljivosti predstavlja le potreben pogoj za zlorabo sredstev. Zadosten pogoj za zlorabo sredstev je prisotnost groženj, ki izkoriščajo ranljivosti. V naslednji tabeli so prikazane prepoznane posledice za prepoznane trojice grožnja–ranljivost–sredstvo. Določene so tudi vzročne odvisnosti posledic.

Grožnja	Ranljivost	Sredstvo	N	Posledica	Vzročna odvisnost posledice
Vdiralec	Pomanjkanje fizične zaščite zgradbe, vrat in oken: informacijski sistem za nadzor fizičnega dostopa	UL FRI: Strojna oprema	1	Kraja opreme	-
		UL FRI: Izpad pedagoškega in raziskovalnega procesa	2	Izpad pedagoškega in raziskovalnega procesa, zaradi pomanjkanja osnovne opreme ter zamik izvajanja zaradi nabavnih in namestitvenih rokov.	1
		3GEN: Strojna oprema	3	Kraja opreme	-
		3GEN: Izpad kritičnih poslovnih procesov	4	Krajši izpad kritičnih poslovnih procesov, zaradi pomanjkanja informacij na delovnem mestu	3
		3GEN: Kršenje zaupnosti podatkov	5	Kršenje zaupnosti podatkov in morebitne odškodninske posledice.	3
Industrijsko vohunjenje	Pomanjkanje fizične zaščite zgradbe, vrat in oken: informacijski sistem za nadzor fizičnega dostopa	UL FRI: Strojna oprema	6	-	-
		UL FRI: Izpad pedagoškega procesa	7	-	-
		3GEN: Strojna oprema	8	-	-
		3GEN: Izpad kritičnih poslovnih procesov	9	-	-
		3GEN: Kršenje zaupnosti podatkov	10	Kršenje zaupnosti podatkov in morebitne odškodninske posledice.	-

Tabela 5: Tabela prepoznanih posledic

Rezultat prepoznavanja posledic so scenariji incidentov z njihovimi posledicami za sredstva in poslovne procese. Z uporabo zgornje tabele bo predstavljen le en sam scenarij – »Vdiralec«. Zaradi pomanjkanja podatkov in nesodelovanja podjetja RRC, scenarija »Industrijski vohun« ni mogoče kredibilno predstaviti.

Scenarij »Vdiralec«

Janezu Vdiralcu se je pred kratkim ponudila nova poslovna priložnost. Pridobil je seznam slovenskih podjetij, ki uporabljajo ranljivo opremo za nadzor fizičnega dostopa. Janez Vdiralec ne prodaja varnostnih storitev kot ste morda sprva domnevali, temveč je poklicni tat in preprodajalec računalniške opreme.

V zadnjih letih je veliko podjetij menjalo način fizičnega dostopa do svojih prostorov z metode ključavnice in ključa na sistem brezkontaktnih kartic. Podjetja so s tem načinom nadzora dostopa zadovoljna zaradi vrste razlogov:

- ni potrebno kopirati ključev za vsakega uslužbenca posebej,
- postopek preklica v primeru izgube poverilnice je enostavnejši, saj se v primerjavi s preprostim preklicem kartice morajo zamenjati vse ključavnice izgubljenih ključev,
- omogoča sledenje vstopov v prostor, saj se vsak vstop v prostor samodejno beleži v zgodovino dostopov informacijskega sistema za nadzor fizičnega dostopa in
- optimizacija stroškov, saj je z novim sistemom delovno mesto vratarja / varnostnika potrebno le še v zmanjšanem obsegu.

Tudi Janez je navdušen nad opisanimi funkcionalnimi lastnostmi sistema, še bolj pa se navdušuje nad slabo implementacijo nefunkcionalne lastnosti sistema, tj. varnostjo sistema. Na Internetu je odkril dve pomanjkljivosti sistema, in sicer napako v protokolu kartice in protokolu čitalca (glej Napad na protokol kartice in Napad na protokol čitalca). Janez ima preomejeno tehnično znanje, da bi lastnoročno sestavil orodje za napad na protokol kartice, vendar to premosti z veliko volje in z nakupom opreme za izkoriščanje ranljivosti protokola kartice HID Indala FlexCard preko spleta za manj kot 100 EUR.

