UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO
Kandidat: TONE ŽAGAR
Mentor: doc. dr. MARKO BAJEC

Doprinos vizualizacije pri boju z goljufijami v telefonskih sistemih

MAGISTRSKO DELO

Ljubljana, 2008

Zahvala

Iskreno se zahvaljujem vsem, ki so mi pomagali pri izdelavi magistrske naloge. Še posebej pa se zahvaljujem:

- mentorju doc. dr. Marku Bajcu, ki mi je omogočil izdelavo magistrske naloge in me usmerjal skozi celotno delo
- članom projektne skupine Laboratorija za Informatiko za pomoč in koristne nasvete
- sodelavcem v podjetju Hermes SoftLab za razumevanje in spodbudo

Kazalo

Kazalo slik

Uporabljene kratice

NGN	omrežje nove generacije (angl. Next Generation Network)
IP	internetni protokol (angl. Internet Protocol)
SCN	komutirano omrežje (angl. Switched Communications Network)
PSTN	javno komutirano telefonsko omrežje (angl. Public Switched Telephone Network)
ISDN	integrirane storitve preko digitalnega omrežja (angl. Integrated Services Digital Network)
DSL	digitalni naročniški vod (angl. Digital Subscriber Line)
SS7	signalni sistem 7 (angl. Signaling System 7)
GSM	globalni sistem za mobilne telekomunikacije (angl. Global System for Mobile Communications)
UMTS	univerzalni sistem za mobilne telekomunikacije (angl. Universal Mobile Telecommunication System)
ITU	mednarodno telekomunikacijsko združenje (angl. International Telecommunication Union)
GSMA	združenja globalnega sistema za mobilne telekomunikacije (angl. Global System for Mobile Communications Association)
SIP	protokol za opis seje (angl. Session Initiation Protocol)
VoIP	telefonija preko internetnega protokola (angl. Voice over IP)
PRN	komercialna številka (angl. Premium Rate Number)
PRS	komercialna storitev (angl. Premium Rate Service)
FMS	sistem za upravljanje z goljufijami (angl. Fraud Management System)
SLA	dogovor o ravni storitve (angl. Service Level Agreement)
IMEI	mednarodna identifikacijska številka mobilne opreme (angl. International Mobile Equipment Identity)
NIC	omrežna kartica (angl. Network Interface Card)
MAC	fizični naslov naprave (angl. Media Access Control).
CDR	zapis o klicu (angl. Call Detail Record)
UDR	zapis o storitvi (angl. Usage Detail Record)
IPDR	zapis o storitvi v omrežjih nove generacije (angl. Internet Protocol Detail Record)
XML	razširljiv označevalni jezik (angl. eXtensible Markup Language)
SMS	kratko sporočilo (angl. Short Message Service)
IDS	sistem za odkrivanje vdorov (angl. Intrusion Detection System)
IPS	sistem za preprečevanje vdorov (angl. Intrusion Prevention Systems)
IRP	delovanje v primeru incidenta (angl. Incident Response Program)
CIRT	odzivna skupina za delovanje v primeru incidenta (angl. Computer Incident Response Team)
VPN	navidezno zasebno omrežje (angl. Virtual Private Network)
UML	poenoteni jezik modeliranja (angl. Unified Modeling Language)
TCP	protokol za nadzor prenosa (angl. Transmission Control Protocol)
SQL	strukturiran povpraševalni jezik (angl. Structured Query Language)
API	programski vmesnik (angl. Application Programming Interface)
SIM	naročniški identifikacijski modul (angl. Subscriber Identity Module)
IMSI	mednarodna identiteta mobilnega naročnika (angl. International Mobile Subscriber Identity)
BTS	bazna postaja (angl. Base Transceiver Station)

MPS	sistem za lociranje mobilne postaje (angl. Mobile Positioning System)
PBX	zasebna naročniška centrala (angl. Private Branch eXchange)
DISA	storitev, ki omogoča klicanje iz centrale skozi zunanjo linijo (angl. Direct Inward System Access)

1 Povzetek

Finančne izgube v telefoniji, ki jih povzročijo goljufije, predstavljajo od štiri do šest odstotkov dohodka telekomunikacijskih podjetji. Odgovor na naraščajočo grožnjo, ki jo predstavljajo goljufije, iščemo v izpopolnjevanju sistemov za upravljanje z goljufijami. Ena izmed slabo raziskanih poti na tem področju je uporaba vizualizacije pri odkrivanju in preprečevanju goljufij. Namen tega dela je preučiti in oceniti prispevek vizualizacije. Za dosego cilja je bilo najprej potrebno klasificirati goljufije. Nato je sledila razčlenitev sistema za upravljanje z goljufijami na posamezne faze, definirane na osnovi nalog, ki jih ta opravlja. Na podlagi nalog in tipov goljufij smo nato iskali ustrezne vizualizacijske rešitve. Ugotovili smo, da vizualizacija ni kritični del sistema, je pa zaželen in dobrodošel pripomoček. Uporabnost je odvisna tudi od preferenc analitika, kajti nekaterim je vizualizacija bližje oziroma je zanje lažje razumljiva kot za druge. Vendar pa se moramo pri tem držati določenih napotkov in pristopov, brez katerih bi bila vizualizacija neuporabna. Upoštevati moramo tako videz kot funkcionalnost predstavitve. V fazi preprečevanja goljufij je vizualizacija v pomoč pri analiziranju povratne informacije z zaščitnih elementov, v fazi odkrivanja je v pomoč pri analiziranju velike količine podatkov, v fazi obravnave izjem pa je v pomoč pri analiziranju alarma. Rezultat dela je sistematičen pregled skozi problematiko, model aplikacije za vizualizacijo podatkov in prototipi posameznih vizualizacijskih pristopov. Tako so teoretična razmišljanja potrjena tudi z praktičnimi primeri. Nadaljnje raziskave tega področja morajo potekati v tesnem sodelovanju z analitiki, ki skrbijo za upravljanje z goljufijami. Empirične metode bi namreč hitreje pripeljale do novih idej in izboljšav.

Ključne besede: vizualizacija, sistem za upravljanje z goljufijami, telefonija, goljufije

2 Abstract

Financial losses in telephony caused by fraud represent four to six percents of telecommunication industry income. An answer to this threat is increasing research of fraud management systems. One of the less researched branches of this field is the usage of visualization in fraud detection and prevention. The purpose of this work is to research and give an estimate for the usability of it. Taxonomic classification of fraud and fraud management system was the first step in order to get a clear picture of the tasks that fraud management system has to carry out. With that and visualization theory in mind we then searched for the suitable visual representations for each task. The conclusion was that visualization is not a critical part of the system but a valuable additional tool that will increase the productivity of the analyst. In the fraud prevention phase visualization will help to analyze information received from elements that are used to protect the system, detection phase will benefit as visualization is efficient for huge dataset analysis and in the last processing phase visualization will help to filter the alarms reported from the previous phase. But we have to be careful, as visualization is only useful if properly implemented, with presentation appearance and functionality in mind. The contribution of this work is a systematical overview of the addressed topic, application model and visualization prototypes based on real life examples. The theoretical findings were confirmed with practical examples. Further work should include a closer cooperation with fraud analysts and research with empirical methods. That would most likely bring us closer to new ideas and better results.

Key words: visualization, fraud management system, telephony, fraud

3 Uvod

Namen magistrske naloge je ugotoviti, ali in kako je lahko vizualizacija v pomoč pri upravljanju z goljufijami v telefoniji. Kot bo razloženo v nadaljevanju, gre pri upravljanju z goljufijami za njihovo preprečevanje, odkrivanje in obravnavo, k telefoniji pa v tem primeru štejemo storitve za prenos govora po stacionarnih in mobilnih omrežjih ter omrežjih nove generacije (angl. Next Generation Network – NGN).

Problem, ki je obravnavan v magistrski nalogi, zahteva razumevanje različnih področij: telekomunikacijske sisteme za prenos govora, statistične metode, rudarjenje podatkov, grafični dizajn, vizualizacijo informacij in razvoj informacijskih sistemov. Neodvisno med seboj so ta sicer dobro raziskana, na njihovem stičišču pa je bilo zaradi specifičnosti problemske domene izvedenih le malo raziskav, katerih rezultati so dostopni širši javnosti.

Primer raziskave uporabe vizualizacije za odkrivanje goljufij v telefonski domeni navajajo Cox in drugi [**1**]. Tu je opisana aplikacija razvita v sodelovanju med laboratoriji Bell[1] in AT&T[2]. Druge v magistrski nalogi omenjene raziskave pa so večinoma povezane z odkrivanjem goljufij v telekomunikacijskih sistemih brez uporabe vizualizacije ali z uporabo vizualizacije za nadzor omrežij, ki temeljijo na internetnem protokolu (angl. Internet Protocol – IP).

Same goljufije oziroma tehnična ozadja goljufij so občutljiva tema, o kateri ni lahko najti veliko informacij. Telekomunikacijska podjetja so nedvomno vložila veliko časa in denarja v raziskovanje goljufij, vendar pa pridobljenega znanja ne delijo s širšo javnostjo in konkurenco, saj je to konkurenčna prednost. Tehnične informacije o določenih goljufijah tako pogosto ostajajo skrbno varovane skrivnosti posameznih operaterjev. S širjenjem teh informacij bi končno le izobraževali goljufe, negativne posledice skrivanja informacij pa slednji s pridom izkoriščajo. Ko nek operater odkrije in prepreči nadaljevanje goljufije, lahko goljufi preprosto nadaljujejo isto goljufanje pri naslednjem operaterju.

Da bi ocenili pomen vizualizacije na področju upravljanja z goljufijami, moramo najprej odgovoriti na vprašanje, kaj je goljufija in kako poteka upravljanje z goljufijami brez podpore vizualizacije. V četrtem poglavju so tako na kratko predstavljena aktualna omrežja za prenos govora, v petem pa je opredeljen pojem goljufije v telefoniji. Kako deluje preprečevanje goljufij brez vizualizacije, je opisano v šestem poglavju. Naslednja tri poglavja so namenjena natančnejšemu opisu posameznih faz obravnavanja goljufij. Deseto, najobsežnejše, poglavje je namenjeno vizualizaciji. Najprej so predstavljene osnove vizualizacije velike količine večdimenzionalnih podatkov, nato pa model aplikacije, ki z vizualizacijo prispeva k upravljanju z goljufijami. Na koncu istega poglavja so predstavljeni nekateri primeri znanih goljufij in vizualizacijskih pristopov, ki so v pomoč pri upravljanju z njimi.

---

[1] Laboratoriji Bell (http://www.bell-labs.com/).
[2] Laboratoriji AT&T (http://www.research.att.com/).

4 Omrežja

V magistrski nalogi je poudarek na govornih storitvah, neodvisno od omrežja in protokolov, na katerih temeljijo. Za lažje razumevanje obravnavane teme pa je dobro vedeti nekaj o omrežjih, v katerih se te storitve izvajajo. V nadaljevanju je nekaj osnovnih informacij o trenutno najbolj razširjenih omrežjih.

V literaturi s podobno tematiko je predstavitev omrežij pogosto poenostavljena tako, da ločimo le IP-omrežje in komutirano omrežje (angl. Switched Communications Network – SCN) [**2**]. Akterja v SCN sta stacionarni in mobilni telefon, v IP-omrežju pa IP-telefoni. Tu ločimo omrežje za fiksno telefonijo, mobilno omrežje in omrežje nove generacije.

4.1 Omrežje za fiksno telefonijo

Omrežje, ki omogoča fiksno telefonijo, se imenuje javno komutirano telefonsko omrežje (angl. Public Switched Telephone Network – PSTN). Bistvena razlika med IP- in PSTN-omrežjem je, da slednje uporablja komutiran stikalni sistem, ki povezavo rezervirana za celotni čas klica. Rezervirana povezava omogoča raven kakovosti prenosa govora, ki jo IP-omrežja za zdaj težko zagotovijo. Brez dodatne digitalne tehnologije doseže hitrost prenosa podatkov največ 56 kb na sekundo. Za boljše prenose se omrežje nadgradi v PSTN/ISDN (angl. Integrated Services Digital Network), ki omogoča hitrosti do 128 kb na sekundo, in v PSTN/DSL (angl. Digital Subscriber Line) za višje hitrosti. Omrežje je razen »zadnje milje« do uporabnika v celoti digitalizirano. V omrežju PSTN se večinoma uporablja množica protokolov, imenovana signalni sistem 7 (angl. Signaling System 7 – SS7).

PSTN je preverjeno omrežje, v katerem ni pričakovati novih tehničnih goljufij, ki bi izkoriščale pomanjkljivosti v zasnovi omrežja, ranljivo pa postane pri integraciji z IP-omrežjem.[3]

Na prvi pogled se zdi, da bi omrežje, ki omogoča predvsem prenos zvoka, moralo biti preprosto. A izkaže se, da to ni res. Zaradi različnih standardov in dolge zgodovine razvoja ima nešteto različnih obrazov. Komentar na kompleksen razvoj PSTN-omrežja, je naslednji: »Naučiš se lahko vse, kar se je zgodilo do danes, in jutri boš poznal le včerajšnje novice.« [**3**].

---

[3] Povezavo med IP- in PSTN-omrežjem omogočajo prehodi (angl. gateway). Prehod je razdeljen na nadzornik medijskih prehodov (angl. Media Gateway Controller – MGC), ki omogoča nadzor nad prenosom, in medijski prehod (angl. Media Gateway – MG), ki omogoča pretvarjanje iz PSTN v IP in nasprotno (65). Najzanimivejša pretvorba je PSTN – IP – PSTN, saj omogoči pretvorbo mednarodnega klica v dva lokalna PSTN-klica, kar občutno poceni klic.

4.2 Omrežja za mobilno telefonijo

Prva generacija (1G) mobilnega omrežja je bila razvita leta 1980. To je bilo analogno omrežje, ki se je v drugi generaciji (2G) digitaliziralo in prešlo v širšo uporabo. Najpogostejši standard v omrežju druge generacije je globalni sistem za mobilne telekomunikacije (angl. Global System for Mobile Communications – GSM). Z bliskovitim razvojem omrežja se je začelo zlato obdobje za goljufe, saj je bilo odkritih kar nekaj pomanjkljivosti v zasnovi GSM-standarda [**4**], ki pa so bile z uvedbo nadgradenj in nato tretje generacije odpravljene.

Tretja generacija omrežja je pri nas bolj znana kot univerzalni sistem za mobilno telekomunikacijo (angl. Universal Mobile Telecommunication System – UMTS). Gre za univerzalen telekomunikacijski sistem, ki omogoča hitrejši prenos podatkov kot njegovi predhodniki, uporabo novih storitev, hkraten prenos besedila, slike in zvoka ter videotelefonijo. Splošno ime za omrežje tretje generacije je IMT-2000, za razvoj skupine standardov v okviru IMT-2000 pa skrbi Mednarodno telekomunikacijsko združenje ITU (angl. International Telecommunication Union).

Po podatkih združenja globalnega sistema za mobilne telekomunikacije (angl. Global System for Mobile Communications Association – GSMA[4]) je januarja 2007 mobilni telefon uporabljajo približno 2,2 milijarde ljudi od 6,5 milijarde celotne svetovne populacije. Le dvajset odstotkov uporabnikov se je odločilo za mobilni sistem tretje generacije. Omrežje tretje generacije velja za zrelo in varno omrežje.

