Elektrotehniški vestnik 74(3): 131-137, 2007
Electrotechnical Review: Ljubljana, Slovenija

Pregled zlorab IKT in njihovo odkrivanje s pomočjo dvosmernih umetnih nevronskih mrež

Andrej Krenker, Matevž Mesojednik, Mojca Volk, Janez Bešter, Andrej Kos

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana, Slovenija
E-pošta: andrej.krenker@ltfe.org

Povzetek. Življenje in delovanje posameznika in družbe je v razvitem svetu močno odvisno od delovanja informacijsko-komunikacijskih tehnologij (IKT), sistemov in storitev. Zaradi kompleksnosti in zahtevnosti tehnologije, potreb po združevanju različnih sistemov, zahtev po čim krajšem roku prihoda proizvodov oziroma storitev na trg, boljših ali slabših standardov in nezadostnega testiranja končnih izdelkov so takšni sistemi ranljivi za zlorabe. Za uspešno zaščito pred zlorabami IKT je le-te najprej treba identificirati ter jih dobro poznati. S tem namenom v tem prispevku predstavljamo osnovne in najpogostejše zlorabe v IKT in metode, ki se uporabljajo za njihovo odkrivanje in preprečevanje. Vsaka zloraba sistemov IKT in storitev je specifična, vendar imajo določene zlorabe nekatere skupne lastnosti, kot na primer način zlorabljanja ali pa točno določen del sistema, ki ga zlorabljajo. Zaradi preprostejšega obravnavanja zlorab in poznejšega odkrivanja in preprečevanja posamezne zlorabe združimo v skupine. Strokovna literatura najpogosteje navaja delitev zlorab na kloniranje mobilnih terminalov, zlorabo pri zaračunavanju storitev, naročniško zlorabo, socialni inženiring, računalniške vdore in zlorabe kreditnih kartic. Odkrivanje in preprečevanje zlorab v sodobnih telekomunikacijah, še posebej pa v omrežjih nove generacije, postaja ključen in neizogiben element širše infrastrukture. Metode za odkrivanje zlorab IKT se že nekaj časa močno opirajo na umetne nevronske mreže. V tem prispevku predlagamo za odkrivanje zlorab IKT uporabo naprednih dvosmernih umetnih nevronskih mrež, ki so bile sicer razvite za druge namene. V prispevku podajamo osnovni princip delovanja dvosmernih umetnih nevronskih mrež in njihovo vključitev v celoten sistem za odkrivanje zlorab IKT. Na koncu predstavimo še njihovo primernost uporabe pri odkrivanju posameznih zlorab IKT.

Ključne besede: kloniranje mobilnih terminalov, zloraba pri zaračunavanju storitev, naročniška zloraba, socialni inženiring, računalniški vdori, zloraba kreditnih kartic, dvosmerne umetne nevronske mreže

An Overview of ICT Frauds and their Detection with Bi-directional Artificial Neural Networks

Extended abstract. Life and work of individuals and the overall society have become strongly dependant on information communication technology (ICT) systems and services. Due to their complexity, pretentiousness, need of convergence, demand to reduce the time-to-market for new products and services, quality of standards and insufficient testing of end products, ICT systems are vulnerable to frauds. To prevent ICT frauds, it is necessary to identify and know them well. For this purpose we present the most usual and the most frequent ICT frauds and examples and methods used for their detection. Though every ICT fraud is specific, they altogether still have certain common properties, according to which we group them. In literature, ICT frauds are grouped into cloning fraud, toll fraud, subscriber fraud, social engineering fraud, computer intrusion fraud and credit card fraud. They are all discussed in this paper. Methods for detecting ICT frauds have been using artificial neural networks for quite some time. Instead of them we propose to employ sophisticated bi-directional artificial networks that were initially developed for other purposes. We introduce their basic working principle and their incorporation into the system for detecting ICT frauds. In the last section we discuss their adequacy for detecting individual ICT frauds.

Keywords: cloning fraud, toll fraud, subscriber fraud, social engineering fraud, computer intrusion and credit card fraud, bi-directional artificial neural network.

Prejet 9. oktober, 2006
Odobren 5. december, 2006

1. Uvod

Življenje v razvitem svetu je čedalje tesneje prepleteno z IKT, pri tem pa se premalo zavedamo, kakšno potencialno grožnjo pomeni ta tehnologija. Z razvojem novih sistemov IKT, omrežij in storitev nove generacije (NGN) ter seljenjem čedalje več aktivnosti posameznika in družbe na sisteme IKT moramo pričakovati tudi čedalje več zlorab IKT, ki ogrožajo način njihovega delovanja in njihov finančni obstoj.