Po ogledu različnih lokacij za krajo se odloči za prostore RRC, saj je pričakovana vrednosti plena računalniške opreme velika in zaradi odhoda varnostnika po 20. uri zvečer. Še posebej mu je všeč (nerodna) integracija alarmnega sistema s sistemom nadzora fizičnega dostopa. S pajdaši pripravi vlom v prostore podjetja RRC in krajo opreme podjetij RRC, 3GEN in UL FRI na naslednji način:

- Janez se pretvarja, da je študent. V avli na kavču sede čaka na prihod profesorja. V rokah drži šolsko torbo polno potrebščin. Med čakanjem se sprehaja mimo njega veliko oseb; tudi tisti, ki imajo privilegije vstopa v vse prostore, kot so na primer hišnik, varnostnik in uprava podjetja. Kar ostali ne vedo, je dejstvo, da se med Janezovimi potrebščinami nahaja tudi nelegitimni čitalnik, katerega sestavljajo baterija, vezje in zmogljiv oddajnik/sprejemnik, ki ta čas shranjuje odzive kartic. Le-te bo druščina uporabila v naslednji fazi napada.

- Zločinska družba shranjene odzive kartic uporabi dne 1.1.2011, ko je stavba prazna in se vsi brezskrbno zabavajo na novoletni zabavi. V zgradbo vstopijo s ponovnim predvajanjem poverilnice člana uprave in na enak način onemogočijo tudi alarmni sistem. Preko stranskih vrat ukradejo vso računalniško opremo v stavbi, za sabo pa pustijo precejšnje razdejanje in velik napis: »Srečno in zdravo novo leto 2011!«.

Okvirna ocena tveganja

Ocena posledic

Določitev ocene posledic, ki bi podjetji 3GEN in UL FRI utrpeli zaradi scenarija »Vdiralec«, je prikazana na spodnji tabeli, katera je izpeljana iz tabele prepoznanih posledic (glej Tabela 5).

Scenarij	Grožnja	Ranljivost	Sredstvo	N	Posledica	Vzročna odvisnost posledice	Ocena Posledic
Vdiralec	Vdiralec	Pomanjkanje fizične zaščite zgradbe, vrat in oken: informacijski sistem za nadzor fizičnega dostopa	UL FRI: Strojna oprema	1	Kraja opreme	-	~300.000 EUR
			UL FRI: Izpad pedagoškega in raziskovalnega procesa	2	Izpad pedagoškega in raziskovalnega procesa, zaradi pomanjkanja osnovne opreme ter zamik izvajanja zaradi nabavnih in namestitvenih rokov.	1	~10.000 EUR
			3GEN: Strojna oprema	3	Kraja opreme	-	~5.000 EUR
			3GEN: Izpad kritičnih poslovnih procesov	4	Krajši izpad kritičnih poslovnih procesov, zaradi pomanjkanja informacij na delovnem mestu	3	~6.000 EUR
			3GEN: Kršenje zaupnosti podatkov	5	Kršenje zaupnosti podatkov in morebitne odškodninske posledice.	3	5 (kvalitativna ocena na lestvici 1-5)
						Spodnja meja Ocena posledic scenarija:	~320.000 EUR

Tabela 6: Tabela ocena posledic za napadena sredstva scenarija »Vdiralec«

Ocena posledic scenarija »Vdiralec« je ocenjena na približno 320.000 EUR in je konservativna, saj ne upošteva posledice 5 – kršenja zaupnosti podatkov podjetja 3GEN, katero vrednotenja sredstva je bilo podano kvalitativno. Ocena posledic prav tako ne upošteva škode, ki bi zaradi kraje opreme, izpada kritičnih poslovnih procesov in kršenja zaupnosti podatkov utrpelo podjetje RRC.

Ocena verjetnosti incidenta

Verjetnost incidenta scenarija »Vdiralec« je ocenjena **srednje** do **zelo verjetno** zaradi naslednjih razlogov:

- Zgodovine preteklih treh vlomov v prostore podjetja RRC v zadnjih nekaj letih.
- Enostavno izkoriščanja ranljivosti informacijskega sistema nadzora fizičnega dostopa s sistemom kartic HID Indala FlexCard.

Bolj natančne ocene verjetnosti incidenta za scenarij »Vdiralec« ni mogoče podati, saj podjetje RRC ni pripravljeno posredovati varnostno pomembnih podatkov za raziskavo. To posledično otežuje pravilno korelacijo dogodkov informacijske varnosti in groženj scenarija.