4.3 Omrežje nove generacije

Omrežje nove generacije je širok in pogosto rabljen pojem, ki opisuje prehod iz omrežja, namenjenega izključno glasu, v omrežje za prenos vseh tipov informacij in storitev. Poudarek je na prenosu glasu, videa in podatkov. Omrežja so zgrajena na IP-protokolu, torej se vsi podatki prenašajo v obliki paketov. Na aplikacijskem nivoju se uporablja protokol za opis seje (angl. Session Initiation Protocol – SIP).

Omenjeno omrežje je zanimivo predvsem zato, ker z varnostnega stališča ni korak naprej, pač pa odpira nove možnosti za goljufije. Slabosti s stališča občutljivosti za goljufije sta predvsem dejstvo, da NGN-omrežje temelji na IP-protokolu, in povečano število načinov dostopa do omrežja. Po oceni skupine Gartner[5] več kot sedemdeset odstotkov napadov na omrežje nekega podjetja cilja na aplikacijski nivo, in ne omrežni ali sistemski [**5**]. Ta ocena je še posebej zanimiva za NGN-omrežje, saj je tu aplikacijski nivo v veliki meri še nestandardiziran. Gre torej za distribuirano, odprto in zapleteno omrežje, ki nima standardiziranih varnostnih mehanizmov, poleg tega pa se v njem hitro pojavljajo nove storitve, ki niso nujno primerne za uporabo. Ker dobički na področju storitev hitro rastejo, postaja vedno zanimivejše za

[4] Združenje GSMA (http://www.gsmworld.com/).
[5] Analitična hiša Gartner Group (http://www.gartner.com/).

goljufe, ki se tako ne posvečajo več samemu prenosu zvoka, pač pa prenosu podatkov, na katerih temeljijo storitve.

Tipična storitev v NGN-omrežju je VoIP (angl. Voice over IP). Zanimiv podatek prihaja iz laboratorijev podjetja Sipera Systems,[6] katerih naloga je odkrivanje ranljivosti VoIP-protokolov in opreme. V zadnjih treh letih so prepoznali kar 20 000 varnostnih lukenj [**6**].

Po svetu so še vedno tri milijarde ljudi, ki nimajo dostopa niti do osnovnega telefonskega priključka, torej obstaja še ogromen trg, primeren tudi za manj napredna omrežja. Vendar pa na splošno velja, da se bodo dnevi zvoka kot posebne kategorije kmalu končali.

[6] Podjetje s sedežem v Richardsonu v Teksasu je bilo ustanovljeno leta 2003. Ukvarja se z razvojem aplikacij, ki omogočajo varnost v okolju VoIP (http://www.sipera.com/).

5 Goljufije

Pred obravnavo sistemov, ki omogočajo preprečevanje goljufij, je treba najprej predstaviti pojem goljufije, zato se poglavje začne z opredelitvijo omenjenega pojma, nadaljuje pa z navajanjem nekaterih razlogov za goljufijo ter pregledom različnih tipov goljufij. Predstavljen je tudi poskus napovedi trendov razvoja.

5.1 Opredelitev in vpliv goljufij

Goljufije so se pojavile skoraj z začetkom telefonije. PSTN je bil dolgo najzapletenejši in najnaprednejši telekomunikacijski sistem v javni uporabi, zaradi česar je bil priljubljena tarča radovednih posameznikov, ki so poskušali razumeti, kako deluje. Ne glede na to, ali so posamezniki to delali zaradi učenja (to so bili predhodniki današnjih hekerjev) ali z namenom goljufije, je razumevanje pogosto razkrilo pomanjkljivosti, ki so omogočile zlorabo oziroma brezplačno uporabo telefonskih storitev.

Goljufija v telekomunikacijah je opredeljena kot prenos glasu ali podatkov po telekomunikacijskem omrežju, pri katerem se pošiljatelj namerava izogniti zakonitim stroškom prenosa [**7**].

Kadar govorimo o goljufijah v telefonskem omrežju, ta opredelitev ni dovolj natančna. Ni nujno, da je povzročitelj goljufije ravno pošiljatelj. Kot primer vzemimo goljufijo, pri kateri goljuf pošiljatelja prepriča, naj ga pokliče na komercialno številko (angl. Premium Rate Number – PRN), pri tem pa ga ne opozori na višjo ceno klica oziroma ga zavaja glede nujnosti ali vsebine klica [**8**]. V tem primeru je goljufijo povzročil prejemnik klica oziroma tretja oseba, ki je zavedla pošiljatelja. Goljuf je torej lahko kdor koli. Naslednja pomanjkljivost je določitev stroška. Poleg stroška prenosa, ki je v definiciji omenjen, je tu še strošek storitve. Pri klicih na komercialno številko je strošek prenosa zanemarljiv. Zadnja pomanjkljivost pa je neopredeljena ciljna množica, torej ogoljufana oseba. To je lahko telefonski operater, ponudnik storitve ali pa tretja oseba, ki jo goljuf izkoristi pri izvedbi goljufije. Tipičen primer oškodovanja tretje osebe je kraja mobilnega telefona.

Z upoštevanjem naštetih pomanjkljivosti lahko goljufijo v telefonskem omrežju opredelimo kot prenos glasu ali podatkov po telekomunikacijskem omrežju, pri katerem pride do okoriščanja z oškodovanjem telefonskega operaterja, ponudnika storitve ali uporabnika telefonskega omrežja.

Ker je v magistrski nalogi govor o preprečevanju goljufij, je pozornost osredinjena predvsem na telefonske operaterje, ki praviloma skrbijo za to. Pojavi pa se dvom o resnosti problema, povezanega z goljufijami. Na prvi pogled se zdi, da posledice takih goljufij ne morejo bistveno vplivati na poslovanje telefonskih operaterjev. Glede na razmeroma nizke cene (vsaj v primerjavi z bližnjo preteklostjo) tako mednarodnih kot lokalnih klicev ter malo ustreznih kandidatov z dovolj tehničnega znanja, ki so pripravljeni storiti kaznivo dejanje, bi pričakovali, da to velja. Ko pa si podrobneje ogledamo posamezne goljufije, ugotovimo, da lahko povzročijo veliko škode.

Ko goljuf pridobi nadzor nad viri telefonskega omrežja, lahko počne naslednje:

- Preprodaja klice po precej nižji ceni, kot jo ponuja operater. Praviloma so take goljufije hitro odkrite, vendar pa lahko dobro organizirani goljufi v kratkem času naredijo veliko prometa.
- Preusmerja klice na komercialne številke oziroma številke 090. Goljufija običajno zahteva sodelovanje lastnika komercialne storitve (angl. Premium Rate Service – PRS). Cilj je usmeriti čim več »nelegalnega« prometa na te številke.

Da so goljufije resen problem, potrjujejo ocene škode, ki jo v Združenih državah Amerike povzročijo posredno in neposredno. Različni viri, npr. [**9**] in [**10**], navajajo, da ta znaša od štiri do šest odstotkov dohodka telekomunikacijskih podjetji. Pri novejših operaterjih, ki nimajo izkušenj ter ne upoštevajo utečenih postopkov za preprečevanje in odkrivanje goljufij, lahko finančne izgube znašajo tudi do 20 odstotkov dohodka.

Pri interpretaciji navedenih podatkov moramo biti previdni, saj izgube, ki jih operater javno prikaže, niso vedno zanesljive. Glavni razlogi za to so naslednji:

- Finančne izgube, ki jih povzročijo goljufije, je izjemno težko oceniti, saj se posledice kažejo na različnih področjih. Najočitnejša je finančna škoda, ki jo goljufija neposredno povzroči, nekoliko manj očitna in nezanesljiva pa je posredna škoda, ki se kaže v marketingu (operaterji so previdni pri ponujanju novih storitev), odnosu s strankami (če pride informacija o varnostnih težavah med naročnike), odnosu z delničarji in podobno.
- Včasih operaterji nočejo priznati izgub, ker bi to pomenilo slabo reklamo. Novica o pomanjkljivi varnosti sistema ne bo pritegnila novih uporabnikov.
- Nasprotno operaterji prikažejo večje izgube, kadar želijo doseči spremembo zakonodaje. Zakoni, ki ščitijo zasebnost podatkov, so na primer lahko trn v peti pri iskanju povzročiteljev goljufij.

Zanimiv izračun, ki ponazarja vpliv goljufij na dohodek, navajata Bolton in Hand [**9**]. Če predpostavimo, da je od vseh transakcij 0,1 odstotka takih, ki pomenijo goljufijo, in da je vsaka vredna deset funtov, podjetje na sto milijonov transakcij izgubi milijon funtov. AT&T je že leta 1998 prenesel 275 milijonov transakcij na dan, torej je imel po takem izračunu dnevno za 2,75 milijona funtov izgube.

Težave, ki še stopnjujejo izgubo operaterja, so:

- Naročniki ne bodo več lojalni in ne bodo dolgo odlašali z zamenjavo operaterja, če izvedo, da ima trenutni operater težave s preprečevanjem goljufij.
- Povečano število pritožb zaradi visokih računov in motenj ter zlorab osebnih podatkov povzroči veliko dodatnih stroškov, tožbe in slabo reklamo.

- Zaradi pridobivanja novih in ohranjanja zdajšnjih strank je treba ponujati nove storitve. Operaterji, ki imajo slabe izkušnje z goljufijami, pogosto odlašajo z novimi storitvami, dokler niso prepričani, da so varne. Zaradi tega pa zamujajo priložnost biti prvi na trgu z novo storitvijo. Tako vedenje odvrača stranke, ki želijo preizkusiti nove tehnologije (angl. early adopters). Za nove oziroma napredne storitve so pogosto značilne številne varnostne luknje, ki se s časom odkrijejo in zakrpajo [**11**].
- Nadgradnje storitev so drage.
- Fleksibilnost storitev se povečuje, s tem pa tudi kompleksnost njihove zaščite.
- Vsaka zaščita ima svojo ceno.
- Pogoste tožbe in kazni zaradi kršenja zakonodaje, če na primer osebni podatki strank niso bili dovolj dobro zaščiteni. Kadar govorimo o občutljivih podatkih, se lahko pojavi tudi sum namerne zlorabe na strani operaterja.

Zavedati se moramo, da govorimo o zelo konkurenčnem trgu, na katerem je vsaka stranka dragocena, zato ni mesta za napake in slabo reklamo. Tudi če operater strankam krije neposredne stroške goljufije, še vedno ostajajo posredni stroški, ki jih operaterji običajno ne krijejo in jih je težko oceniti. Sem spadajo na primer oškodovan dober ugled stranke (primer je samodejno posredovanje prihodnjih klicev na številke vročih linij) in stroški, ki nastanejo zaradi prekinitev storitve, ki jo ponuja operater.

Brez posebnega tveganja lahko zaključimo, da so goljufije eden večjih problemov, s katerimi se spopadajo telefonski operaterji. Tisti z dolgoletnimi izkušnjami in napredno opremo so seveda odpornejši od operaterjev v državah v razvoju, ki beležijo največje izgube. Po podatkih iz [**12**] je bilo leta 2006 v povprečju največ goljufij zabeleženih v Pakistanu, na Filipinih in Kubi ter v Indiji in Bangladešu. V istem viru je navedeno, da izgube v svetovnem merilu znašajo od 54,4 milijarde do 60 milijard dolarjev, kar je za 52 odstotkov več kakor leta 2003.

Za lažje razumevanje poglavij, ki sledijo, je treba opozoriti, da je ponekod namesto besede *goljufija* rabljen izraz *napad*. Če ni posebej omenjeno, obe besedi označujeta isto dejanje. Podobno je tudi oseba, ki povzroči goljufijo, poimenovana *goljuf* ali pa *napadalec*.

5.2 Razlogi za goljufije

Poskusimo odgovoriti na vprašanje, zakaj sploh prihaja do goljufij. Prvo in najpomembnejše vodilo je vsekakor zaslužek. Goljuf lahko zasluži s preusmerjanjem klicev na PRN (zato je treba sodelovati z lastnikom PRS) in z nadaljnjo preprodajo klicev (sam postane ponudnik storitev in jih prodaja po nižji ceni kot ogoljufani telefonski operater). Drugo vodilo je uporaba storitev brez plačila. Včasih je bilo to zanimivejše zaradi dragih klicev v tujino, ki pa so zdaj veliko dostopnejši (na primer klic iz Slovenije v

Združene države Amerike stane 0,3 evra na minuto)[7]. Naslednje vodilo je zahteva glede anonimnosti. V takih primerih je telefonska goljufija povezana z neko drugo nezakonito dejavnostjo. Tukaj ne gre za dobiček, pač pa za zakrivanje sledi. Dober »legalen« pripomoček za skrivanje identitete so predplačniški naročniški paketi, vendar je oseba še vedno vezana na eno telefonsko številko. Zadnji razlog za goljufije pa je izziv za napadalca in status med vrstniki (navadno gre za mlajše osebe). Raziskovanje telefonskega omrežja sicer izgublja priljubljenost, saj je internet mnogo privlačnejši. S selitvijo telefonije v IP-domeno pa lahko raziskovanje takih sistemov spet postane zanimivo.

5.3 Vrste goljufij

Po nekaterih ocenah [**13**] je vsaj dvesto različnih goljufij, katerih tarče so telefonski operaterji, s širjenjem uporabe NGN-omrežij in mobilnih omrežij pa se ta številka še povečuje.

Goljufije so glede na način izvedbe tehnične in netehnične. Tehnične so tiste, ki izkoriščajo pomanjkljivosti v zasnovi omrežja ali varnostnih elementov omrežja. Kot primer vzemimo goljufijo s storitvami VoIP, o kateri se je veliko govorilo leta 2006. Edwin Pena je deloval kot veleprodajalec telefonskih storitev, ki jih sam ni kupoval, pač pa jih je nezakonito pridobil od različnih ponudnikov storitev VoIP. Za dostop do usmerjevalnikov legalnih ponudnikov storitev VoIP in vmesnih strežnikov, ki so bili namenjeni za zakrivanje sledi, je poskrbel njegov sodelavec Robert Moore.[8] Po njegovih besedah vdiranje v zasebna omrežja ni bilo zapleteno. Šlo je za iskanje šibkih točk, kot so sistemi s prednastavljenimi gesli, šibkimi gesli, ki se jih je dalo ugotoviti s t. i. napadi s slovarjem (angl. dictionary attack) ali grobo silo (angl. brute force attack) in s sistemi brez kritičnih popravkov. Po podatkih ameriškega zveznega preiskovalnega urada (angl. Federal Bureau of Investigation – FBI) so na tak način prodali deset milijonov minut klicev in zaslužili več kot milijon ameriških dolarjev.[9] Netehnične goljufije pa temeljijo na izkoriščanju neznanja, naivnosti ali površnosti uporabnikov in skrbnikov omrežja. Pogosto omenjena metoda v tej skupini je socialni inženiring. To je zbirka tehnik manipuliranja z ljudmi z namenom razkritja zaupne informacije ali kot je opredeljeno v [**14**]: »Bistvo socialnega inženiringa je, da prepričaš ljudi o tem, da si nekdo drug, ob podpori tehnologije ali brez nje. To storiš z manipulacijo, vplivanjem in s prepričevanjem. Ko ljudi prepričaš, lahko od njih pridobiš informacije, ki jih želiš.« Netehnične goljufije so uspešne predvsem zaradi slabega zavedanja ljudi o njihovi razširjenosti.