Zloraba na področju IKT se zgodi, ko oseba z goljufijo uporablja storitve, ne da bi zanje v celoti ali vsaj delno plačala. Zlorabe IKT so globalni problem in po ocenah evropskega združenja Communication Fraud Control Association znašajo od 3 do 8 odstotkov letnega prihodka telekomunikacijske panoge [14], v nerazvitih državah pa celo do 20 odstotkov [14], [17]. Ti odstotki pomenijo nekaj deset milijard ameriških dolarjev na letni ravni. Odstopanja v ocenah zlorab nastopijo zato, ker nekaterih zlorab nikoli ne odkrijemo, zaradi različnih kriterijev pri postopku ocenjevanja in zaradi skrivanja slabih rezultatov, ki bi lahko škodovali ugledu izdelovalcev in ponudnikov telekomunikacijskih rešitev oziroma storitev.

Zlorabe na področju IKT se izvajajo na razne načine in z različnimi nameni, na podlagi katerih so nastale različne klasifikacije zlorab. V literaturi (npr. [11], [8], [18]) se najpogosteje uporablja klasifikacija, ki deli zlorabe na (slika 1):

- kloniranje mobilnih terminalov,
- zlorabe pri zaračunavanju storitev,
- naročniške zlorabe,
- socialni inženiring,
- računalniške vdore in
- zlorabe kreditnih kartic.

Zaradi pogostosti zgoraj uporabljene klasifikacije smo v nadaljevanju predstavili posamezne skupine teh zlorab, pri tem pa se je treba zavedati, da obstajajo še druge klasifikacije, kot na primer delitev na tehnične in netehnične zlorabe, na zlorabe, ki prizadenejo posameznika, in na zlorabe, ki prizadenejo ponudnika storitve, ali pa na skupine zlorab, kjer je napaden natančno določen element sistema IKT, oziroma na skupino zlorab, pri katerih je bila uporabljena natančno določena metoda.

2. Predstavitev zlorab

2.1 Kloniranje mobilnih terminalov

Kloniranje SIM kartic mobilnih terminalov je zloraba, ki se ponovno širi [21]. Te zlorabe omogočajo zlorabljevalcu, da opravi klice, s katerimi lahko naredi velike stroške mobilnemu operaterju oziroma uporabniku, čigar SIM kartica je bila klonirana. Osnovna ideja pri kloniranju mobilnih terminalov je zajemanje in snemanje signalov ter dešifriranje kodirnih algoritmov, ki se uporabljajo pri pošiljanju in sprejemanju informacij z mobilnim terminalom. Za zlorabo prvotnih sistemov so zlorabljevalci potrebovali osem ur (zajem in dešifriranje signalov). Kljub uvedbi naprednejših kodirnih algoritmov so zaradi razvoja tehnologije, ki jo uporabljajo zlorabljevalci v današnjem času, le-ti sposobni zlorabiti sistem že v nekaj minutah. Prvotno so bili te vrste zlorab le telefonski klici, z razvojem m-bančništva pa je ta problem postal bolj pereč. V tem primeru lahko zlorabljevalec pridobi v zelo kratkem času materialne dobrine velike vrednosti.

Slika 1: Delitev zlorab IKT in njihova umestitev glede na (ne)uporabo tehnologij

Ker se tovrstne zlorabe najpogosteje odkrijejo pri izstavljanju računov naročnikom, ki so bili oškodovani, je pri uspešnem in dolgoročnem izvajanju tovrstnih zlorab potrebna dobra strategija, ki upošteva tudi psihološke vidike. Zlorabljevalci čedalje pogosteje klonirajo SIM kartice službenih mobilnih terminalov posameznikov, ki so zaposleni v velikih podjetjih in političnih organizacijah. Še posebej zanimive tarče so vodilne osebe, katerih podrejeni in odgovorni za poravnavo računov v podjetjih si od njih ne upajo zahtevati obrazložitev velikega števila opravljenih klicev in izklop njihovega mobilnega terminala. V publikaciji [19] je opisan primer, kako se je tega načina posluževala teroristična skupina za opravljanje mednarodnih klicev.

Metode za odkrivanje tovrstnih zlorab temeljijo na dveh različnih postopkih. Prvi postopek temelji na analizi podatkov TT (Toll Tickets). Cilj teh postopkov je ugotoviti, ali so bili izvedeni sočasni klici ali sta bila dva klica posameznega uporabnika izvedena v zelo kratkem času na zelo oddaljenih lokacijah (metodi prekrivanja in hitrostne pasti), kar nedvoumno nakazuje na to, da obstajata dva mobilna terminala z isto telefonsko številko. Ti postopki ne potekajo v realnem

času. Druga vrsta postopkov pa temelji na odkrivanju zlorab v realnem času. Uporabljen je tako imenovani sistem elektronskih prstnih odtisov [6]. Ta sistem posname elektronski prstni odtis mobilnega terminala in njegovo informacijo poveže s SIM kartico. Na splošno lahko rečemo, da ima vsak mobilni terminal ob vzpostavitvi klica drugačne časovne karakteristike. Če sistem zazna drugačno karakteristiko terminala v povezavi z določeno SIM kartico, označi ta mobilni terminal za nelegitimnega in prepreči uporabo storitve. Ti sistemi so veliko bolj primerni in prijazni do uporabnika kot sistemi, ki so zahtevali vnos posebnih kod uporabnika za vsak klic posebej. Sistemi z elektronskimi prstnimi odtisi naj bi bili sposobni zmanjšati tovrstne zlorabe za 85 odstotkov [23].