Raven ocene tveganja

Okvirna ocena tveganja je predstavljena kot kombinacija verjetnosti scenarija incidenta in njegovih posledic. Za scenarij »Vdiralec« je okvirna ocena tveganja podana z naslednjo tabelo.

Scenarij	Ocena verjetnosti incidenta	Grožnja	Ranljivost	Sredstvo	N	Posledica	Vzročna odvisnost posledice	Ocena Posledic
Vdiralec	Možno - Zelo verjetno (kvalit. ocena)	Vdiralec	Pomanjkanje fizične zaščite zgradbe, vrat in oken: informacijski sistem za nadzor fizičnega dostopa	UL FRI: Strojna oprema	1	Kraja opreme	-	~300.000 EUR
				UL FRI: Izpad pedagoškega in raziskovalnega procesa	2	Izpad pedagoškega in raziskovalnega procesa, zaradi pomanjkanja osnovne opreme ter zamik izvajanja zaradi nabavnih in namestitvenih rokov.	1	~10.000 EUR
				3GEN: Strojna oprema	3	Kraja opreme	-	~5.000 EUR
				3GEN: Izpad kritičnih poslovnih procesov	4	Krajši izpad kritičnih poslovnih procesov, zaradi pomanjkanja informacij na delovnem mestu	3	~6.000 EUR
				3GEN: Kršenje zaupnosti podatkov	5	Kršenje zaupnosti podatkov in morebitne odškodninske posledice.	3	5 (kvalitativna ocena na lestvici 1-5)
							Spodnja meja Ocena posledic scenarija:	~320.000 EUR

Tabela 7: Tabela okvirne ocena tveganja z določeno spodnjo mejo ocene posledic in določeno verjetnostjo incidenta informacijske varnosti

Vrednotenje tveganja

Zadnji korak pri določitvi ocene tveganja predstavlja vrednotenje tveganja. Tveganje vrednotimo na naslednji način.

Raven tveganja, ki se nahaja v tabeli okvirne ocene tveganja (Tabela 7) je potrebno primerjati z merili za vrednotenje tveganja in merili za sprejetje tveganja. Rezultat tega je **ocena vpliva na poslovanje**.

Z uporabo ocene na vpliv poslovanja, verjetnosti incidenta in tabele za vrednotenje tveganja (glej Tabela 8) določimo iskano oceno tveganja za dan scenarij. Če obstaja več scenarijev, je potrebno ocene tveganja prednostno razvrstiti za prednostno obravnavo največjega tveganja.

		Verjetnost scenarija incidenta				
		Zelo neverjetno	Neverjetno	Možno	Verjetno	Zelo verjetno
Vpliv na poslovanje	Zelo nizko	0	1	2	3	4
	Nizko	1	2	3	4	5
	Srednje	2	3	4	5	6
	Visoko	3	4	5	6	7
	Zelo Visoko	4	5	6	7	8

Tabela 8: Tabela za vrednotenje tveganja ob upoštevanju verjetnosti scenarija incidenta in ocenjenim vplivom na poslovanje

Oceno tveganja interpretiramo na naslednji način. Rezultat od 0 do 2 (zeleno) predstavlja **nizko tveganje**, rezultat od 3 do 5 (rumeno) **srednje tveganje** in rezultat od 6 do 8 (rdeče) **visoko tveganje**.

Za določitev ocene vpliva na poslovanje posameznega podjetja bi potrebovali merila za vrednotenje tveganja podjetij RRC, 3GEN in UL FRI. Zahtevanih meril nam ni uspelo pridobiti od nobenega podjetja, zato bomo sami podali približno oceno vpliva na poslovanje.

Ocena tveganja za UL FRI

Verjetnost scenarija incidenta »Vdiralec« je možna do zelo verjetna. Ocena posledic za ta scenarij znaša približno 310.000 EUR. Naše mnenje je, da bi posledice scenarija imele **srednji vpliv** na poslovanje podjetja.

		Verjetnost scenarija incidenta				
		Zelo neverjetno	**Neverjetno**	**Možno**	**Verjetno**	**Zelo verjetno**
Vpliv na poslovanje	**Zelo nizko**	0	1	2	3	4
	Nizko	1	2	3	4	5
	Srednje	2	3	4	5	6
	Visoko	3	4	5	6	7
	Zelo Visoko	4	5	6	7	8

Tabela 9: Vrednotenje tveganja UL FRI za scenarij »Vdiralec«

Zgornja tabela prikazuje interval ocene tveganja UL FRI za scenarij »Vdiralec« in je vrednotena kot **srednje do visoko tveganje**.