---

[7] Družba Mobitel (http://www.mobitel.si).
[8] Moorova spletna stran (http://www.moorer-software.com).
[9] Nekaj podatkov o primeru. Obtožnici:
http://www.usdoj.gov/usao/nj/press/files/pdffiles/penacomplaint.pdf in
http://www.usdoj.gov/usao/nj/press/files/pdffiles/moorecomplaint.pdf
Podatki dokumentarne oddaje »America's most wanted«:
http://www.amw.com/fugitives/brief.cfm?id=49218

Drugo, natančnejšo, delitev dobimo, če goljufije razvrstimo po kritičnem elementu, ki omogoča goljufijo. Gre torej za šibko točko telekomunikacijskega sistema, brez katere ne bi mogli izvesti goljufije. Po natančnem pregledu znanih primerov goljufij smo ugotovili, da so kritični dejavniki pomanjkljivi varnostni mehanizmi, oprema v lasti operaterja, oprema v lasti uporabnika, postopki operaterja, zaposleni pri operaterju in uporabniki. Goljufijo omogoča eden ali več omenjenih dejavnikov.

Primeri, s katerimi je mogoče ponazoriti tako delitev goljufij, so naslednji:

- Pomanjkljivi varnostni mehanizmi. Omenjena goljufija v zvezi s storitvami VoIP je bila izvedljiva zaradi prednastavljenih ter šibkih gesel in sistemov brez kritičnih popravkov. Gre za tipične predstavnike prve skupine.
- Oprema v lasti operaterja. Primer, ko operaterjeva oprema omogoča izvedbo goljufije, je nedovoljeno spreminjanje zapisov v zbirki podatkov HLR[10]. V njej goljuf poveže neregistrirani MSISDN[11] s številko IMSI[12] naključne stranke. Ker je treba spremeniti zapise v HLR, taka goljufija zahteva vpletenost notranjega sodelavca. Posledica takega spreminjanja zbirke podatkov je, da se klici z neregistriranega MSISDN-ja ne zaračunavajo (če sistem ni izdelan tako, da predvideva takšne scenarije).
- Oprema v lasti uporabnika. Vsem znan primer zlorabe uporabnikove opreme je kraja mobilnega telefona. Goljufija je v teku, dokler uporabnik operaterja ne obvesti, da je bil telefon ukraden.
- Postopki operaterja. Primer neustreznega postopka na strani operaterja je pomanjkljivo preverjanje veljavnosti naročniških razmerij, ki jih sklene posrednik. Za učinkovitejšo prodajo svojih storitev operaterji posrednikom omogočajo, da v njihovem imenu iščejo nove naročnike. Za vsako sklenjeno naročnino dobi posrednik določeno plačilo. Poznamo primere, ko posrednik na podlagi lažnih podatkov sklene naročnino in od operaterja zahteva plačilo. Da operater dobi potrdilo o aktivni naročnini, posrednik opravi le en kratek klic z nove številke [**15**]. Telefonski operater plača posredniku, ker ne ve, da je sklenjena naročnina neveljavna.
- Zaposleni pri operaterju. Uporabimo isti primer kot pri opremi v lasti operaterja. Kot rečeno, spreminjanje zbirke podatkov HLR zahteva notranjega sodelavca. Ni pa nujno, da gre pri tem vedno za zlonamerno ravnanje zaposlenih, ti so le ljudje, ki delajo nenamerne napake, kar pa lahko omogoči izvedbo goljufije.
- Uporabniki. Pomembna je vloga neznanja in naivnosti uporabnikov. Primerov je veliko, med njimi tudi polnjenje predplačniškega mobilnega telefona prek tretje osebe brez njenega soglasja. Goljufija

---

[10] HLR je angleška kratica za register domače lokacije (angl. Home Location Register). To je zbirka podatkov, ki vsebuje podatke o naročnikih, identifikacijskih številkah mobilnih telefonov in njihovo trenutno lokacijo.

[11] MSISDN je angleška kratica za identifikacijsko številko mobilnega telefona (angl. Mobile Station Integrated Services Digital Network – MSISDN).

[12] IMSI je angleška kratica za mednarodno identiteto mobilnega naročnika. Gre za unikatno 15-številčno oznako naročnika v mobilnem telefonskem omrežju. Prvi niz števil označuje naročnikovega operaterja, drugi niz pa naročnika.

je v Sloveniji izvedljiva, če tarča uporablja mobilno storitev Moneta[13], ki jo ponuja družba Mobitel. Goljuf si od naključne osebe sposodi mobilni telefon, pod pretvezo, da bo opravil nujen klic, ki bo zelo kratek. Medtem ko tarča ne gleda, goljuf hitro vtipka ukaz za polnjenje Mobiračuna[14] (Mobitelovega predplačniškega računa).

Seveda to niso edine možnosti za delitev goljufij. Na primer v [**16**] je predstavljena delitev glede na njihov izvor. Tako poznamo goljufije, povezane s stranko, ponudnikom storitev in ponudnikom vsebin.

Spet drugje [**11**] so goljufije razporejene v štiri skupine (metode):

- sklenitev pogodbe z lažno dokumentacijo;
- uporaba telefonskega omrežja brez pooblastila;
- zavajanje telefonskega omrežja;
- notranji sodelavci.

5.4 Trendi

Vrednost transakcij in število storitev se bo povečevalo. Goljufije se bodo temu prilagodile tako, da bodo specializirane za posamezno storitev. Večina novih goljufij bo vezanih na storitev, in ne na povezavo [**17**] [**10**]. S porastom števila storitev se bo krajšala njihova življenjska doba. Podobno bodo tudi goljufije hitreje zastarele.

Vedno kompleksnejše storitve bodo občutljivejše za goljufije, vsaj dokler ne bo ustrezne standardizacije pri zbiranju podatkov iz omrežja in sistema za zaračunavanje.

Največja težava pri preprečevanju goljufij je (in bo tudi v prihodnosti) zagotavljanje varnosti internih informacij. Po podatkih iz [**17**] kar 73 odstotkov goljufij vključuje sodelovanje zaposlenih pri telefonskem operaterju, torej zlorabo notranjih informacij.

---

[13] Gre za storitev, ki omogoča plačevanje z uporabo mobilnega telefona (http://www.moneta.si/).

[14] Primer uporabe z uradne Mobitelove spletne strani.
Uporabnik Monete pri Mobitelu z mobilno številko 041 700 700 želi s petimi evri napolniti Mobiračun na številki 031 500 500. Kode PIN za Moneto ni aktiviral in je pri plačevanju z Moneto ne uporablja.
Ukaz: *127*5*031500500#

6 Sistem za upravljanje z goljufijami

Kot odgovor na naraščajočo nevarnost, ki jo predstavljajo goljufije, so telekomunikacijska podjetja začela razvijati sisteme za preprečevanje in odkrivanje goljufij. Rezultat takih prizadevanj imenujemo sistem za upravljanje z goljufijami (angl. Fraud Management System – FMS). V [**17**] je naslednja opredelitev: »Sistem za upravljanje z goljufijami je namenjen odkrivanju, raziskovanju in preprečevanju goljufij ter odpravljanju posledic, ki jih povzročijo.«

V delu [**18**] je podobna opredelitev: »Telekomunikacijski sistem za upravljanje z goljufijami je avtomatizirano orodje za odkrivanje in upravljanje z goljufijami v telekomunikacijskih storitvah. Običajno ima napredni grafični vmesnik, ki vključuje orodja za ročno raziskavo goljufij.«

Kot opozarja navedena definicija, je ročna raziskava goljufij pomemben del sistema. To pa je področje, na katerem lahko izkoristimo prednosti vizualizacije. Da bi lažje razumeli vlogo vizualizacije v takih sistemih, je treba najprej vedeti, kako ti delujejo.

V magistrski nalogi je sistem za upravljanje z goljufijami logično razčlenjen na faze, ki jih lahko opredelimo na podlagi nalog, ki jih sistem opravlja. Med nalogami so preprečevanje, odkrivanje, raziskovanje in odpravljanje posledic. Skupno ime zanje je upravljanje z goljufijami. Preslikava med nalogami in fazami ni bijektivna, naloge so združene v tri faze: preprečevanje, odkrivanje in obravnavanje.

Vsaka goljufija se začne s poskusom goljufije. Če je sistem ustrezno zaščiten in prepozna poskus, bo ta onemogočen in do goljufije ne bo prišlo. Za primer vzemimo gostovanje v tujini. V preteklosti je bilo zaradi slabe usklajenosti med operaterji možno ukraden telefon, katerega uporabo je lokalni operater že onemogočil, še nekaj časa uporabljati v tujini. Z uvedbo posodobljenih protokolov za izmenjavo podatkov med operaterji[15] se je čas odkrivanja takega poskusa goljufije skrajšal na nekaj sekund [**19**]. Naloga, ki jo opravimo v tej fazi, je preprečevanje, zato govorimo o *fazi preprečevanja*, v kateri postavimo prvi obrambni zid pred goljufijami.

Kadar sistemu ne uspe preprečiti goljufije, se loti naloge odkrivanja. V množici vsakodnevnih transakcij (v telefonskem omrežju je transakcija običajno telefonski klic) iščemo tiste, za katere obstaja možnost goljufije. Primer odkrivanja je uvedba pravila, ki opozori na dvakratno prekoračitev povprečnega tedenskega prometa naročnika. Faza, v kateri opravljamo to nalogo, je poimenovana *faza odkrivanja*.

Ko goljufijo odkrijemo (oziroma potrdimo, da je prišlo do suma goljufije), je čas za raziskovanje. Če je sum goljufije potrjen, jo preprečimo in začnemo odpravljati posledice. Skupek teh nalog zato lahko poimenujemo *faza obravnave*.

---

[15] Izmenjava podatkov iz gostovanja v skoraj realnem času (angl. Near Real-Time Roaming Data Exchange – NRTRDE) bo s prvim oktobrom 2008 postala obvezna za vse članice združenja GSMA.

Podobna razčlenitev je v [**15**], kjer je delovanje sistema za upravljanje z goljufijami opredeljeno v treh fazah – preprečevanje, odkrivanje in odvračanje.

Razlika je predvsem v tem, da tu obravnavamo fazi preprečevanja in odvračanja skupaj v fazi preprečevanja, dodamo pa še ločeno fazo, ki omogoča obravnavo odkritih goljufij (Slika 1). Kot bomo videli v nadaljevanju, je zadnja zanimiva predvsem zaradi možnosti uporabe vizualizacijskih orodij, s katerimi lahko obvladujemo množico alarmov, ki jih generira faza odkrivanja.

Slika 1: Sistem za upravljanje z goljufijami

Cilj sistema je zagotoviti okolje, v katerem bo večina goljufij preprečenih, preden bo povzročena večja škoda. Kako natančen naj bo ta sistem, pa je odvisno od meje, do katere je še smiselno raziskovati. Z višanjem meje preprečenih goljufij se zvišujejo stroški odkrivanja. Podobno, pretirano nadzorovanje strank, vodi v njihovo nezadovoljstvo. Zmerna meja nadzora (na primer opozarjanje ob preseženem limitu)[16] pa kaže le na pozornost ali dodatno skrb operaterja za naročnike.

Dober sistem za upravljanje z goljufijami lahko odloči, ali bo telekomunikacijsko podjetje preživelo ali ne. V delu [**11**] so podatki za srednje veliko podjetje, ki je imelo brez sistema za upravljanje z goljufijami mesečno tri milijone funtov stroškov, povezanih z goljufijami. Ko so v podjetju vzpostavili sistem za upravljanje z goljufijami, so se stroški v treh mesecih znižali na petdeset tisoč funtov mesečno.

[16] Tako storitev na primer ponuja Mobitel (http://www.mobitel.si). Imenuje se Monitor Alarm, ki uporabniku omogoča, da sam omeji mesečni znesek porabe. Ko doseže vnaprej določeni mejni znesek, je o tem obveščen s sporočilom SMS (angl. Short Message Service – SMS) in po elektronski pošti. Mobilni telefon lahko uporablja še naprej, vendar v vednosti, da je prestopil lastno določeno mejo mesečne porabe.

Stopnja preprečenih goljufij je bistvenega pomena pri merjenju uspešnosti sistema FMS, ki je vreden toliko, kolikor goljufij smo z njim onemogočili in preprečili. Ker je to težko oceniti, se uporabljajo kazalniki, kot so [**10**]:

- odstotek transakcij, za katere se pojavi sum goljufije (izjem) in se izkaže, da niso goljufije;
- odstotek izjem, za katere se izkaže, da so goljufije;
- povprečni čas, potreben za obdelavo izjeme;
- odstotek neobdelanih izjem.

V nadaljevanju so nekoliko natančneje predstavljene posamezne faze sistema za upravljanje z goljufijami.

7 Prva faza upravljanja: preprečevanje goljufij

V fazi preprečevanja goljufij poskušamo poskrbeti, da do goljufij sploh ne pride, oziroma zagotovimo elemente, ki bodo omogočili takojšnjo preprečitev poskusa zlorabe. Primer prvega je uvedba posebnega kanala za prenos kontrolnih signalov v SS7 (angl. out-of-band signaling), ki je preprečil manipulacijo s kontrolnimi signali. Za primer drugega pa nadaljujmo z goljufijo spreminjanja zapisov v zbirki podatkov HLR (glejte razdelek 5.3 Vrste goljufij; razvrstitev po kritičnem elementu). Take goljufije preprečimo z omejevanjem dostopa do zbirke podatkov HLR. Dostop omogočimo samo ključnim osebam, ki jim zaupamo. Vsi popravki in dodani zapisi v HLR vsebujejo tudi ID osebe, ki je naredila popravek ali vnesla nov zapis. Vpeljemo postopke za odkrivanje klicev z neregistriranega MSISDN-ja.

Preprečevanje goljufij zahteva dobro poznavanje omrežja, ki ga uporabljamo, vseeno pa lahko opredelimo nekaj splošnih metod, ki veljajo za večino omrežij. Metode za preprečevanje in odvračanje goljufij so v magistrski nalogi razdeljene na tehnične in netehnične. Podobno so v [**20**] razdeljene na tehnične metode in metode socialnega inženiringa. Netehnične so zastavljene malo širše.

7.1 Tehnične metode

Gre za metode oziroma pristope, ki temeljijo na tehničnih rešitvah, najznačilnejše med njimi pa so naslednje:

- Skrb za varnost in zanesljivost protokolov za prenos podatkov. Primer je razvoj iz mobilnih omrežij 1G in 2G v 3G, ki je na področju nepooblaščenega zajemanja podatkov in nelegalne uporabe storitev precej varnejše kakor njegova predhodnika [**4**] [**21**].
- Strog nadzor nad mednarodnimi klici, še posebej v države z visoko stopnjo možnosti goljufije (na primer Pakistan).
- Uporaba tehničnih rešitev, kot so gesla, identifikacijske številke, preverjanje identitete pred klicem, overjanje identitete in uporaba enkripcije. Zanimiv pristop, opisan v [**22**], je zagotovitev avtentičnosti z digitalnim vodnim žigom (angl. digital watermark). Prednost takega pristopa je, da ne poveča količine podatkov, ki se prenašajo od oddajnika do sprejemnika.
  Problematično varnostno področje je pretvarjanje med različnimi protokoli. Pri prehodu iz omrežja PSTN v omrežje NGN se na primer pretvarja tudi med varnostnimi mehanizmi.
- Uporaba sistema honeypot (namenjenega izključno privabljanju napadalcev; dobesedni prevod iz angleščine je *lonček medu*, nekoliko primernejši pa je izraz *muholovec*) za analiziranje in preprečevanje napadov [**23**] [**24**].
- Občasno izvajanje preskusov odpornosti proti prodiranju (angl. penetration tests). Najbolj nepristranske rezultate dobimo, če za to najamemo zunanje sodelavce.
- Integracije »samoobrambe« pred določenimi napadi na ravni usmerjevalnikov (angl. Self-Defending Networks) [**25**].