2.2 Zloraba pri zaračunavanju storitev

Zloraba pri zaračunavanju storitev je definirana kot nedovoljena uporaba telefonskega sistema posameznega podjetja. Pomeni krajo medoperaterskih klicev s strani zunanjih oseb, oseb zaposlenih pri operaterjih, in oseb, ki so zaposlene v podjetjih. Najpogosteje uporabljane metode za izvršitev teh zlorab so dostop prek brezplačnih linij, manipulacija PBX (Private Branch Exchange), vdor v sistem govornih sporočil, manipuliranje s podatki CDR (Call Detail Record), uporaba porta za vzdrževanje PBX, zloraba oddaljenega dostopa do PBX in zloraba uslužbencev. Zlorabljevalec lahko že v eni uri vdre v sistem in izvaja takšno zlorabo. Tovrstne zlorabe se dogajajo med delovnim časom oziroma takrat, ko je PBX prometa veliko, kar omogoča, da te zlorabe ostanejo neopažene. Zlorabljevalec pridobi telefonske kode za dostop do central PBX najpogosteje z metodami socialnega inženiringa ali pa jih preprosto pridobi na internetu in v raznih glasilih, ki jih objavljajo zlorabljevalci teh sistemov. Nedovoljeno pridobivanje kod za dostop do PBX in njihova preprodaja je za zlorabljevalce izredno zanimiva, ker ima ena sama koda na črnem trgu vrednost od 3000 do 5000 ameriških dolarjev. V publikaciji [24] ocenjujejo, da naj bi samo v Združenih Državah Amerike tovrstne zlorabe pomenile več kot milijardo dolarjev na leto.

Leta 1990 je Kevin Poulsen s tem, ko je prevzel nadzor nad telefonsko centralo radijske postaje, prevzel in blokiral vse njene dohodne klice – razen svojega, ki so bili namenjeni za sodelovanje v nagradni igri, in tako zmagal ter si »priigral« avtomobil znamke Porsche 944 S2. Z zlorabami je nadaljeval in dobil še drugi Porsche, 22000 ameriških dolarjev, dve potovanji na Havaje ter tri leta zapora [16].

Metoda odkrivanja teh zlorab je metoda rudarjenja podatkov, ki pa se ne odvija v realnem času. Za preprečevanje teh zlorab je potrebno predvsem kakovostno izobraževanje uporabnikov in skrbnikov central PBX o načinih nastajanja in izvajanja tovrstnih zlorab.

2.3 Naročniška zloraba

Definicija naročniških zlorab je pridobitev storitve z navajanjem lažnih osebnih podatkov brez namena poravnanja stroškov, ki nastanejo pri uporabi te storitve. Značilnost teh zlorab je, da jih zaznajo v povprečju od 70 do 100 dni po tem, ko so se zgodile [15]. Pomembno je poudariti, da neizterjani dolgovi znanih uporabnikov ne spadajo v to vrsto zlorab. To ni tehnična zloraba, pri njej pa podjetniško naravnan zlorabljevalec v zelo kratkem času pridobi velik prihodek ob relativno majhnih investicijskih stroških [3].

Če se želijo ponudniki storitev obvarovati pred tovrstnimi zlorabami, je edini način uvedba novih naprednih sistemov, ki omogočajo ocenitev nevarnosti za zlorabo že pri sklenitvi naročniškega razmerja med uporabnikom in ponudnikom storitev. Pri tem so uporabljene metode, ki temeljijo na umetnih nevronskih mrežah ter mehki logiki oziroma kombinaciji obojih. Takšni sistemi omogočajo analizo podatkov, ki jih navede nov naročnik. Znano je namreč, da zlorabljevalci pogosto na prijavnih obrazcih večkrat uporabijo iste ali zelo podobne podatke. Po končanem prijavnem postopku nadziramo novega uporabnika storitve. Če ima oseba, ki je prvič sklenila naročniško razmerje, zelo veliko porabo, lahko to že zbudi sum o morebitni naročniški zlorabi.

2.4 Socialni inženiring

Pri socialnem inženiringu je zlorabljeno posameznikovo zaupanje. Pri teh zlorabah zlorabljevalci pridobivajo pomembne informacije, za katere ljudje ponavadi ne mislijo, da bi bile lahko pomembne. Socialni inženiring različni avtorji definirajo drugače [2], [12], [22], vsi pa se strinjajo, da je na splošno socialni inženiring spretna manipulacija s človeškim nagnjenjem do zaupanja. Tarče takšnih napadov so ponavadi velika telekomunikacijska podjetja, korporacije, vojska, zdravstvo in druge vladne institucije. Razširjenost teh zlorab je posledica relativne preprostosti v primerjavi z drugimi tehničnimi načini vdora in zlorabe sistemov.