Ocena tveganja za podjetje 3GEN d.o.o.

Verjetnost scenarija incidenta »Vdiralec« je možna do zelo verjetna. Ocena posledic za ta scenarij znaša približno 10.000 EUR. Pri tem niso upoštevane posledice, ki bi nastale zaradi kršitve zaupnosti podatkov in morebitnih odškodninskih tožb. Podjetje 3GEN sodeluje s poslovnimi partnerji, ki razpolagajo z zaupnimi informacijami. Zaradi teh razlogov menimo, da bi posledice scenarija imele **srednje do visok vpliv** na poslovanje podjetja.

		Verjetnost scenarija incidenta				
		Zelo neverjetno	**Neverjetno**	**Možno**	**Verjetno**	**Zelo verjetno**
Vpliv na poslovanje	**Zelo nizko**	0	1	2	3	4
	Nizko	1	2	3	4	5
	Srednje	2	3	4	5	6
	Visoko	3	4	5	6	7
	Zelo Visoko	4	5	6	7	8

Tabela 10: Vrednotenje tveganja podjetja 3GEN d.o.o. za scenarij »Vdiralec«

Zgornja tabela prikazuje interval ocene tveganja 3GEN d.o.o. za scenarij »Vdiralec« in je vrednotena kot **srednje do visoko tveganje**.

Ocena tveganja za podjetje RRC d.o.o.

Verjetnost scenarija incidenta »Vdiralec« je možna do zelo verjetna. Ocena posledic za ta scenarij zaradi nesodelovanje podjetja RRC ni znana. Podjetje RRC ponuja storitve poslovnim partnerjem, ki razpolagajo z zaupnimi informacijami. Na primer, znano je, da podjetje RRC nudi storitev upravljanja podatkov Davčne uprave RS (DURS). Posledice, ki bi nastale zaradi kršitve zaupnosti podatkov in morebitnih odškodninskih tožb, bi lahko bile nepredstavljivo visoke. Zaradi tega razloga menimo, da bi posledice scenarija imele **visok do zelo visok vpliv** na poslovanje podjetja.

		Verjetnost scenarija incidenta				
		Zelo neverjetno	**Neverjetno**	**Možno**	**Verjetno**	**Zelo verjetno**
Vpliv na poslovanje	**Zelo nizko**	0	1	2	3	4
	Nizko	1	2	3	4	5
	Srednje	2	3	4	5	6
	Visoko	3	4	5	6	7
	Zelo Visoko	4	5	6	7	8

Tabela 11: Vrednotenje tveganja podjetja RRC d.o.o. za scenarij »Vdiralec«

Zgornja tabela prikazuje interval ocene tveganja RRC d.o.o. za scenarij »Vdiralec« in je z izjemo enega primera vrednotena kot **visoko tveganje**.

Zaključek

Pravna služba podjetja HID je zelo kompetentna in uspešno varuje poslovni model prodaje zastarele varnostne tehnologije, pri nastanku katere so bili varnostni pomisleki sekundarnega pomena. V podjetju HID s pravnimi manevri njim v prid vzdržujejo asimetrijo informacij. Ranljivosti sistema so na ta način poznane podjetju samemu, redkim posameznikom in seveda tistim, ki imajo motiv in voljo sistem zlorabiti. Tehnično predznanje napadalca tukaj ne igra velikega pomena, saj je mogoče orodja za vdor nabaviti kar preko spleta.

Podjetje HID je še pred demonstracijo Westhuesa in Pageta objavilo poročilo [9], v katerem želimo izpostaviti spodnji citat.

»These security measures are not implemented in proximity cards, giving contactless smart cards a significant security advantage.«[2]

Naša domneva je, da se je podjetje HID zavedalo ranljivosti sistema od samega začetka naprej in da je s tem dokumentom želelo prenesti tveganje na končne uporabnike sistema po načelu »Bili ste obveščeni in vedeli ste, v kaj ste se spustili.«

Povzetek rezultatov

Rezultat prepoznavanja tveganja je prepoznavanje pomanjkljivosti informacijskega sistema nadzora fizičnega dostopa v prostore RRC s sistemom kartice HID Indala FlexCard in prepoznavanje ponesrečene sistemske integracije sistema nadzora fizičnega dostopa z alarmnim sistemom.