7.2 Netehnične metode

V to skupino spadajo metode oziroma pristopi, ki ne temeljijo na tehničnih rešitvah. Gre predvsem za izobraževanje in odnose med udeleženci. Primeri netehničnih metod so naslednji:

- Kazensko zasledovanje povzročiteljev goljufij. Odmevne sodbe, katerih rezultat so visoke denarne odškodnine in zaporne kazni, delujejo na morebitne goljufe kot psihološka ovira. Če ti vedo, da z goljufijo veliko tvegajo, bodo dvakrat premislili, preden se je bodo lotili. Tudi strogo (oziroma prestrogo) kaznovanje nedolžnih vdorov lahko močno vpliva na število poskusov goljufij v prihodnosti. Pomembno je, da se prenese sporočilo – ne dotikajte se našega sistema.
- Vzdrževanje črnega seznama rizičnih držav in PRN-številk, ki jih uporabnik ne more klicati. Mednje spadajo države in številke, ki se pri goljufijah pogosto pojavljajo. Če jih uporabnik želi klicati, mora podpisati dodatek k veljavni pogodbi. Tako se učinkovito zmanjša populacija naročnikov, ki so občutljivi za dolg seznam goljufij brez posebnega posega v uporabnost storitev.
  Po podatkih AT&T[17] je dobro biti pozoren tudi na klice, ki izvirajo s »sumljivih območij«. Kot primera sta navedeni območni kodi 212 in 718 v New Yorku (gre za Bronx, Queens, Brooklyn ...).
- Obveščanje uporabnika, ko pride do večje porabe sredstev. Uporabnik mejo, pri kateri želi biti obveščen, določi, ko podpiše naročniško pogodbo.
- Omejevanje uporabe za nove naročnike. Pomembno je natančno preverjanje identitete novega naročnika.
- Izobraževanje zaposlenih v telekomunikacijskem podjetju, da so pripravljeni na napade, ki vključujejo metode socialnega inženiringa. Vpeljati je treba postopke, ki zmanjšujejo možnost takih napadov. Pomembno pa je tudi izobraževanje strank. Predvsem zaposleni v podjetjih s hišnimi centralami morajo biti dobro seznanjeni z morebitnimi goljufijami.
- Naročniške pogodbe, ki določajo varnostne parametre in predvideni profil naročnika.
- Lobiranje za poostritev zakonov, ki vplivajo na kaznovanje storilcev goljufij, in omilitev tistih, ki ščitijo varovanje osebnih podatkov. Slednji preprečujejo učinkovito zbiranje podatkov o storilcih goljufij.

7.3 Posebni pristopi

V [**23**] je govor o bolj kontroverznem načinu preprečevanja goljufij – agresivni samoobrambi. To pomeni, da takrat, ko zasledimo poskus goljufije, preidemo v napad na morebitnega povzročitelja goljufije. Cilj je identificirati napadalca. V istem delu je opisan model ADAM (angl. Active Defense Algorithm and Model), ki je razdeljen na stopnje, in sicer načrtovanje, odkrivanje, evaluacijo, odločitev, akcijo, eskalacijo in

[17] Več je na spletnem naslovu: http://www.corp.att.com/business_billing/fd_fraud2.html.

vzdrževanje stanja. Pristop je kontroverzen, ker lahko pri analizi napada nenamerno kršimo pravice strank ali strežnikov, ki so uporabljeni kot vmesne točke pri napadu.

7.4 Pomen vizualizacije

Ali lahko vizualizacija prispeva k učinkovitejšemu delovanju te faze? Načeloma ne, saj tu govorimo o zaščitnih elementih, ki so že vgrajeni v sistem (primer je geslo za dostop do e-poštnega predala). Lahko pa uporabimo povratne informacije zaščitnih elementov. Gre za to, da opazujemo dogodke, ki aktivirajo določen zaščitni element. Program, namenjen preverjanju identitete uporabnika, ki ima dostop do e-poštnega predala, bo sporočil, ali uporabnik večkrat vpiše napačno geslo. To pa je že informacija, ki jo lahko vizualiziramo. Tako na primer lahko odkrijemo uporabnika, ki bo z iste številke poskušal izvesti dostop do več različnih e-poštnih predalov, pri čemer bo ugibal gesla za dostop do njih. Primer take vizualizacije so stolpičasti grafi, ki prikazujejo obvestila o aktiviranju zaščitnih elementov in mape za prikaz lokacije kršitev. Natančnejši primeri so predstavljeni v nadaljevanju.

Cilj je prikaz povratnih informacij z zaščitnih elementov.

8 Druga faza upravljanja: odkrivanje goljufij

Ta faza je namenjena hitremu in učinkovitemu odkrivanju goljufij, ki se jim je uspelo izogniti prvi fazi in se torej že izvajajo. V delu [**10**] se iskanje goljufije primerja z iskanjem igle v kopici sena, saj se vedenje običajnih uporabnikov storitev in goljufov ne razlikuje preveč. Običajno vedenje pri prvem lahko pomeni goljufijo pri drugem.

V [**16**] je predstavljen model faze (oziroma v tem primeru sistema) odkrivanja goljufij. Razdeljen je na štiri ravni. Po avtorjevem mnenju lahko vsako goljufijo odkrijemo na eni izmed naslednjih ravni:

- Na ravni cilja goljufije, ki je najsplošnejša raven, so vse goljufije enake. Da bi na primer prepoznali uporabnike, ki se poskušajo izogniti plačilu (cilj), primerjamo porabo resursov v omrežju s stanjem v sistemu za zaračunavanje.

  Primeri ciljev: izogibanje plačilu, kršitev dogovora o ravni storitve (angl. Service Level Agreement – SLA) in skrivanje identitete.

- Na ravni akterjev lahko s preučevanjem odnosov med akterji z določeno natančnostjo ugotovimo, kdo je morebitni goljuf in kdo morebitna žrtev.

  Primeri akterjev: ponudnik e-plačila (tretja oseba, ki skrbi za finančne transakcije), uporabnik, gost (akter, ki ni registrirani uporabnik), ponudnik storitve (tretja oseba, ki ponuja storitve, kot so brezplačne številke – običajno je to operater) in ponudnik vsebine (tretja oseba, ki ponuja vsebine za storitve, na primer klic v stiski, ki deluje na brezplačni številki).

- Raven tveganja za storitev je specifična za posamezne storitve. Z dobrim poznavanjem storitve lahko predvidimo, kako jo bodo goljufi poskusili napasti. Značilnosti goljufije lahko opredelimo na podlagi poznavanja storitve.

- Na ravni tehnike goljufije, ki je najmanj splošna raven, obravnavamo posamezne goljufije. Goljufije poskušamo odkriti z znanimi tehnikami in s tarčami napada. Opazujemo tehnične prvine, kot so mehanizmi preverjanja istovetnosti, registracije novih strank in podobno.

  Primeri takih vrst tehnike so socialni inženiring, kraja in prisluškovanje.

Tradicionalno iščemo goljufije v razmerju med stranko in operaterjem. Novost opisanega modela je natančnejša opredelitev vira goljufije, ki ne prihaja samo od strank oziroma zunanjega sveta, pač pa tudi od poslovnih partnerjev. To so lahko ponudniki storitev, ponudniki vsebin in ponudniki e-plačila. Nekatere možne goljufije so zaračunavanje storitev, ki jih stranka ni opravila, na strani ponudnika e-plačila, prikrivanje resničnih podatkov ponudnika storitev o prodaji pred ponudnikom vsebin in podobno.

Nekoliko manj obširen model zasledimo v delu [**26**], kjer je faza odkrivanja goljufij omejena na algoritem za odkrivanje, sestavljen iz dveh komponent. Prva predstavlja povzetek aktivnosti na računu, ki se lahko osvežuje v realnem času, druga pa pravila, ki jih uporabljamo pri tem povzetku in ki omogočajo

identificiranje goljufije. To sicer ni zelo natančna definicija, podaja pa dobro osnovo za razumevanje faze, o kateri je govor.

Pri opredelitvi faze odkrivanja goljufij je lahko v pomoč tudi naslednja splošna definicija, ki jo zasledimo v [**16**]. Tu je faza odkrivanja goljufij opredeljena kot skupek tehnik za odkrivanje dogodkov v sistemu, ki kršijo varnostno politiko. Ta je lahko opredeljena eksplicitno ali pa implicitno.

Ne glede na model oziroma definicijo od sistema za upravljanje z goljufijami pričakujemo, da v fazi odkrivanja goljufij poskrbi za:

- odkrivanje goljufij v realnem času, ko se mora odzvati na dogodke (angl. event driven); goljufijo mora zaznati, medtem ko se ta izvaja, in ne šele takrat, ko je že končana, kajti če predolgo ne ugotovimo, da je prišlo do goljufije, so izgube precej večje;
- analizo vseh prejetih podatkov v realnem času, pri čemer je hitrost procesiranja zelo pomembna;
- uporabo ugotovitev iz te faze za izboljšanje faze preprečevanja goljufij;
- sposobnost učenja in prepoznavanja legitimnih sprememb v vedenju naročnika;
- prepoznavanje že znanih goljufij in sposobnost učenja prepoznavanja novih; oblike goljufij in vedenje strank se hitro spreminjajo, zato so sistemi, ki tega ne zagotovijo, kmalu zastareli;
- modularno zgradbo sistema, ki omogoča hitro in preprosto nadgraditev;
- Neodvisnost od omrežja, v katerem se izvajajo storitve;
- neodvisnost od storitve, sicer moramo storitev zelo dobro poznati pri zbiranju podatkov;
- zmožnost samodejne inicializacije pri dodajanju novih uporabnikov in storitev.

Za učinkovito odkrivanje goljufij potrebujemo kakovostne podatke o transakcijah, o katerih je govor v naslednjem razdelku.

8.1 Zajem podatkov

Najpomembnejša vira informacij za raziskavo in odkrivanje goljufij sta sistem za zaračunavanje (angl. billing system) in posredovalni sistem (angl. mediation system), v katerem se pripravljajo podatki tudi za prvega.

Informacije, ki jih potrebujemo pri iskanju oziroma identifikaciji goljufij, so predstavljene v nadaljevanju.

- Informacije o naročniku.

  Fiksna telefonija:

  - telefonska številka,
  - identifikacijska številka uporabnika (naročniška številka).

  Mobilna telefonija:

  - telefonska številka,
  - identifikacijska številka uporabnika,
  - mednarodna identifikacijska številka mobilne opreme (angl. International Mobile Equipment Identity – IMEI).[18]

  Telefonija VoIP:

  - identifikacijska številka uporabnika,
  - naslov MAC.

    Kot računalniki imajo vsi IP-telefoni omrežno kartico (angl. Network Interface Card – NIC). Ta je nujna, ker priskrbi MAC-naslov (angl. media access control).[19] Za sledenje naročniku je uporaben tudi IP-naslov s številko vrat (angl. port), vendar pa zaradi dinamičnosti storitve ni dovolj za enolično identifikacijo.

- Informacije o storitvi. Zanimiv podatek je na primer način plačila storitve. Plačnik je lahko tretja oseba, oseba, ki je zahtevala storitev (pri telefonskem klicu je to klicoči) ali soudeleženec pri storitvi (pri telefonskem klicu je to klicani). Pomembni so še drugi podatki o storitvi, na primer tip razmerja (predplačniško ali naročniško razmerje, testni uporabnik …).
- Podatki o klicih ali pa transakcijah. Poenotene in urejene zapise dobimo iz posredovalnega sistema, ki zbira zapise o klicih ter jih poveže s tipom storitve in ceno na enoto [**15**]. Na podlagi vseh dosegljivih

[18] To je unikatna 15-številčna oznaka mobilne opreme, shranjena v mobilnem telefonu na SIM- kartici.
[19] Običajno je predstavljen v šestnajstiški obliki. Primer veljavnega MAC-naslova je 00-0A-E4-02-7B-99.

informacij tvori nov zapis, ki vsebuje prečiščene informacije vhodnih zapisov. Vhodni podatki so med drugim lahko:

- Zapis o klicu

  Zapis o klicu (angl. Call Detail Record – CDR)[20] je glavni vir podatkov za posredovalni sistem. Tipični CDR vsebuje informacije o identifikaciji vira in cilja, številki vira in cilja, dolžini klica, času začetka klica in posebnostih klica (na primer konferenčni, lokalni, mednarodni …).

- Zapis o storitvi

  Posplošen zapis CDR ali zapis o storitvi (angl. Usage Detail Record – UDR) beleži vsak dogodek, ki nastane pri uporabi neke storitve, na primer konec telefonskega klica, sprejeti klic, poslano kratko sporočilo SMS, opravljeni klic v gostovanju in sprejeto glasovno pošto. Zapis ni standardiziran, zato je veliko različic. Glavni problem uporabe UDR-zapisov v omrežjih nove generacije je, da niso dovolj fleksibilni in zanesljivi za opis vseh vedno raznovrstnejših storitev [**17**]. Alternativa UDR-zapisom v omrežjih nove generacije je zapis IPDR[21] (angl. Internet Protocol Detail Record).

- Zapis o storitvi v IP-okolju IPDR

  Vsak IPDR vsebuje pet elementov, ki opisujejo storitev: kdo, kdaj, kaj, kje in zakaj. Dodatni atributi, ki natančneje opisujejo določeno storitev, se določijo, če je treba. Dodamo na primer informacije o kakovosti storitve, pasovni širini, prehodnem času (angl. latency) in stanju klica (končan običajno, v teku, napaka v omrežju, napačen naslov …). Če storitev to zahteva, vsebuje tudi informacije o uporabi različnih virov v omrežju [**27**]. IPDR lahko zapišemo v dveh formatih: XML (angl. eXtensible Markup Language) in XDR (angl. eXternal Data Representation).

  Če storitev to omogoča, so zelo zaželene informacije o fizični lokaciji uporabnikov, ki dodatno omogočajo identifikacijo goljufov.

- Podatki iz sistema za zaračunavanje.

  Sistem za zaračunavanje nadzira uporabo storitev in ustrezno spreminja strankin račun na podlagi uporabe in cene teh storitev [**27**]. Podatki iz njega omogočajo spremljanje, kdaj je stranka plačala račun, ali ji je bilo treba poslati enega ali več opominov, morda izključiti storitev, dokler ne plača računa, kolikšen je povprečni čas, v katerem stranka plača račun, koliko znaša povprečni račun posamezne stranke v določenem časovnem obdobju in podobno.

- Povzetki zgodovine so koristni, ker ni praktično vedno znova analizirati vseh podatkov. Novejši podatki so pomembnejši in zato močneje uteženi.

---

[20] Včasih se uporablja tudi oznaka Toll Ticket oziroma zapis SMDR (angl. Station Message Detail Record).
[21] Za specifikacijo IPDR-zapisa glejte [**2**].

- Podatki iz omrežnega, aplikacijskega, avtentikacijskega in dostopnega nivoja [**18**] [**28**], na primer varnostni dnevniki prometa iz kritičnih elementov omrežja (usmerjevalniki, medijski prehodi in požarni zidovi).
- NGN-omrežja lahko vsebujejo tudi sisteme za odkrivanje vdorov (angl. Intrusion Detection System – IDS[22]) in sisteme za preprečevanje vdorov (angl. Intrusion Prevention Systems – IPS), ki so odličen vir podatkov in dober indikator nevarnosti goljufije [**25**].