Eden izmed načinov uporabe socialnega inženiringa je pridobivanje podatkov po telefonu. V tem primeru zlorabljevalec klicanim ponudi pomoč in podporo, pri čemer mu morajo uporabniki v zameno zaupati uporabniška imena in gesla. Drug način pridobivanja podatkov je iskanje zavrženih priročnikov, spominskih enot, odslužene strojne opreme, pomembnih dokumentov, koledarjev prireditev, internih telefonskih imenikov, dopisov in raznih zapiskov. Skratka vse, kar lahko je morebiten vir informacije o sistemu oziroma načinih za vstop v te sisteme. Tretji način je tako imenovani »on-line« socialni inženiring. Gre za pridobivanje informacij s pomočjo interneta. Najprej zlorabljevalci pridobivajo informacije o uporabniških imenih in geslih za dostope do elektronske pošte in podobnih javnih spletnih storitev, ki so praviloma laže

dostopne. Nato se uporabniku pošlje elektronska ali klasična pošta, kjer navedejo različne razloge za pridobitev njihovih uporabniških imen in gesel. V četrtem načinu zlorabljevalec pridobiva zaupanje osebe, od katere namerava pridobiti določene informacije. S posameznikom se spoprijateljijo ali pa se izdajajo za njegovega znanca. Pri petem načinu se zlorabljevalec predstavi kot nadrejena oseba, ki jo zaposlena oseba sprašuje o podatkih, ki naj jih uporabi za upravljanje sistema IKT (npr. dodajanje novih uporabniških imen in gesel).

V praksi zlorabljevalci združujejo vse zgoraj naštete prijeme socialnega inženiringa. V publikaciji [20] je predstavljen primer, ko je pred leti nekaj posameznikov vkorakalo v veliko podjetje in v nekaj urah pridobilo popoln nadzor nad njihovim informacijskim omrežjem. Pred samim prihodom v podjetje so s pomočjo telefonskih imenikov in telefonskih klicev v podjetje pridobili informacije, kdo so vodilni v podjetju in kdaj bodo odsotni. V zgradbo in njene dele so prišli s pretvezo, da so izgubili identifikacijske priponke. V praznih pisarnah so z odklenjenih računalnikov pridobili uporabniška imena. Pomembne dokumente so v košu za smeti odnesli iz stavbe. Po telefonu so se izdajali za nadrejenega, ki nujno potrebuje novo uporabniško ime in geslo. Na srečo podjetja so bili to samo svetovalci za varnost, ki so testirali varovanje v podjetju.

Pri napadih s pomočjo socialnega inženiringa ne moremo nadgraditi varnostnih sistemov v tehnološkem pogledu. Treba je imeti dobro varnostno politiko, ki se izvaja strogo, dosledno in brez izjem. Mila varnostna politika pomeni visoko stopnjo tveganja zlorab, medtem ko preveč natančna varnostna politika prinese v poslovni proces podjetja velike nevšečnosti. Na drugem mestu je potrebno dobro fizično varovanje zgradb in sistemov IKT. V zgradbe in prostore ne smemo spuščati nepooblaščenih oseb, moramo pa tudi onemogočiti odtujitev strojne opreme oziroma dokumentov iz prostorov. Za uspešno varovanje pred socialnim inženiringom je potrebno dobro izobraževanje uslužbencev. Uslužbenci morajo vedeti, kdo in kako je upravičen do njihovih uporabniških imen in gesel ter drugih informacij. Zaposleni se morajo zavedati, da nikoli ne smejo dajati občutljivih informacij osebam, ki se ne držijo za to predpisanih postopkov.

2.5 Računalniški vdori

Računalniške sisteme lahko na splošno delimo na žične in brezžične. Vdori v obe vrsti omrežij so si zelo podobni. Edina razlika je v dostopu do fizičnega medija, po katerem poteka komunikacija med posameznimi elementi omrežja. Pri brezžičnih računalniških sistemih je zaradi narave tehnologije takšne napade nekoliko laže izvesti. Prispevek [14] govori o osmih vrstah računalniskih vdorov, tri najpogostejše so opisane v nadaljevanju: napadi zavrnitve storitve, mož v sredini in razbijanje ključa WEP (Wired Equivalent Privacy).