Pri okvirni oceni tveganja za namišljen scenarij »Vdiralec« nas preseneča zanemarljivi finančni vložek napadalca (< 100 €) in zelo velik učinek napada ($\gg 100000$ €). Pričakovan faktor dobičkonosnost naložbe napadalca ROI znaša tako najmanj:

$$ROI_{napadalec} > \frac{(Dobiček[€] - Vložek[€])}{Vložek[€]} \cong 999 \qquad (1)$$

Faktor dobičkonosnosti napadalca[3] $ROI_{napadalec} > 999$ in zgodovina vlomov v prostore podjetja RRC so resen varnostni indikator za povečano tveganje poslovanja vseh podjetij, ki delujejo v prostorih RRC.

[2] Po [22] se izkaže, da je standardna postavitev sistema HID iClass »Standard Security« ranljiva, saj ključ za 3DES ni tajen in je »standarden« v vseh napravah. Ta napaka popolnoma razvrednoti pojem »Standard Security«. Žal, tudi protokol kartice ni brez napake, saj ne pozna overjanja sporočil. To ga izpostavi za napad z možem na sredini v vseh ti. »varnostnih načinih delovanja« HID iClass.

[3] To nas spominja na podoben, a nepovezan dogodek informacijske varnosti v ameriški vojski [26], kjer je vrednost faktorja ROI prav tako bila velika številka. S ceneno opremo je bilo mogoče zlorabiti varnostno luknjo dragega sistema.

Podjetju RRC zato priporočamo sprožitev faze **ukrepaj** v okviru njihovega lastnega sistema SUVI in uporabo procesa obvladovanja tveganja za varovanje informacij (glej Slika 11) zaradi:

a) lastne skrbnosti za minimizacijo tveganja informacijske varnosti RRC,
b) dolžnosti skrbnosti za minimizacijo tveganja informacijske varnosti njihovih poslovnih partnerjev in
c) dolžnosti skrbnosti za minimizacijo tveganja informacijske varnosti predpisano s strani zakonodajalca.

Priporočila za obravnavo tveganja

V okviru sproženega procesa obvladovanja tveganja za varovanje informacij s strani podjetja RRC ponujamo naslednja priporočila pri procesu obravnave tveganja:

1. Zadržanje tveganja je najmanj priporočljivo, saj bi ta izbira ohranila obstoječe nezadovoljivo stanje.

2. Prenos tveganja se doseže z zavarovanjem, vendar se je pri tej izbiri potrebno zavedati, da vsega ni mogoče zavarovati in zavarovalnica škode v celoti ne povrne, ampak le ocenjeno trenutno vrednost sredstva.

3. Izognitev tveganju predstavlja zadržanje obstoječega sistema in najem komplementarne rešitve, npr. fizičnega varovanja vse dni in vse ure v letu.

4. Zmanjšanje tveganja se doseže:

    a) z namestitvijo protiukrepov, ki bi omogočali varno uporabo obstoječe sistema:

        - Namestitvijo Faradayeve kletke v področje kartice in v delovno področje čitalca za elektromagnetno ločitev dveh fizičnih domen. Fizično varovanje prostora bi zagotavljal lastnik kartice, ki je hkrati tudi uporabnik čitalca.

          Medtem ko je namestitev takšne kletke v delovno področje čitalca strokovno opravilo, ki ga izvede strokovnjak (na primer slovensko podjetje Miška http://www.miska.si), je namestitev kletke v področje kartice enostavnejše. Zadostuje nakup zaščitnih folij za kartice (na primer http://www.rfid-shield.com/). Kartico se ob uporabi izvleče iz folije in po uporabi pospravi nazaj.

          Navedene tehnične ukrepe bi bilo v nadaljevanju potrebno podkrepiti z varnostnim izobraževanjem uporabnikov tega sistema.

        - Oklopljen kabel med čitalcem in zalednim delom sistema, katerega notranji vodniki so zaščiteni s prevodno folijo, tj. Faradayovo kletko za elektromagnetno ločitev dveh fizičnih domen. Idealno bi tak kabel še

vseboval stikalo proti vtikanju (*angl.* tamper switch). Fizično varnost bi zagotavljala vgradnja kabla v betonsko steno.

b) ali z zamenjavo obstoječega sistema:

   - pri čemer se pri naročilu varnostne opreme eksplicitno navedeta dva varnostna kriterija porazdeljenega sistema nadzora fizičnega dostopa: zagotavljanje celovitosti in zaupnosti sistema.