Naslednji korak je analiziranje pridobljenih podatkov, ki je najpomembnejši del faze odkrivanja goljufij.

8.2 Analiza

Pri analizi vhodnih podatkov iščemo značilne pokazatelje goljufij, kot so dolgi in pogosti klici ter klici na PRN-številke, ki jih obravnavamo v določenem kontekstu. Kontekst je na primer ura, časovno okno in pripadnost določeni skupini strank.

Nekateri najznačilnejši pristopi k analizi podatkov in ugotavljanju anomalij so naslednji:

- Določitev fiksnega praga (angl. threhold-based techniques)

  Določimo fiksno mejo, ki ne sme biti prekoračena. Primer takega praga je dolžina klica na PRN-številke, omejena na 15 minut. Taka preprosta pravila so dobra za odkrivanje goljufij, pri katerih se pojavijo ekstremna odstopanja.

- Pravila (angl. rules-based techniques)

  Na podlagi izkušenj se postavi množica pravil, pri katerih se sprožijo alarmi. Značilni primeri pravil so nenadno precejšnje povečanje prometa na računu, klici iz dveh geografsko oddaljenih mest v kratkem časovnem razmiku in klici z istega računa, ki se prekrivajo.

- Profil

  Profil je statistični model, ki opisuje zgodovino vedenja naročnika. Primerjava trenutnega vedenja z zgodovinskim omogoča odkrivanje spremembe v vedenju uporabnika storitve. Profil predstavlja

[22] Metode odkrivanja, ki jih uporabljata sistema IDS in FDS, so v večini primerov zelo podobne, čeprav sta to tradicionalno dve popolnoma ločeni področji. Zaradi prehoda na NGN pa se pojavlja zahteva po njuni združitvi. Več raziskav je bilo izvedenih za sisteme IDS. Zanimivo je, da v gradivu, ki preučuje sisteme FDS, ni veliko referenc za IDS-vire.

običajno vedenje, vsakršno večje odstopanje pa je znak za alarm. Gradi se na podlagi zgodovine, ki se redno posodablja, in trenutnega stanja.

Izdelamo ga lahko na ravni posamezne storitve, skupine uporabnikov ali posameznega uporabnika storitve. Prva raven je namenjena iskanju odstopanja vedenja posameznega uporabnika od povprečja storitve. Kadar predvidevamo, da se bodo določene skupine uporabnikov vedle podobno [**15**], izberemo drugo možnost. Uporabnike na primer razdelimo v skupine glede na tip naročniškega razmerja. Od naročnikov poslovnega paketa lahko pričakujemo veliko klicev, tudi mednarodnih, medtem ko tako vedenje za lastnike študentskega naročniškega paketa ni najznačilnejše.

Ker iščemo odstopanja od modela, zgrajenega na podlagi zgodovine računa, lahko naletimo na nekaj težav. Problemi pri izgradnji modelov so novi naročniki, ki še nimajo zgodovine, intervali obnavljanja (lahko se obnavljajo ob fiksno določenih intervalih ali pa stalno; slednje je seveda boljše, a težje izvedljivo) in čistost profila (ta vsebuje tudi vedenje ob neodkritih goljufijah).

Pri izdelavi profila ocenjujemo vrednosti, kot so povprečna in najdaljša dolžina klica ter število klicev v določeno regijo, pri tem pa upoštevamo tudi parametre, kot sta čas v dnevu in tip storitve.

- Nevronske mreže

  Gre za učenje na podlagi vzorcev nevronskih mrež, ki so zanimivi prav zaradi sposobnosti učenja, ki omogoča odkrivanje še neznanih goljufij.

- Metoda podpornih vektorjev

  Metoda podpornih vektorjev (angl. Support Vector Machine – SVM) je razmeroma nova družina metod s področja strojnega učenja, ki nadomešča nevronske mreže.

Obstaja pa tudi splošnejša delitev analiz, pri kateri ločimo dva tipa:

- Pri absolutni analizi (angl. supervised analysis) imamo množico, ki predstavlja običajno vedenje, in množico, ki predstavlja vedenje v primeru goljufije. Rezultat analize je uvrstitev opazovanih zapisov v eno izmed množic. Slabost tega tipa analize je, da moramo imeti množico, ki predstavlja vedenje v primeru goljufije.
- Pri diferencialni analizi (angl. unsupervised analysis) ne potrebujemo množice, ki predstavlja vedenje v primeru goljufije, pač pa iščemo zapise, ki se precej razlikujejo od povprečja in kažejo na nenadne spremembe v vedenju uporabnika storitve. Bistvo te vrste analize je v tem, da zgodovinsko povprečje primerjamo s trenutnim stanjem, slabost pa se na primer pokaže pri vpeljavi novih storitev, saj se bodo njihovi zapisi precej razlikovali od dotedanjih.

Ker pri procesu odkrivanja goljufij govorimo o ogromni količini podatkov, so pomembne tudi metode odkrivanja zakonitosti v podatkih (angl. data mining techniques).[23] Še prej pa je treba podatke združiti v obvladljivo in razumljivo celoto. Uporabljajo se metode združevanja, umikanja redundantnih zapisov in grupiranja z gručami (angl. data clustering). S primerno grafično predstavitvijo podatkov je včasih lažje kar z ročnim pregledom izslediti nenavadna odstopanja od povprečja, ki spremljajo goljufijo [**20**]. Podrobnosti o tem so predstavljene v poglavju 10 Vizualizacija.

Rezultat analize je verjetnost, da je prišlo do goljufije (angl. suspicion score). Analiza le redkokdaj lahko potrdi, da je zagotovo prišlo do goljufije. Namenjena je le za alarmiranje, da je prišlo do nepravilnosti v vedenju uporabnika, torej da obstaja sum goljufije.

8.3 Izhodni podatki

V fazi odkrivanja goljufij iz pridobljenih podatkov za vsakega uporabnika izluščimo informacije, kot so:

- število oziroma trajanje lokalnih klicev v posameznem intervalu;
- število oziroma trajanje klicev v tujino v posameznem intervalu;
- število oziroma trajanje klicev na številke, za katere obstaja velika verjetnost, da so vpletene v goljufijo, v posameznem intervalu;
- verjetnost, da je uporabnik vpleten v goljufijo;
- kategorija uporabnika (npr. goljuf, osumljen goljufije, dolžnik, običajen in partner).

Poleg tega za uspešno obravnavo v naslednji fazi za vsako transakcijo, ki je označena kot sumljiva, posredujemo naslednje podatke:

- od kod izvira transakcija, za katero obstaja sum goljufije (izvor);
- cilj transakcije, za katero obstaja sum goljufije (ponor);
- verjetnost goljufije;
- kritičnost goljufije;
- začetek, trajanje in dodatne lastnosti transakcije;
- opis goljufije (namenjen je le za orientacijo analitikom).

[23] Odkrivanje zakonitosti v podatkih ali podatkovno rudarjenje je multidisciplinarno področje, ki vključuje tehnologije zbirk podatkov, statistiko, umetno inteligenco in strojno učenje.

Morebitne izboljšave, ki bi prispevale h kakovostnejšim izhodnim podatkom in predvsem k hitrejšemu odkrivanju goljufij, so naslednje:

- zaračunavanje v realnem času (angl. real time billing), podobno kot v predplačniškem naročniškem razmerju;
- standardizacija zapisa o uporabi storitve;
- razvoj splošnih indikatorjev, ki so neodvisni od opazovane storitve.

8.4 Pomen vizualizacije

V primerjavi s prejšnjo fazo je tu veliko več možnosti za uporabo vizualizacije. Na voljo je veliko večdimenzionalnih vhodnih podatkov, ki opisujejo transakcije. Te želimo predstaviti na način, ki bo izpostavil transakcije z izstopajočimi vrednostmi posameznih atributov (na primer dolge klice na mednarodne številke), relacije med atributi (na primer prikaz odvisnosti med vrednostjo klica in tipom naročniškega paketa) in relacije med transakcijami (na primer primerjavo lastnosti vseh klicev v tujino, ki so daljši od neke mejne vrednosti). Mogočih je veliko pristopov k vizualizaciji velike količine podatkov, značilna pa je predvsem uporaba grafov in tabel. Natančnejši primeri so predstavljeni v nadaljevanju.

Cilj je pomagati analitiku pri odkrivanju goljufij.

9 Tretja faza upravljanja: obravnava izjem

V fazi obravnavanja izjem poskrbimo za grupiranje in natančnejšo analizo alarmov. Glavna naloga je učinkovit odziv na morebitne goljufije (izjemne transakcije oziroma izjeme).

V fazi obravnavanja izjem je pomembno naslednje:

- Pri obravnavi izjem moramo biti izjemno previdni.

  Vsako nadpovprečno trajanje klica ali povečano število klicev še ne pomeni, da je res prišlo do goljufije. Kot rečeno, faza odkrivanja goljufij le z določeno verjetnostjo potrdi, da je prišlo do goljufije.

  O resnosti problema nenatančnosti odkrivanja goljufij pričajo podatki za sisteme IDS, kjer velja, da lahko povprečen sistem vrne kar do 99 odstotkov lažnih alarmov [**29**] [**30**]. Poleg tega pa še vedno obstaja verjetnost, da je zgrešil goljufijo.

  Manj kritične alarme lahko ignoriramo, seveda pa s tem povečamo možnost, da nam uide več goljufij ali pa vsaj, da zgrešimo predhodne znake, ki bi prispevali k preprečitvi goljufije.

- Med komunikacijo z »osumljenimi« uporabniki moramo biti prijazni in pri njih vzbuditi vtis, da skrbimo za njihovo varnost.

  Gre za uporabnike, ki opravijo nadpovprečno veliko prometa in so zato dobrodošli pri vseh operaterjih.

- Izjeme po prioriteti razdelimo na več razredov.

  Vsak razred ima svoj proces obravnavanja izjem. Izjema z veliko verjetnostjo goljufije ali verjetnostjo, da bo morda povzročila veliko škode, bo šla v prvi razred z najvišjo prioriteto in bo tako takoj prišla v obravnavo.

- Uporabimo pridobljeno znanje.

  Podatki, ki jih pridobimo o novih goljufijah, se uporabijo kot izhodišče za izboljšanje zaščitnih elementov telekomunikacijskega sistema.

Faza obravnavanja izjem ima svojo ceno in se je ne da stoodstotno avtomatizirati. Odločiti se je treba, kako natančno bomo zasledovali izjeme. Nekaterih preprosto ni vredno preverjati, saj so stroški zasledovanja večji od morebitne škode, ki bi jo goljufija lahko povzročila. Del avtomatizacije je filtriranje že znanih alarmov, ki so nenevarni, in jih ne nameravamo zasledovati.

Algoritem GSAL [**31**] grupira do 95 odstotkov alarmov v že znane skupine, torej ostane le nekaj odstotkov za natančnejšo obravnavo. V omenjenem delu se sicer obravnava sistem za odkrivanje vdorov, namenjen računalniškim omrežjem. Primerljive rezultate lahko pričakujemo tudi v omrežju NGN, saj se to približuje oziroma je že enakovredno klasičnim računalniškim omrežjem [**16**].

Prehod v fazo obravnavanja izjem sta opis izjeme in verjetnost, da je izjema v resnici goljufija. Ko potrdimo, da gre za goljufijo, govorimo o incidentu. V [**32**] je varnostni incident opredeljen kot nedovoljen dogodek ali nevarnost v informacijskem sistemu. To je med drugim lahko nedovoljen dostop, uporaba škodljive kode, nedovoljeno nadziranje in pregledovanje sistema ter napad, ki preprečuje dostop do storitve (angl. denial of service attack). Dejavnosti, povezane z obvladovanjem incidenta, združimo v program za delovanje v primeru incidenta (angl. Incident Response Program – IRP).

9.1 Načrt delovanja v primeru incidenta

Če se organizacija (ponudnik telefonskih storitev) ne zna pravilno odzvati na zaznano goljufijo, se lahko znajde v velikih težavah. Poleg finančne škode sta povzročena še izguba časa zaposlenih, ki vsak po svoje neorganizirano poskušajo onemogočiti in preprečiti nelegalne dejavnosti, in izguba zaradi motenj v opravljanju storitev. Odgovor na to sta zbirka znanja, ki združuje dozdajšnje znanje o goljufijah, in program, ki določa delovanje v primeru incidenta.

Priprava načrta delovanja v primeru incidenta je eden izmed cenovno najučinkovitejših varnostnih ukrepov, ki jih lahko sprejme neka organizacija [**33**]. Izdelava načrta ni enkratno opravilo, pač pa proces, ki mora zagotoviti, da se ta obnovi ob organizacijskih in infrastrukturnih spremembah ter takrat, ko odkrijemo nove nevarnosti ali ranljivosti sistema. To se lahko zgodi, kadar pride do incidenta, ali pa ko iz drugih virov prejmemo ustrezne informacije.

Vpliv učinkovitega načrta se neposredno odraža na škodi, ki jo neka goljufija povzroči, in posredno na ugledu podjetja. Zadnje lahko utrpi nepopravljivo škodo, če se organizacija ne zna odzvati na goljufijo, in se nasprotno lahko celo izboljša, če z goljufijo opravi hitro in učinkovito. To v večini primerov pomeni, da prevzame nadzor, prepreči nadaljnje goljufije takega tipa in kaznuje odgovorne osebe.

Inštitut SANS (angl. SysAdmin, Audit, Network, Security) je populariziral metodologijo, ki je bila razvita za potrebe ameriških vladnih institucij. Metodologija v šestih korakih določa delovanje v primeru incidenta (angl. incident response). Vsebuje naslednje korake: priprave (angl. preparations), identifikacijo (angl. identification), prevzem nadzora (angl. containment), čiščenje (angl. eradication), obnovitev (angl. recovery) in zasledovanje (angl. follow-up). Ne glede na resnost incidenta je pomembno, da opravimo vse korake [**32**].

Gre za splošno metodologijo, ki pa jo lahko brez težav povežemo z delovanjem v primeru goljufije. Posamezni koraki so natančneje predstavljeni v nadaljevanju.

Priprave

V tem koraku poskrbimo za vse, kar je treba narediti pred incidentom oziroma v našem primeru pred sumom goljufije. Vsebuje dejavnosti, kot so:

- pripravo orodij, ki jih bomo potrebovali v naslednjih fazah;
- preučevanje sistema in zbiranje informacij;
- konfiguracijo sistema, ki omogoča zbiranje podatkov in optimalno delovanje naslednjih korakov;
- določitev odgovornosti in formacijo skupine;
- pripravo procedure delovanja v primeru incidenta;
- postavitev poti obveščanja in načinov sporočanja (uporabimo lahko osebni klicnik (angl. pager), mobilni telefon, glasovno in elektronsko pošto …).

Z zbiranjem informacij o delovanju sistema lahko že v tem koraku prepoznamo možnosti za izboljšanje varnosti, ki zmanjšujejo verjetnost, da bo prišlo do incidenta. Podobno se moramo prepričati, da je sistem posodobljen z zadnjimi popravki in nadgradnjami[24] ter da so zaposleni primerno seznanjeni z najnovejšimi varnostnimi smernicami. V našem primeru za take dejavnosti poskrbimo v fazi preprečevanja goljufij.

Bistveno je, da se v tem koraku pripravijo procedure delovanja v primeru incidenta, ki so vgrajene v splošno varnostno politiko organizacije. Ta mora preprečiti zmešnjavo, ki nastane ob odkritju incidenta.