Namen napadov zavrnitve storitve je preprečitev dostopa do storitve vsem uporabnikom. Običajna metoda takšnih napadov je poplavljanje omrežja s protokolnimi sporočili, ki preplavijo legitimna sporočila. Napadeni sistemi niso več zmožni obdelovati tolikšnega števila zahtev, kar povzroči njihovo neodzivnost. Najpogostejši način izvedbe tega napada v brezžičnih sistemih je postavitev anten, katerih signali so veliko močnejši od signalov anten, na katerih opravljajo določeno storitev, v žičnih pa preprosta priključitev na omrežje. Pri napadih tipa »mož v sredini« obstajata dve obliki teh napadov, prisluškovanje in manipulacija. Pri prisluškovanju napadalec preprosto posluša sporočila, ki se prenašajo po povezavi med uporabnikom in ponudnikom storitve. Pri manipulaciji povezave pa napadalec nadomesti legitimnega uporabnika in sam uporablja storitev. Pri razbijanju ključa WEP je uporabljeno preprosto dejstvo, da kodirni ključi niso dovolj močni. Zaradi neprimernosti teh ključev danes poteka pospešen razvoj novih sistemov za kodiranje. Posebne vrste napadov so še računalniški virusi, črvi in trojanski konji ter nezaželena sporočila.

Pri pridobivanju zaupnih informacij iz računalniških sistemov je edina morebitna sled, ki jo pusti oseba, ki je vdrla v računalniški sistem, zaporedje ukazov, ki so bili potrebni za vdor. Zato poznavalci, ki poskušajo zaščititi računalniški sistem, v večini primerov uporabljajo tehniko analize zaporedij. Metode, ki se uporabljajo za odkrivanje vdorov v računalniški sistem, najpogosteje temeljijo na skritih Markovih modelih in metodah, ki delujejo na podoben način kot biološki imunski sistem.

2.6 Zlorabe kreditnih kartic

Najpreprostejša zloraba je kraja kreditne kartice. Zloraba pri zaprošanju za kreditno kartico se zgodi, ko posameznik v prošnji za pridobitev nove kreditne kartice navede lažne osebne podatke. Zloraba, pri kateri ni potrebna prisotnost zlorabljevalca oziroma lastnika kreditne kartice, se izvede na podlagi podatkov, zapisanih na površini kreditne kartice. Takšne transakcije zajemajo nakupe po telefonu oziroma interneta in pomenijo večinski delež pri zlorabah kreditnih kartic. Način, kako zlorabljevalci pridejo do teh informacij, je nedovoljeno kopiranje kreditnih kartic, pridobivanje informacij s preprostim opazovanjem kartic pri blagajnah in čakalnih vrstah ter izdajanje za uslužbenca podjetja, ki je izdalo kreditno kartico.

Pri zlorabah, pri katerih zlorabljevalci pridobijo kreditne kartice na podlagi lažne identitete, si lahko pomagamo z ocenjevalnimi točkami [7], ki nam omogočajo odkrivanje lastnikov kreditnih kartic, ki najverjetneje ne bodo izpolnili obveznosti. Ocenjevalne točke se izračunajo na podlagi podatkov, ki jih poda lastnik kreditne kartice na prijavnem obrazcu. Odkrivanje zlorab kreditnih kartic, pri katerih ni

potrebna fizična prisotnost lastnika, se ugotavlja z odkrivanjem sprememb v načinu uporabe kreditne kartice. Podjetje, ki je lastnik kreditne kartice, ima v svojih podatkovnih bazah shranjene vse transakcije vseh posameznikov. Te informacije se primerjajo z vsako novo transakcijo in če je odstopanje preveliko, je transakcija zavrnjena. Najpogosteje uporabljene metode za reševanje zgoraj omenjenih problemov so metode na podlagi pravil in umetnih nevronskih mrež (metode z nadzorovanim učenjem). Uporaba umetnih nevronskih mrež za odkrivanje zlorab kreditnih kartic je podrobneje opisana v delih [1], [4], [5] in [10].

3. Uporaba dvosmernih umetnih nevronskih mrež

Ena izmed metod odkrivanja zlorab IKT, ki ne potekajo v realnem času, je uporaba uporabniških profilov, v katerih je zapisano obnašanje uporabnikov. Na podlagi shranjenih informacij v uporabniških profilih lahko sklepamo, kakšno bo obnašanje uporabnikov v prihodnosti.
Če pride do odstopanj v napovedanih vrednosti in dejanskih vrednosti, lahko z določeno gotovostjo trdimo, da je prišlo do zlorabe. S kakšno gotovostjo pa lahko to trdimo, je odvisno od uporabljene metode napovedovanja prihodnjih vrednosti. Kot metodo za napovedovanje prihodnjih vrednosti predlagamo uporabo dvosmernih umetnih nevronskih mrež.