Za konec ponovno izpostavimo, da prepoznani ranljivosti v protokolu kartice in čitalca ter ponesrečena sistemska integracija z alarmnim sistemom predstavljata nizko viseče sadje na dosegu hekerjeve roke.

Ocena tveganja za uporabo obstoječega sistema za nadzor dostopa je srednje do visoko tvegana in prepričani smo, da bi se v tem trenutku sistem s ključem in ključavnico obnesel mnogo bolje. Prikazane metode napada puščajo vhodna vrata v prostore široko odprta.

Jonatan Westhues je demonstriral vdor v enak sistem na sedežu zvezne vlade Kalifornije ZDA leta 2006. Fakulteta za računalništvo in informatiko je podala oceno tveganja tega sistema leta 2011. Vrata v stavbo so široko odprta že 5 let. Odgovornost podjetja RRC je, da ukrepa in zavaruje skupne interese. Nočemo reprize demonstracije vdora; tokrat v črni kroniki.

Literatura

1. RFID @ wiki.yobi.be. http://wiki.yobi.be/wiki/RFID.

2. proxmark3: Firmware development for the Proxmark3 3 RFID device. http://code.google.com/p/proxmark3/wiki/HomePage.

3. Proxmark3. http://www.proxmark3.com/.

4. Proxmark3 "RFID Survival Kit": Here Be Dragons Edition - 26C3. http://hackable-devices.org/products/product/proxmark3/.

5. Anderson, R. Responsible disclosure and academic freedom. 2010. http://www.cl.cam.ac.uk/~rja14/Papers/20101221110342233.pdf.

6. Dolev, D. and Yao, A.C. On the security of public key protocols. *22nd Annual Symposium on Foundations of Computer Science (sfcs 1981)*, (1981), 350-357.

7. Franken, Z. Access Control Devices. *LayerOne*, 2007. http://layerone.info/?page_id=9.

8. Franken, Z. Biometric and Token-Based Access Control Systems. 2008. https://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf.

9. HID. *Smart Cards for Acces Control: Advantages and Technology Choices*. 2005.

10. HID. *Understanding Card Data Formats*. 2006.

11. HID. HID GLOBAL CORPORATION's Intellectual Property. 2007.

12. HID. *HID Global Product Catalog: 125 kHz Proximity Cards and Readers*. 2008.

13. ISO/IEC. *ISO/IEC 7498-1:1994, Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model*. ISO/IEC, 1994.

14. ISO/IEC. *ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements*. ISO/IEC, 2005.

15. ISO/IEC. *ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management*. ISO/IEC, 2005.

16. ISO/IEC. *ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management*. ISO/IEC, 2008.

17. ISO/IEC. *ISO/IEC 27000:2009, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. ISO/IEC, 2009.

18. Johnson, M. Responsible Disclosure Pratice. 2010. http://www.cl.cam.ac.uk/~rja14/Papers/20101221110342233.pdf.

19. Juels, A. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications 24*, 2 (2006), 381-394.

20. Lehpamer, H. *RFID Design Principles (Artech House Microwave Library)*. Artech House Publishers, 2007.

21. Mandel, J., Roach, A., and Winstein, K. MIT Proximity Card Vulnerabilities. 2004. http://josephhall.org/tmp/mit_prox_vulns.pdf.

22. Meriac, M. and Plotz, H. Analyzing a Modern Cryptographic RFID System. *27th Chaos Communication Congress: "We come in peace"*, 2010. http://events.ccc.de/congress/2010/Fahrplan/attachments/1784_HID-iClass-27C3.pdf.

23. Paget, C. RSA: Door cards - the enterprise's weakest link. http://www.infoworld.com/ifwclassic/video/archives/2007/02/rsa_ioactive.html.

24. Republika Slovenija. Zakon o elektronskih komunikacijah (uradno prečiščeno besedilo) (ZEKom-UPB1). *Uradni list Republike Slovenije*, 13 (2007), 44.

25. Schneier, B. Cloning RFID Chips Made by HID. *Crypto-Gram Newsletter*, 2007. http://www.schneier.com/blog/archives/2007/02/cloning_rfid_ch_1.html.

26. Shachtman, N. Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video). *Wired*, 2009. http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

27. Westhues, J. Cloning RFID Tags in Sacramento. 2006. http://www.youtube.com/watch?v=4jpRFgDPWVA.

28. Westhues, J. Cq.cx: Prox / RFID mark 3. http://www.cq.cx/proxmark3.pl.