Procedure za delovanje v primeru incidenta vsebujejo tudi navodila za določitev prioritetnega razreda izjeme. Naslednja tabela prikazuje preprost primer klasifikacije incidentov.

[24] Odličen vir za posodobitve je internet. Na primer za sisteme CISCO je na voljo veliko pomembnih informacij na http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Prioriteta	Definicija	Primer
Visoka	Incident povzroča kritičen vpliv na poslovanje organizacije ali izvajanje storitev.	Ustanovitev ponudnika storitev VoIP z namenom goljufije (glejte razdelek 10.8.10 Ustanovitev ponudnika storitev VoIP z namenom goljufije)
Srednja	Incident vpliva na poslovanje organizacije ali izvajanje storitev.	Beige box (glejte razdelek 10.8.2 Beige box)
Nizka	Incident ne vpliva preveč na poslovanje organizacije ali izvajanje storitev.	Nedovoljeno nadziranje in pregledovanje sistema

Identifikacija

V našem primeru opozorila, da je prišlo do poskusa ali dejanske goljufije, prihajajo z različnih strani. Glavni vir je faza odkrivanja goljufij, od katere pričakujemo največ opozoril. Drugi pomemben vir je klicni center, ki na podlagi strankinih težav in pritožb sklepa, da se v sistemu dogaja nekaj neobičajnega. Ta opozorila so načeloma zanesljivejša od prvih, saj jih je delno že potrdilo osebje v klicnem centru. Tretji vir informacij je redno pregledovanje sistema (na primer dnevnikov prometa pri kritičnih elementih sistema).

V tem koraku moramo najprej potrditi, da je res prišlo do incidenta. Analiziramo vse podatke, ki so na voljo. Pri tem moramo biti izjemno pozorni, kako ravnamo s podatki, ki so povezani z incidentom. Ti so lahko uporabljeni kot dokazno gradivo na sodišču, če pride do kazenskega pregona. Zabeležimo natančno zaporedje odvijanja dogodkov, ki so pripeljali do incidenta, pri tem pa pazimo, da podatkov ne kontaminiramo. Glavni viri podatkov, o katerih govorimo, so dnevniki dogajanja na različnih elementih v omrežju, ugotovitve analitikov in izsledki sistema, ki je posredoval opozorilo, da je prišlo do incidenta. Če sumimo, da je do incidenta prišlo v podjetju, sta zanimiva dnevnik dostopa po navideznem zasebnem omrežju (angl. Virtual Private Network – VPN) in dnevnik fizičnega dostopa do prostorov organizacije.

Tudi starejši dnevniki dogajanja so lahko koristni, saj je zelo verjetno, da je napadalec že prej zbiral podatke o sistemu in iskal njegove šibke točke. Taki na videz nedolžni dogodki so zapisani v dnevnikih in lahko pomagajo identificirati napadalca.

Prevzem nadzora

V tem koraku preprečimo širjenje incidenta in poskušamo omejiti škodo s preprečevanjem dostopa do sistema, z rekonfiguracijo sistema, zamenjavo ali nadgradnjo varnostnih elementov in onesposobitvijo rizičnih računov.

Poskrbeti moramo, da ne izgubimo morebitnih dokazov o incidentu. Ker sisteme potrebujemo za običajno delovanje in jih ne moremo izolirati kot dokazno gradivo, si lahko pomagamo z izdelavo varnostnih kopij oziroma posnetkov stanja prizadetih sistemov, ki jih potem uporabimo za nadaljnje analiziranje.

Čiščenje

Poskrbimo, da so vsi dejavniki, ki so pripeljali do incidenta, odstranjeni ali onesposobljeni. Ti pogosto vključujejo sistemske ranljivosti, slabe konfiguracije, neposodobljeno programsko opremo in pomanjkljivo politiko za dostop do sistemov.

Obnovitev

V koraku obnovitve se operacije v organizaciji vrnejo v običajno stanje. Sistemi so obnovljeni in postavljeni tako, da preprečujejo ponovitev incidenta. Običajno ohranimo obdobje povečanega nadzora nad sistemom, da se prepričamo o stabilnosti rešitve. Slabosti, ki so omogočile incident, preprečimo na ravni celotne organizacije, čeprav je bil prizadet le določen oddelek.

Zasledovanje

Korak zasledovanja je namenjen temu, da se iz celotnega procesa kaj naučimo. Novo znanje vgradimo v varnostni sistem organizacije. Da se na enak način ne bo pojavil novi incident, smo že zagotovili v koraku čiščenja, zdaj pa lahko nekaj časa namenimo natančnejšemu analiziranju problema in poskrbimo še za podobne primere.

Izdelati je treba poročilo o incidentu, ki je namenjeno vodstvu. Vsebovati mora natančen opis korakov, ki so bili potrebni za uspešno sklenitev posameznih faz delovanja, ter povzetek izkušenj in znanja, ki smo ga

pridobili med postopkom. Lahko vsebuje tudi opis orodij in postopkov, ki jih je uporabljal napadalec. Dokument se doda v zbirko znanja, ki je namenjena izboljšanju procesa delovanja v primeru incidenta.

9.2 Oblikovanje posebne skupine

V velikih organizacijah, kakršna so telekomunikacijska podjetja, je nujna ustanovitev posebne odzivne skupine za delovanje v primeru incidenta (angl. Computer Incident Response Team – CIRT) [**34**]. To mora biti formalna skupina, katere člani dobro poznajo sistem za upravljanje z goljufijami in varnostne mehanizme v organizaciji. Naloge in odgovornosti skupine so:

- postavitev in vzdrževanje sistema za obravnavanje izjem;
- vzdrževanje dokumentov;
- izbira orodij in tehnologije za odkrivanje izjem;
- odločitev, ali se bo neka izjema zasledovala, in določitev obsega preiskave (npr. vključitev zunanjih strokovnjakov in pomoč varnostnih institucij);
- zbiranje in analiziranje podatkov, povezanih z incidentom;
- povrnitev sistema v prvotno stanje;
- preprečitev ponovitve incidenta;
- promocija varnosti in preventivnih ukrepov v organizaciji.

Pogosto je težko pridobiti podporo vodstva za ustanovitev take skupine. Obstaja verjetnost, da je nikoli ne bomo potrebovali, prav tako pa tudi ni poceni, saj zahteva zelo usposobljen kader in specializirano opremo. Vrednost take skupine se izkaže šele takrat, kadar dejansko pride do incidenta, zato je pri odločitvi za vzpostavitev skupine pomembno razmisliti o morebitni škodi, ki bi jo organizacija utrpela, če take skupine ne bi imela. Učenje na izkušnjah glede pomembnosti omenjene skupine je lahko zelo drago.

9.3 Pomen vizualizacije

V primerjavi s prejšnjo fazo imamo tu opravka s precej manj podatki. Prikaz informacij se zato močno poenostavi. Vizualizacija v tej fazi je primerna za razvrščanje in filtriranje alarmov ter iskanje odvisnosti med atributi posameznih alarmov. Filtriranje alarmov je nujno zaradi lažnih alarmov, ki jih generira faza odkrivanja goljufij.

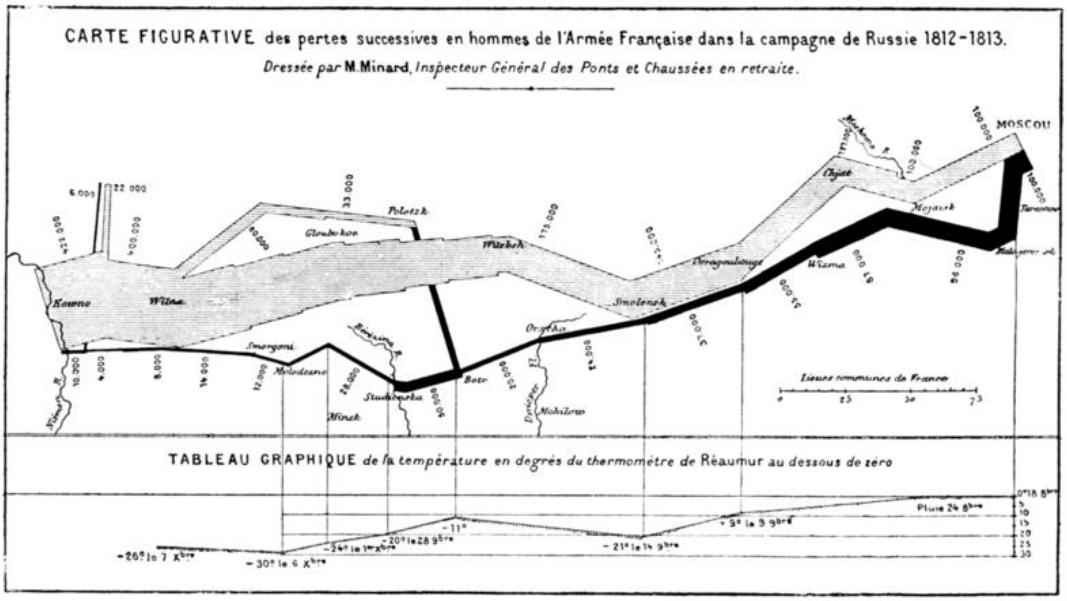
Osnovni cilj je priskrbeti dovolj informacij, da se analitik lažje odloči o tem, katera izjema zahteva prioritetno obdelavo. Sekundarna cilja sta prikaz relacij med alarmi (ali so med seboj povezani) in pomoč pri iskanju informacij o izjemi (vizualizacija transakcij in preprost dostop do podrobnosti).

10 Vizualizacija

Vizualizacija je torej lahko v pomoč v vseh fazah upravljanja z goljufijami. V prvi fazi je lahko namenjena za prikaz povratnih informacij zaščitnih elementov, v drugi kot podpora samodejnih metod in v tretji kot orodje za filtriranje alarmov.

Dodatna uporaba vizualizacije je nadzor nad delovanjem omrežja, kar pomaga pri prepoznavanju tehničnih težav (ozkih grl v sistemu, napak v strežnikih, ki niso povezane z goljufijami …) in zagotavljanju pogojev, določenih v SLA. Omenjene uporabe tukaj ne bomo zasledovali, dobro pa je vedeti, da obstaja.

Uporaba vizualizacije se ni pojavila šele z razvojem računalnikov; za pionirja na tem področju velja Charles Joseph Minard (1781–1870). Izdelal je množico zemljevidov in grafov, ki so bili v pomoč pri odločanju in načrtovanju. Ob koncu dvajsetega stoletja ga je proslavil Edward Tufte, ki je njegov grafični prikaz Napoleonovega pohoda v Moskvo[25] označil za najboljši statistični graf v zgodovini. Ta prikaz je zavidanja vreden, ker na preprost in berljiv način prikaže pet dimenzij podatkov: čas, fizično lokacijo (kje je pohod potekal), velikost vojske v času, temperaturo v času in smer gibanja vojske (Slika 2).



Slika 2: Prikaz Napoleonovega pohoda v Moskvo

[25] Napoleonov pohod v Moskvo ali *Carte figurative des pertes successives en hommes del'Armee Francais dans la campagne de Russe 1812–1813* je bil izdelan v paru s Hannibalovim pohodom iz Iberije v Italijo *Carte Figurative des pertes successives en hommes de l'arme qu'Annibal conduisit d'Espagne en Italie en traversant les Gaules*. Drugi je le redkokdaj omenjen [**72**], medtem ko prvi velja za umetnino.

Cenjenost prikaza daje slutiti, da vizualizacija velike količine večdimenzionalnih podatkov ne bo preprosto opravilo.

Da bi se približali naši problemski domeni, moramo pogledati nekoliko naprej po zgodovini. Dober približek so orodja za vizualizacijo računalniških omrežij. Nadziranje sistema z namenom vzdrževanja varnosti in zasledovanja porabe virov je bila kritična naloga administratorjev že od začetka, zato so orodja za vizualizacijo na tem področju nepogrešljiva. Gre predvsem za iskanje načinov prikaza ogromne količine podatkov in izpostavljanja podrobnosti, ki kažejo na odstopanje od običajnega vedenja. Problemska domena je zelo podobna obravnavani, s prehodom na omrežje NGN pa postaja skoraj identična. Veliko ugotovitev v tem poglavju je zato izposojenih z omenjenega področja. Drugi pomemben vir informacij so bile splošne raziskave vizualizacije velike količine podatkov. Te so bile pogosto ozko usmerjene, vendar pa lahko potegnemo vzporednice z našo problemsko domeno. Prvo ključno vprašanje, na katero želimo odgovoriti, je uporabnost vizualizacije oziroma katere so prednosti njene uporabe.

Sledi poglavje, v katerem bomo našteli prednosti uporabe vizualizacije, nato opis tipičnih problemov, na katere naletimo pri vizualizaciji, napotkov za videz predstavitve, delitev vhodnih podatkov in primerov predstavitev.

10.1 Prednosti

V [**35**] se rabi izraz vizualno rudarjenje podatkov kot ena izmed metod podatkovnega rudarjenja oziroma odkrivanja znanja v podatkih. Vizualno rudarjenje podatkov pomeni odkrivanje znanja z orodji za vizualizacijo kot komunikacijskim kanalom med analitikom in računalnikom. Tu so naštete določene prednosti vizualne predstavitve podatkov, ki veljajo tudi za našo problemsko domeno. Vizualna analiza je lahko hitrejša in prinaša boljše rezultate kot statistična analiza in strojno učenje pri:

- izjemno velikih zbirkah podatkov;
- nehomogenih podatkih;
- t. i. umazanih podatkih;
- podatkih, ki jih ne poznamo dovolj dobro;
- nenatančno določenih ciljih analize.

Druga prednost je neodvisnost od tipa storitve in goljufije. Kot vemo, so goljufije izjemno dinamične, in se hitro spreminjajo. Pri vizualizaciji to ne povzroča posebnih težav, saj opazujemo le dejansko stanje v sistemu. Če uporabljamo pravila (npr. za preusmeritev pozornosti analitika na izjemne ali nekonsistentne vrednosti), ta ne bodo specifična za določeno goljufijo, pač pa so le pravila na ravni storitve, ki jo opazujemo. Goljufija se v tem primeru ne more prilagoditi sistemu za odkrivanje (sklepanju analitika na podlagi poznavanja domene in intuicije).

Naslednja prednost vizualizacije je, da izkorišča izjemno zmožnost človeškega vida. Z vidom sprejmemo več informacij kakor z vsemi drugimi čuti skupaj [**36**]. Del možganov, namenjen analizi vizualnih

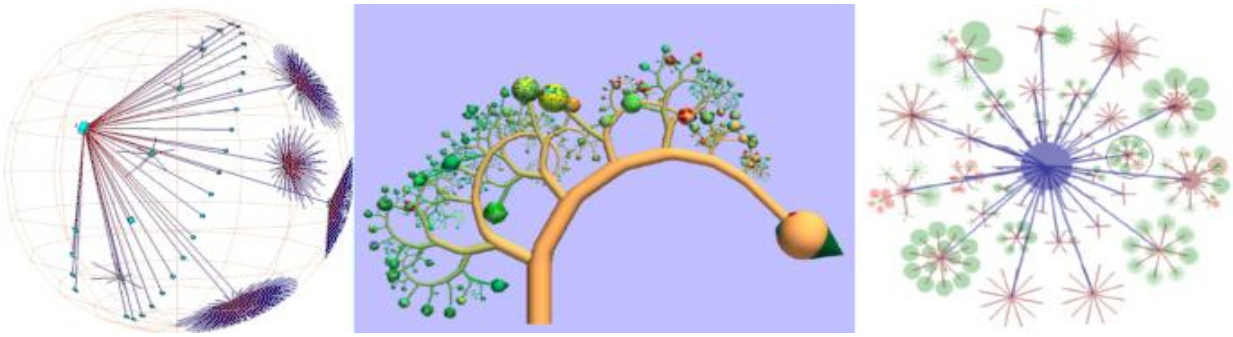
informacij, ima zmogljiv mehanizem za iskanje vzorcev. Prepozna lahko vzorce, ki bi jih zelo težko prepoznali s programsko analizo. V [**1**] je navedeno, da je človeška zmožnost razpoznavanja vzorcev izjemna in mnogo naprednejša od tehnologije za odkrivanje zanimivih vzorcev in nepravilnosti v podatkih. Seveda so za vid značilne omejitve, zato je treba poskrbeti, da razumevanje vizualizacije zahteva čim manj sposobnosti zaznavanja in ne preobremeni opazovalca, pri tem pa moramo paziti, da ne izgubimo preveč podatkov.