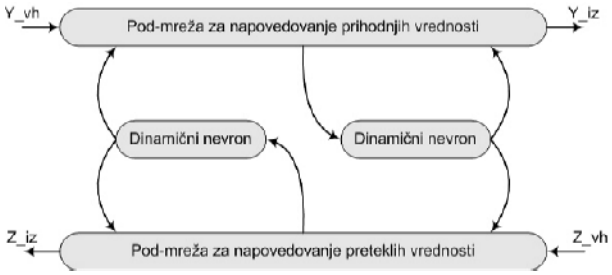
3.1 Dvosmerne umetne nevronske mreže

Dvosmerne umetne nevronske mreže se uporabljajo za napovedovanje prihodnjih vrednosti, zato so primerne za uporabo pri metodah odkrivanja zlorab IKT s pomočjo uporabniških profilov. Dvosmerne umetne nevronske mreže so sestavljene iz dveh posameznih klasičnih umetnih nevronskih mrež, ki sta med seboj povezani. Spadajo v družino dinamičnih umetnih nevronskih mrež. Ena podmreža napoveduje prihodnje vrednosti, druga pa napoveduje pretekle vrednosti. Podmreži sta med seboj povezani z vmesnima dinamičnima nevronoma, ki služita kot pomnilniška elementa in shranjujeta informacijo o preteklih vrednostih v obliki notranjih stanj. Arhitektura dvosmerne umetne nevronske mreže je prikazana na sliki 2.

3.2 Predlagan model sistema odkrivanja zlorab IKT

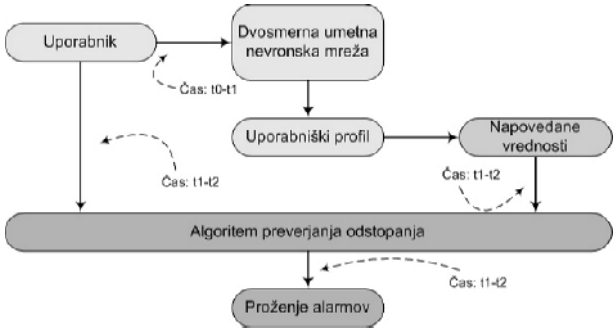
Predpogoj za uporabo dvosmernih umetnih nevronskih mrež pri odkrivanju zlorab IKT je pravilna interpretacija in predstavitev parametrov sistema IKT, ki jih nadzorujemo in pripeljemo na vhod dvosmerne umetne nevronske mreže. Dvosmerne umetne nevronske mreže obravnavajo vhodne parametre kot časovne vrste. Vsak parameter sistema IKT, ki ga spremljamo, vstavimo v svojo časovno vrsto. Umetna nevronska mreža pa nato napove izhodno časovno vrsto, v kateri so zapisane napovedane vrednosti parametra. Vsi parametri morajo biti zapisani oziroma predstavljeni s številskimi vrednostmi.

Na sliki 3 je predlagan konceptualni model sistema za odkrivanje zlorab IKT na podlagi dvosmernih umetnih nevronskih mrež, ki omogoča napovedovanje prihodnjih vrednosti parametrov sistema IKT in njihovo poznejšo primerjavo z dejanskimi vrednostmi.



Slika 2: Arhitektura dvosmerne umetne nevronske mreže

Model predvideva v prvem koraku (v času od t_0 do časa t_1) spremljanje uporabnikovih navad pri uporabi določene storitve IKT in kreiranje uporabniških profilov. Pri uporabi storitev IKT lahko spremljamo različne parametre, v uporabniške profile pa shranjujemo samo najpomembnejše. V tem koraku po potrebi tudi transformiramo zapis parametrov v obliko, ki jo zahteva dvosmerna umetna nevronska mreža. V drugem koraku napovemo vrednosti parametrov za čas od t_1 do t_2. V tretjem koraku preverjamo obnašanje uporabnika v času od t_1 do t_2 in pri odstopanju med izmerjenimi in napovedanimi vrednostmi sprožimo opozorila in alarme. Pri tem pa nenehno osvežujemo uporabniške profile.



Slika 3: Sistem za odkrivanje zlorab s pomočjo dvosmernih umetnih nevronskih mrež

3.3 Odkrivanje zlorab IKT z dvosmerno umetno nevronsko mrežo

Pri zlorabah IKT je najbolj opazna sprememba v načinu uporabe storitve posameznika, katerega napadejo zlorabljevalci. Pri zlorabi, kot je kloniranje mobilnih

terminalov, so najbolj opazne spremembe v številu in dolžini posameznih klicev ter lokacije, s katerih in v katere so bili klici opravljeni. Zloraba pri zaračunavanju storitev se najizraziteje kaže v spremembi klicanih številk, to so najpogosteje klici, opravljeni v druga telekomunikacijska omrežja in države. Pri zlorabi socialni inženiring so karakteristike, ki nam povedo, da se je takšen napad izvedel, odvisne od tehničnega sistema, ki so ga napadli s tovrstno zlorabo. V teh primerih lahko pride do povečanega odstopanja v številu in dolžini opravljenih klicev ter lokacij, iz katerih in v katere so bili klici opravljeni. Pri zlorabah kreditnih kartic pa je najpogosteje opazno občutno povečanje števila opravljenih transakcij, njihova vrednost ter številna nova nakupovalna mesta. Iz karakteristik posameznih zlorab lahko ugotovimo, katere zlorabe lahko odkrivamo s pomočjo uporabe dvosmernih nevronskih mrež (tabela 1).

Zloraba	**Primernost & Spremembe**	
Kloniranje mobilnih terminalov	DA	V številu in dolžini posameznih klicev ter lokacije, s katerih in v katere so bili klici opravljeni.
Zloraba pri zaračunavanju storitev	DA	V klicanih številkah, ki so najpogosteje v drugih telekomunikacijskih omrežjih in državah.
Naročniška zloraba	NE	-
Socialni inženiring	DA	V številu in dolžini opravljenih klicev, lokacij, iz katerih in v katera so bili opravljeni klici.
Računalniški vdori	MANJ	V zaporedju ukazov.
Zloraba kreditnih kartic	DA	Število opravljenih transakcij, njihova vrednost in nakupovalna mesta.

Tabela 1: Primernost uporabe dvosmernih nevronskih mrež pri različnih vrstah zlorab IKT

Iz tabele 1 razberemo, da so dvosmerne umetne nevronske mreže še posebej primerne za zlorabe, kot so kloniranje mobilnih terminalov, zlorabe pri zaračunavanju storitev, socialnem inženiringu in pri zlorabah kreditnih kartic. Pri teh zlorabah lahko na preprost način določimo parametre sistema IKT, ki jih nadziramo. Narava teh parametrov pa je takšna, da jih lahko z malo ali nič predelave vstavimo v časovne vrste, ki jih pripeljemo na vhod dvosmernih umetnih nevronskih mrež. Ti parametri so namreč že v osnovi zapisani s številskimi vrednostmi v podatkovnih bazah lastnikov sistemov IKT. Čeprav smo v tabeli 1 zapisali, da so dvosmerne umetne nevronske mreže manj primerne za odkrivanje računalniških vdorov in neprimerne za odkrivanje naročniških zlorab, to ne pomeni, da jih ne moremo uporabiti v te namene. Pri računalniških vdorih lahko spremljamo, napovedujemo in primerjamo zaporedje ukazov, uporabljenih za vstop v računalniški sistem. V tem primeru imamo le več dela pri predelavi in predstavitvi zaporedij ukazov v obliko, ki je primerna za uporabo dvosmernih umetnih nevronskih mrež. V tem primeru se moramo samo odločiti, ali rezultati odkrivanja tovrstnih zlorab odtehtajo vloženi trud postavitve takšne rešitve. Pri odkrivanju naročniške zlorabe moramo pred izdajo nove kreditne kartice primerjati podatke prosilca s podatki, ki so shranjeni pri izdajatelju kreditne kartice in so bili v preteklosti že uporabljeni pri tovrstnih zlorabah. V tem primeru ne potrebujemo funkcionalnosti napovedovanja, ki je bistvena lastnost in prednost dvosmernih umetnih nevronskih mrež. Zato teh mrež ne uporabljamo za odkrivanje naročniških zlorab.

Ker ne vemo, katera zloraba IKT se bo zgodila, moramo spremljati vse pomembnejše parametre sistema IKT. Na tem mestu smo omenili le pet parametrov, v realnih razmerah pa moramo spremljati tudi do štirideset parametrov in njihove kombinacije.

4. Sklep

Preprečevanje zlorab IKT je najprej potrebno dobro poznavanje le-teh. S tem namenom smo jih podrobneje predstavili v prvem delu tega prispevka. V drugem delu pa smo predlagali metodo odkrivanja zlorab IKT s pomočjo dvosmernih umetnih nevronskih mrež. Uporaba umetnih nevronskih mrež pri napovedovanju prihodnjih vrednosti je čedalje bolj razširjena zaradi prednosti, ki jih imajo pred klasičnimi metodami napovedovanja. Še posebej pomembno vlogo pridobivajo dvosmerne umetne nevronske mreže, ki zaradi izmenjave stanj med podmrežama veliko bolje napovedujejo vrednosti kot klasične enosmerne umetne nevronske mreže [13]. Takšno odkrivanje zlorab IKT sicer ne poteka v realnem času, ima pa kar nekaj dobrih lastnosti. Poleg tega pa je metoda primerna za odkrivanje večine vrst zlorab IKT, tako tistih, ki so tehnološke, kot tistih, ki so netehnološke. Edini pogoj sta pravilna predpriprava in predstavitev vhodnih vrednosti v dvosmerno umetno nevronsko mrežo.

S prvimi analizami dvosmernih umetnih nevronskih mrež, ki smo jih izvedli s pomočjo sintetično generiranih vhodnih vrednosti, smo potrdili primernost uporabe le-teh za uspešno odkrivanje zlorab IKT. V prihodnje načrtujemo prilagoditev in natančno uglaševanje teh mrež z uporabo realnih podatkov sistema IKT.

5. Zahvala

Raziskovalno delo je sofinanciralo slovensko ministrstvo za visoko šolstvo, znanost in tehnologijo.