Omejitve vida niso edina težava, s katero se srečamo pri vizualizaciji. V naslednjem razdelku so predstavljene nekatere najpogostejše.

10.2 Težave

Viri težav pri vizualizaciji so omejitve predstavitve, analitikov in strojne opreme.

Ne glede na primernost predstavitve bo slika, ki prikazuje veliko informacij, vedno vsaj do neke mere kompleksna. Na zaslonu lahko na razumljiv način prikažemo le omejeno število informacij. Omejitev skušamo omiliti na dva načina, in sicer tako, da iščemo nove načine predstavitve (Slika 3), ki zmorejo pokazati več podatkov na sprejemljiv način, ali pa odstranimo določene podatke. Najpogosteje se je treba odločiti za oba načina.



Slika 3: Predstavitev velike količine informacij (primeri za drevesa)

Na sliki 3 je od leve proti desni Munznerjevo hiperbolično drevo (angl. Munzner's hyperbolic tree) [**37**], nato Kleinbergovo botanično drevo (angl. Kleiberg's botanical tree) [**38**] in RINGS (angl. Ringed Interactive-Navigation Graph System) [**39**].

Pri veliki količini podatkov je določena stopnja grupiranja in abstrakcije nujna, kar pa povzroči, da se pokvarita natančnost in reprezentativnost podatkov.

Kadar se odločimo za 3D-predstavitev, moramo biti še posebej pozorni, saj se lahko hitro zgodi, da tretja dimenzija prinese določeno mero dezorientacije in poveča možnosti za napačno interpretacijo. Večdimenzionalno vizualizacijo je pogosteje bolje razčleniti na več vzporednih 2D-vizualizacij [**40**]. To je še posebej očitno pri razpršenih grafih, kjer je tudi z rotacijo zelo težko dobiti dobro 3D-predstavitev. Razmeroma uspešna izvedba večdimenzijskega razpršenega grafa je v delu [**41**], kjer uporabljajo sistem zvezdnih koordinat (angl. Star Coordinates). Uporabnik tu lahko rotira pogled ter dinamično umika in dodaja dimenzije.

Naslednja težava so omejitve, ki jih prinaša analitik. Gre za fizične omejitve, kot so naslednje:

- Imamo omejen spomin.
- Hitro se utrudimo.
- Težko dalj časa ohranjamo pozornost.
- Ne maramo ponavljajočih se opravil.

Alfred Inselberg[26] (idejni oče paralelnih koordinat) je zato sestavil seznam praktičnih pravil za analiziranje slik in grafov [**42**]:

- Ne prestraši se kompleksnosti slike.
- Zastavi si jasne cilje.
- Temeljito preišči sliko.
- Preveri svoje predpostavke, predvsem tiste, ki se ti zdijo očitne.
- Ne moreš vsakič zgrešiti; ne obupaj ob prvem neuspehu.

Dobro orodje je pri tem lahko v veliko pomoč. Nekaj trikov je predstavljenih v nadaljevanju. Ne glede na orodje je tu še dejstvo, da je kader, ki je dovolj usposobljen za vizualno analizo, drag. Tako si večina podjetij ne more privoščiti, da bi analitik porabil veliko časa za ročno analizo dejavnosti v sistemu.

Še pogled iz drugega zornega kota. Ker delamo z veliko količino podatkov, se pogosto zgodi, da vizualizacijsko orodje izgubi določeno uporabnost zaradi performančne neučinkovitosti algoritmov. Klasičen način za opis transakcij med strankami so matrike. Kakršne koli operacije nad matrikami, ki imajo milijone vrstic, morajo biti izjemno dobro zasnovane, da ne povzročajo predolgih zakasnitev.

Ker opazujemo živ oziroma dejaven sistem, moramo vzpostaviti mehanizme za osveževanje stanja, ki ga vidimo na zaslonu. Osveževanje v realnem času največkrat ne bo mogoče. Še vedno pa lahko osvežujemo v določenih intervalih; uporabnik orodja tako v resnici preučuje posnetke stanja.

[26] Inselbergova spletna stran posvečena paralelnim koordinatam (http://www.math.tau.ac.il/~aiisreal/).

10.3 Videz

Na percepcijo in učinkovito razumevanje vizualizacije med drugim vplivajo naslednji dejavniki: barvna shema, vizualni moment, oblika osnovnih elementov, ločitev krajevnega omrežja in zunanjega sveta, sočasni prikaz več pogledov, osvetljenost, natančnost, okolica, kultura in izkušnje uporabnika.

Barvna shema

Barve imajo kritično vlogo v načinu človekovega dojemanja neke slike, zato je pomembno, da so v orodju za vizualizacijo skrbno izbrane. Izbira barvne sheme ni trivialna odločitev. Čeprav je bilo izvedenih veliko raziskav na to temo, še vedno ni pravil, ki bi jih vsi upoštevali. Pogosto so barvne sheme opredeljene le v okviru določene discipline [**43**].

V [**44**] so si zastavili cilj izdelati sistematično metodo, ki bo vrnila največje število barv, ki jih opazovalec še lahko hitro in natančno loči oziroma prepozna na zaslonu. Rezultat je algoritem, ki išče optimalno razdaljo treh parametrov: evklidske razdalje (barvnega modela CIELUV), linearne separacije (zmožnosti linearne ločitve barve, ki jo iščemo v določenem barvnem modelu) in kategorije barve (če barva ne pripada isti kategoriji kot druge, je njeno iskanje počasnejše – barvni model OSA). Na splošno velja, da človeško oko v povprečju razlikuje med 20 000 odtenki barv [**45**]. Omejitev za praktično uporabo je vizualni spomin in ne zmožnost razpoznave. Za branje abstraktnih informacij velja, da več kot 20 do 30 barv na zaslonu že negativno vpliva na berljivost informacij.

Pri izbrani barvni paleti je pomembno tudi, da je estetsko privlačna. Tako vizualizacijo bomo lažje analizirali. Neprivlačne palete povzročajo odpor in vplivajo na razumevanje slike. V delu [**43**] so preverili predpostavko, da so naravne barve (barvne palete, ki jo najdemo v naravi) privlačnejše in lažje berljive od barv v naključno izbranih vizualizacijah v znanstvenih člankih. Osnova za tako razmišljanje je dejstvo, da so bili človeški možgani razviti v naravi in so prilagojeni posebnim pogojem v njej. Predpostavka je bila potrjena; večina ljudi, ki so sodelovali v eksperimentu, je izbrala naravne palete pred »umetnimi«. Med drugim so ugotovili tudi, da so se barvne palete z visokim kontrastom in s sivimi odtenki uvrstile slabše. Najboljše so se odrezale barvne palete z visoko polnostjo barv (angl. saturation) in nizkim kontrastom.

Oglejmo si še primer uporabe barv v grafu. Povezava med vozlišči je obarvana z barvo, izbrano z barvne palete, ki prehaja iz rdeče v svetlo modro. Barva lahko predstavlja prehod iz dolgih klicev v kratke ali prehod iz pogostih v redke klice. Večina programskih jezikov dovoljuje uporabo barvnih modelov RGB (angl. Red, Green, Blue) in HSB (angl. Hue, Saturation, Brightness). Za prehode med barvami je primernejši drugi. Parametri prvega opisujejo barvo za računalnik, medtem ko so parametri drugega prilagojeni temu, kako človek vidi določeno barvo.

Vizualni moment

Pojem vizualni moment je izposojen iz filma in se nanaša na vpliv prehoda med prizori na miselni proces opazovalca. Če vizualnega momenta ni oziroma je šibak, mora opazovalec znova preučiti okolje in se orientirati neodvisno od znanja iz prejšnjega prizora.

Woods [**46**] opozarja na kritičnost ohranjanja vizualnega momenta pri orodjih za vizualizacijo informacij in ponuja nekaj tehnik za povečanje vizualnega momenta, na primer:

- prikaz celotne slike, pri čemer gre za povzetek, ki je namenjen za orientacijo in navigacijo po drugih podatkih; kar pomaga pri koordinaciji drugih prikazov in mora biti vedno prisoten;
- raba razpoznavnih znakov (angl. landmarks), tj. oznak, vidnih na prvi pogled, ki priskrbijo informacije o lokaciji in orientaciji;
- razdelitev na središče in okolico.

  Podatki v središču so povečani in opremljeni z dodatnimi informacijami, podatki v okolici pa so manj očitni (lahko zamegljeni) in ne vsebujejo dodatnih informacij. Središče mora biti premično, uporabnik pa ga lahko premika po celotni strukturi, ki jo opazuje.

Oblika osnovnih elementov

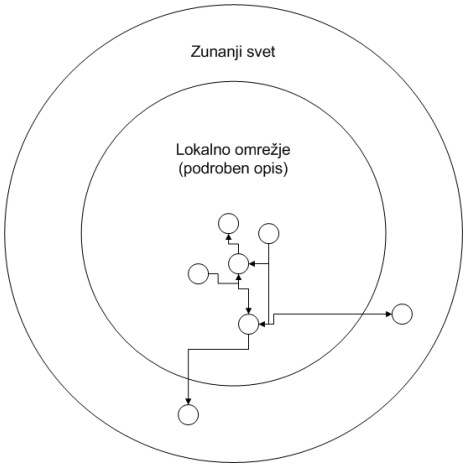
Raziskava pomembnosti vpliva oblike ikon na berljivost UML (angl. Unified Modeling Language) diagrama je potrdila, da so diagrami, katerih ikone (elementi) so sestavljene iz osnovnih 3D geometrijskih 3D-oblik,[27] bolj berljivi kot njihovi 2D-sorodniki [**47**].

Veliko raziskav potrjuje, da so človeški možgani bolje prirejeni za analizo 3D-oblik. Tudi na tem področju se lahko učimo iz narave, saj je bil naš vid prvotno razvit, da bi dobro deloval oziroma hitro razpoznaval objekte v naravnem okolju.

[27] Irving Biederman je v svoji teoriji opredelil 36 osnovnih geometrijskih 3D-oblik.

Ločitev lokalnega omrežja in zunanjega sveta

Naša naloga je odkrivati goljufije v lokalnem sistemu. Seveda pa ne moremo zanemariti dejstva, da ta ni samostojna enota. Zanimiv primer ločitve je v delu [**48**], kjer je lokalno omrežje vizualizirano znotraj kroga, zunanji svet pa v zunanji krožnici (Slika 4).



Slika 4: Ločitev zunanjega sveta

Sočasni prikaz več pogledov

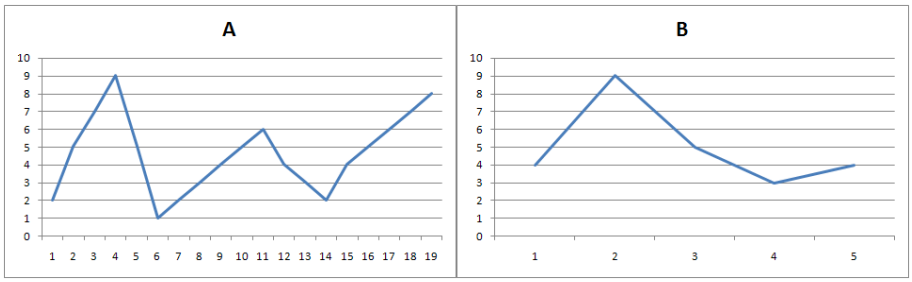
Podatke lahko vizualno predstavimo na mnogo načinov. Včasih je koristno, da uporabimo več pogledov, ki se med seboj dopolnjujejo, na enkrat. Žal je bilo na tem področju izvedenih presenetljivo malo raziskav. Odgovor na vprašanje, kdaj je primerno uporabiti več pogledov, je v delu [**49**].

Tukaj je nekaj napotkov:

Pravilo	Pomen	Ugoden vpliv na	Negativen vpliv na
Raznolikost	Uporaba različnih pogledov je smiselna, kadar obstaja raznolikost atributov, modelov, profilov ali ravni abstrakcije.	spomin	učenje zahtevano procesorsko moč prostor na zaslonu
Dopolnjevanje	Uporaba različnih pogledov je smiselna, kadar novi pogled prinaša dodatne informacije o razmerjih ali razlikah med določenimi atributi v pogledu.	spomin primerjavo preklapljanje konteksta	učenje zahtevano procesorsko moč prostor na zaslonu
Dekompozicija	Delitev kompleksnih pogledov na več bolj obvladljivih delov.	spomin primerjavo	učenje zahtevano procesorsko moč prostor na zaslonu
Previdnost	Previdnost je nujna pri odločitvi za dodaten pogled, ki zahteva večjo zbranost uporabnika in zaseda prostor na zaslonu.	učenje zahtevano procesorsko moč prostor na zaslonu	spomin primerjavo preklapljanje konteksta
Časovne in prostorske omejitve	Uravnotežiti je treba prostorsko in časovno ceno ter prednosti za prikaz več pogledov. V dlančniku bo prostorska cena zelo visoka, zato lahko več pogledov pokažemo sekvenčno. V tem primeru bomo izgubili nekaj več časa.	primerjavo zahtevano procesorsko moč prostor na zaslonu	
Dodatni ključi	Uporaba dodatnih ključev, ki opozarjajo na povezavo med pogledi. Primer so označevanje in poravnava pogledov.	učenje primerjavo	zahtevano procesorsko moč
Konsistentnost	Pogledi naj imajo konsistenten uporabniški vmesnik, videz in stanja.	učenje primerjavo	zahtevano procesorsko moč
Prenos pozornosti	Uporaba ključev, ki so uporabniku v pomoč, da se lahko osredini na pomembnejše dogodke. Med njimi so na primer animacije, zvočni signali, povzetki in premiki.	spomin preklapljanje konteksta	zahtevano procesorsko moč

Orodje, ki omogoča več pogledov, vpliva na večjo učinkovitost uporabnikov, saj poenostavi odkrivanje vzorcev v podatkih in razmerij med atributi. Slabosti takega pristopa pa so kompleksnejši dizajn orodja (sinhronizacija pogledov), počasnejše učenje uporabnikov in večja obremenitev delavnega spomina.

Tufte [**45**] priporoča, da se pogledi, ki so med seboj odvisni, prikažejo na zaslonu v serijah. Na sliki 5 tako grafa A in B postavimo vzporedno. Ker imata enako os Y, se berljivost ne zmanjša.



Slika 5: Prikaz v serijah

Nadgradnja prikaza, kot ga vidimo na zgornji sliki (Slika 5), je uporaba matrik. Vsako polje vsebuje pogled, ki je v razmerju s horizontalnimi in z vertikalnimi sosedi.