6. Literatura

[1] S. Ghosh and D.L. Reilly. Credit card fraud detection with neural network. *Proceedings of the 27th Hawaii International Conference on Systems Sciences,* Vol. 3, pages 621–630. IEEE Computer Society Press, Los Alamitos, CA, 1994.
[2] A. Berg, Al Berg. Cracking a Social Engineer. LAN Times, Nov 6, 1995
[3] M. Johnson. Cause and effect of telecoms fraud. *Telecommunication (International Edition)*, Vol. 12, pages 80–84, 1996.
[4] E. Aleskerov, B. Freisleben, B. Rao. CARDWATCH: A neural network based database mining system for credit card fraud detection. *Proceedings of the IEEE/IAFE 1997 Conference on Computational Intelligence for Financial Engineering (CIFEr)*, pages. 220–226. IEEE Press, 1997.
[5] J. R. Dorronsoro, F. Ginel, C. Sánchez, C. S. Cruz. Neural fraud detection in credit card operations. *IEEE Transactions on Neural Networks*, Vol. 4, pages 827–834, 1997.
[6] D. O'Shea. Beating the bugs: Telecom Fraud. *Telephony*, Vol. 3, page 24, 1997.
[7] D.J. Hand and W.E. Henley. Statistical classification methods in consumer credit scoring: A review. *Statistical Soc.* Vol. A, pages 532–541, 1997.
[8] T. FAwcett, F. Provost, Adaptive fraud detection, *Datamining and Knowledge Discovery*. Vol. 1, pahes 1–28, 1997.
[9] P. Hoath. Telecoms fraud, the glory details. *Computer Fraud and Security*, Vol. 1, pages 10–14, 1998.
[10] R. Brause, T. Langsdorf and M. Hepp. Neural data mining for credit card fraud detection. *Proceedings of the 11th IEEE International Conference on Tools with Artificial Intelligence*, pages 103–106. IEEE Computer Society Press, Silver Spring, MD, 1999.
[11] J. Hollmen. User profiling and Classification for fraud Detection in Mobile Communication Networks. *PhD thesis*, Helsinki University of Technology, Department of Cognitive and Computer Science and Engineering, Espoo, Finland, 2000.
[12] J. Palumbo. Social Engineering: What is it, why is so little said about it and what can be done? SANS Institute. http://www.sans.org/infosecFAQ/social.htm, July 26, 2000.
[13] H. Wak, J. Zurada, Time series prediction by neural network model based on the bi-directional computation style networks. *Proceedings of International Conference on Neural Networks*, pages 2225–2230, 2000.
[14] R. J. Bolton, D. J. Hand. Statistical fraud detection: A review. Institute of Mathematical Statistics. *Statistical Science*, Vol. 3, pages 235–255, 2002.
[15] Fair Isaac. Application and Subscription Fraud Management Solutions for Telecommunications. www.fairisaac.com, 2004.
[16] H. Kvarnström, Intrusion and Fraud Detection, *SWITS-IV*, Vadstena, June 7–8, 2004.
[17] www.hp.com/communications, Fraud management systems (FMS), 2004.
[18] O.A. Abidogun, Data mining, Fraud Detection and mobile Telecommunications: Call Patern Analysis with Unsupervised Neural Networks, *MSc. Thesis*, University of the Western Cape, 2005.
[19] http://www.theregister.co.uk/2005/12/19/terror_phone_clone_scam/, december 2005.
[20] http://www.securityfocus.com/infocus/1527, Januar 2005.
[21] http://www.3g.co.uk/PR/August2002/3876.htm, 2006.
[22] The Complete Social Engineering FAQ! http://packetstorm.deceptions.org/doc/social-ngineering/socialen.txt, 2006.
[23] M. Vadman. Fight cellular cloning with a fraud control system: Electronic fingerprinting is the latest among several technologies for preventing criminals from shifting their long-distance charges to other people's bills. Secret codes and personal identification numbers.
http://mrtmag.com/mag/radio_fight_cellular_cloning/index.html, 2006.
[24] http://www.utexas.edu/its/longdistance/ttollfraud.html, september 2006.

Andrej Krenker je leta 2003 diplomiral na Fakulteti za elektrotehniko v Ljubljani, kjer je tudi zaposlen kot mladi raziskovalec.

Matevž Mesojednik je leta 2004 diplomiral na Fakulteti za elektrotehniko v Ljubljani, kjer je tudi zaposlen kot raziskovalec.

Mojca Volk je leta 2004 diplomirala na Fakulteti za elektrotehniko v Ljubljani, kjer je tudi zaposlena kot mlada raziskovalka.

Prof. dr. Janez Bešter je vodja laboratorija za telekomunikacije na Fakulteti za elektrotehniko v Ljubljani. Področje njegovega dela obsega načrtovanje, realizacijo in upravljanje telekomunikacijskih sistemov in storitev, implementiranje IKT aplikacij v procese izobraževanja. Je član več svetov in odborov ter član AAATE, IEEE, IFIP, ACM in IEICE.

Doc. dr. Andrej Kos je leta 1996 diplomiral in leta 2003 doktoriral na Fakulteti za elektrotehniko v Ljubljani, kjer je tudi zaposlen kot docent.