Na splošno velja, da tako pridobljene dodatne informacije ne povečajo zapletenosti branja.

10.4 Vhodni podatki

Vhodni podatki se razlikujejo od faze, v kateri uporabljamo vizualizacijo. Za vizualizacijo v fazi preprečevanja goljufij potrebujemo podatke z zaščitnih elementov, v fazi odkrivanja goljufij pa podatke o naročnikih in transakcijah. Vhodni podatki za vizualizacijo v fazi obravnavanja izjem so podatki o naročnikih in transakcijah, obogateni z ugotovitvami iz faze odkrivanja goljufij, torej verjetnost, kritičnost in opis goljufije.

Določena raven grupiranja, standardizacije in abstrakcije vhodnih podatkov je nujna, razlogi zanjo pa so naslednji:

- Želimo imeti orodje, ki bo neodvisno od opazovane storitve.
- Analitikom pogosto pomagajo zunanji svetovalci in varnosti strokovnjaki, ki ne potrebujejo dejanskih informacij o okolju, kjer smo zbrali podatke. Podobno tudi operaterji nočejo razkriti več informacij, kot je nujno potrebno.
- Omrežja so zapletena, zato vizualizacije brez poenostavitve postanejo neobvladljive.

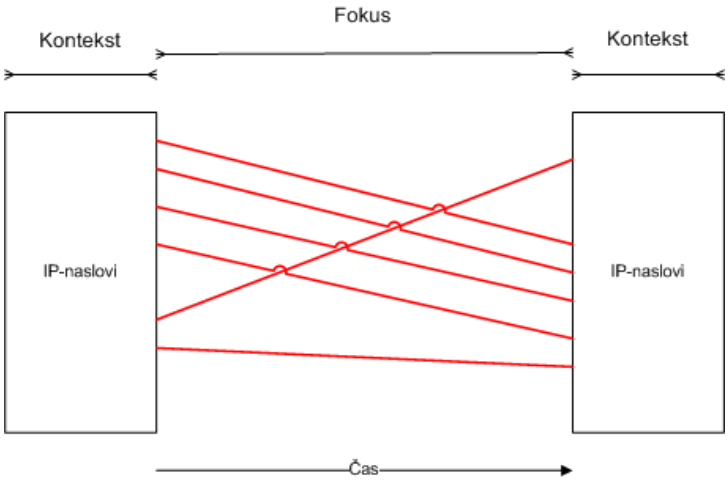
Seveda pa v večini primerov to ne pomeni, da podrobnosti ne smejo biti dosegljive na zahtevo.

10.5 Primeri predstavitev

Na voljo je veliko grafičnih predstavitev, ki jih lahko uporabimo za analizo podatkov. Začnemo lahko s preprostimi stolpičastimi in z razpršenimi 2D-grafi in nadaljujemo z zapletenejšimi 3D-predstavitvami (veliko primerov 3D-grafov je v delu [**50**]; uporabljeni so v orodju VisualMine). V nadaljevanju je nekaj najzanimivejših predstavitev, ki so primerne za problemsko domeno v magistrski nalogi.

Pristop fokus + kontekst

Pristop fokus + kontekst, uporabljen v orodju TVN (angl. Time-based Network traffic Visualizer), [**51**], lahko uporabimo tudi v tej problemski domeni. Na levi in desni strani sta območji, ki podajata kontekst, na sredini pa je območje fokusa. V TVN so v kontekstu IP-naslovi vira in cilja, v fokusu pa so transakcije med naslovi (Slika 6).



Slika 6: Primer predstavitve fokus + kontekst

Podobno kontekst v tem primeru vsebuje identifikacijo vira in cilja (telefonsko številko ali ID uporabnika v omrežju NGN). Ko pride do transakcije, se v območju fokusa vzpostavi povezava med udeleženci. Območje se spreminja s časom in je razširljivo. Povezava je predstavljena s tanko črto, ki se med izvajanjem transakcije odebeli. Območje fokusa lahko predstavi le določen časovni interval. Če v

celotnem intervalu ni prišlo do transakcije na določeni povezavi, se ta izbriše. V fazi obravnavanja izjem se pri sumljivih transakcijah odebeljeni del, ki predstavlja transakcijo, obarva drugače kot regularne transakcije. Uporabimo lahko barvno lestvico od svetlo modre do rdeče. S povečevanjem resnosti in verjetnosti goljufije se premikamo proti rdečemu koncu lestvice.

Dodatni možnosti v takem pogledu sta zamrznitev časa in pregled zgodovine. Taka predstavitev je uporabna za odkrivanje vzorcev, odvisnih od časa nastanka, trajanja in identitete vpletenih uporabnikov.

Predstavitev transakcij z grafom

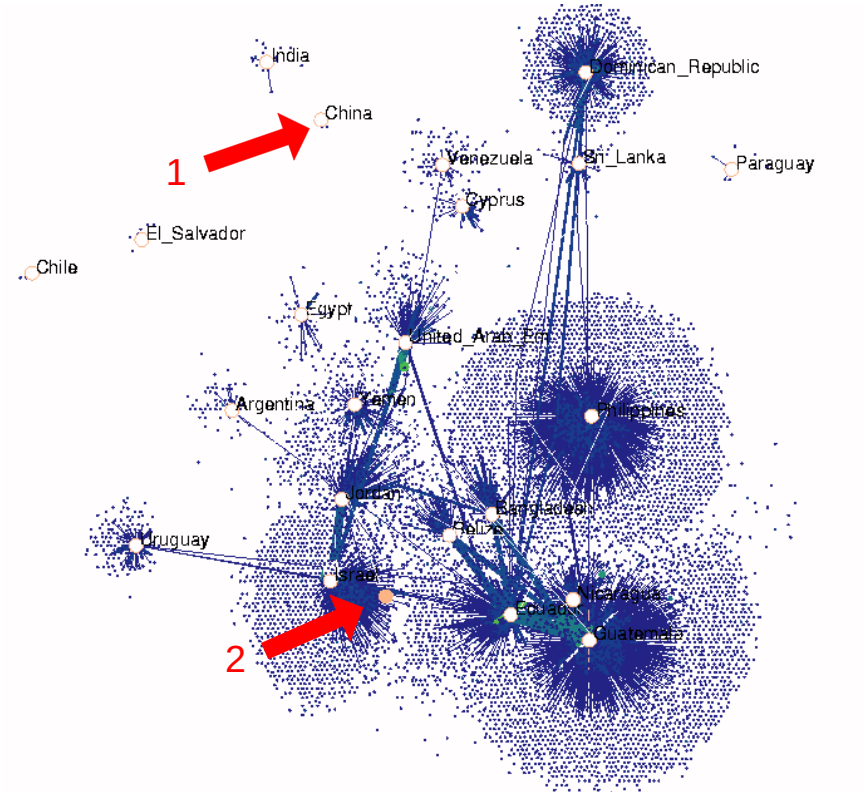
Vozlišče v grafu predstavlja stranko, povezava med vozlišči pa pomeni, da je vsaj enkrat (v intervalu, ki ga določi uporabnik orodja) prišlo do transakcije med strankama. Velikost vozlišča oziroma debelina povezave ter njuna barva predstavljata atribute, ki jih izbere uporabnik orodja. Velikost vozlišča na primer lahko predstavlja povprečno ceno transakcij, ki jih stranka izvede v enem dnevu, barva pa pove, ali obstaja sum, da je stranka vpletena v goljufijo, in ali je to verjetno. Podobno debelina povezave lahko prikaže povprečno ceno transakcije, barva pa, ali obstaja sum goljufije.

Dodatno dimenzijo lahko predstavimo še z dolžino povezave med vozliščema. Razdalja na primer lahko predstavlja število transakcij med strankama. Vozlišči, med katerima je veliko transakcij, sta bližje.

Če storitev omogoča določitev fizične lokacije stranke (v stacionarni in mobilni telefoniji), lahko to uporabimo pri vizualizaciji. Zaradi velike količine podatkov prikaz postane nekoliko nepregleden, a še vedno koristen, kadar vemo, kaj iščemo, kar je uporabno za preprečevanje goljufij ob sklenitvi pogodbe oziroma identifikacijo območij z visoko stopnjo tveganja za goljufije. Če oseba, ki namerava skleniti naročnino, poda svoj pravi naslov, lahko hitro ugotovimo, ali je že prišlo do kakih goljufij na tem naslovu oziroma v bližnji okolici.

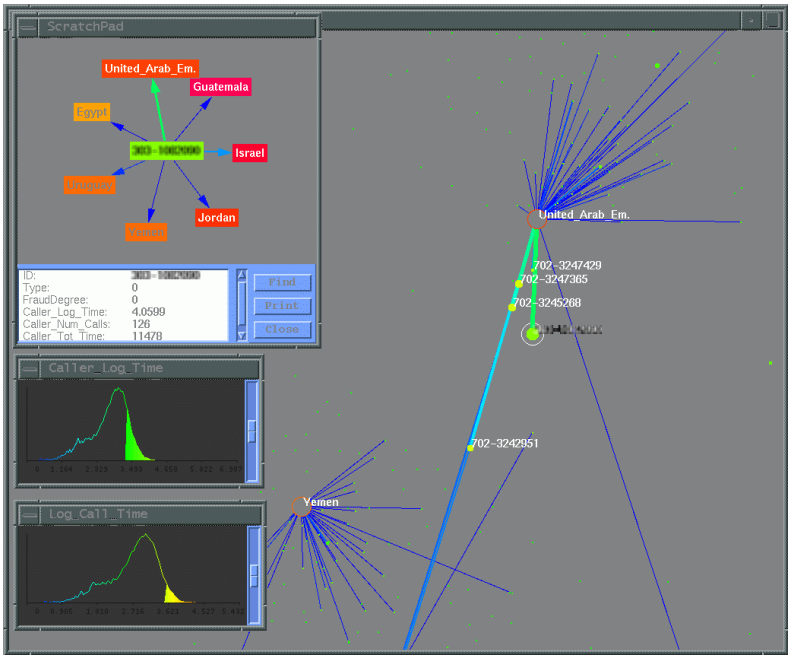
Naslednji primer uporabe zasledimo v storitvah mobilne telefonije, pri čemer lahko ugotovimo, kdaj je prišlo do dveh klicev istega naročnika z oddaljenih lokacij v kratkem času.

Primer povezave fizične lokacije in klicev je v delu [**1**]. Slika 7 prikazuje vse mednarodne klice v zadnjih osmih urah. Prazna vozlišča predstavljajo države (Slika 7, oznaka 1), polna vozlišča so naročniki in povezave klici med naročniki. Velikost in barva vozlišča predstavljata število klicev, ki jih je opravil uporabnik. Če je število visoko, je vozlišče večje in obarvano svetleje (Slika 7, oznaka 2).



Slika 7: Primer predstavitve fizične lokacije klicev – glavni pogled

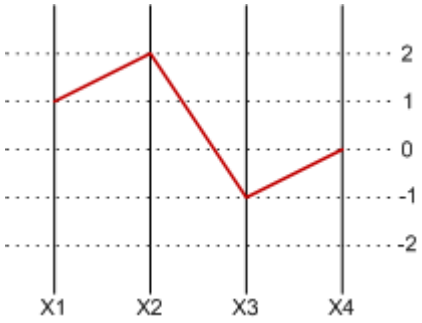
Izbrano vozlišče si lahko ogledamo v podrobnejšem pogledu (Slika 8), kjer se prikažejo le klici izbranega uporabnika. Primer, ki ga vidimo na sliki 8, se je pozneje izkazal za prevaro. Goljuf je v osmih urah opravil 126 mednarodnih klicev.



Slika 8: Primer predstavitve fizične lokacije klicev – podroben pogled

Paralelne koordinate

Za vizualizacijo podatkov, ki imajo več parametrov, ni na voljo veliko uporabnih pristopov. Eden izmed boljših je predstavitev s paralelnimi koordinatami. Navaden 2D-prostor razdelimo na več vzporednih pasov. Vsaka vertikalna os predstavlja svojo dimenzijo. Na naslednji sliki (Slika 9) vidimo primer za štiri dimenzije (X1, X2, X3, X4) z vrednostmi X1 = 1, X2 = 2, X3 = –1 in X4 = 0.



Slika 9: Primer predstavitve paralelne koordinate

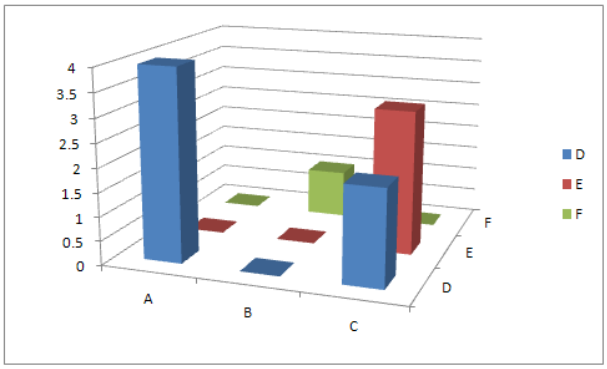
V naši domeni je tak prikaz primeren za vizualizacijo transakcij. Za klic na primer uporabimo dimenzije, kot so trajanje, cena, tip, vir in cilj. Zaradi števila klicev tak prikaz kmalu postane neberljiv, zato si pomagamo s filtriranjem posameznih dimenzij.

Filtriranje lahko omogočimo tudi tako, da transakcije, ki niso bile izbrane, ne izginejo, pač pa se samo zasenčijo. Tako ohranjanje konteksta včasih pomaga odkriti skrite vzorce in zveze med parametri.

Časovno dimenzijo lahko predstavimo z barvami. Na začetku se transakcija obarva rdeče in se s časom ohlaja, preide v svetlo modro barvo.

Stolpičasti graf

Med najpogostejše metode za prikaz preprostih podatkov spadajo stolpičasti grafi. Za manjšo množico večdimenzionalnih podatkov lahko uporabimo stolpičaste 3D-grafe (Slika 10), ki so primerni za predstavitev alarmov. Pri večji množici se pojavi problem prekrivanja podatkov, ki ga do določene mere ublažimo z rotacijo pogleda.



Slika 10: Primer predstavitve s stolpičastim grafom

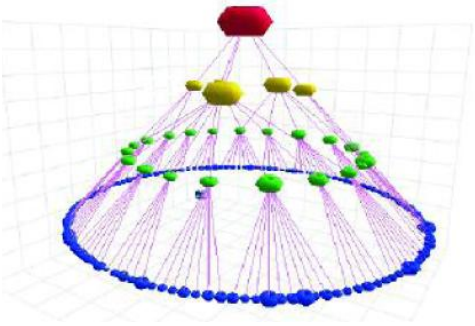
Za osi x in y izberemo vir in cilj transakcije, višina in barva stolpca pa sta atributa, ki ju izbere uporabnik orodja (višina je na primer verjetnost goljufije in barva kritičnost).

Če želimo ujeti časovno dimenzijo, lahko žrtvujemo os y za čas in prikažemo dva vzporedna grafa. V prvem je os x namenjena viru in v drugem cilju.

Pomembno je, da so taki prikazi dovolj dinamični. Omogočati morajo premikanje stolpcev in pogleda, razvrščanje stolpcev, spreminjanje parametrov in podobno.

Stožčasti graf

Stožčasti graf je primeren za prikaz hierarhij (Slika 11). Stožec razdelimo na več nivojev, na katere postavimo vozlišča [**52**].

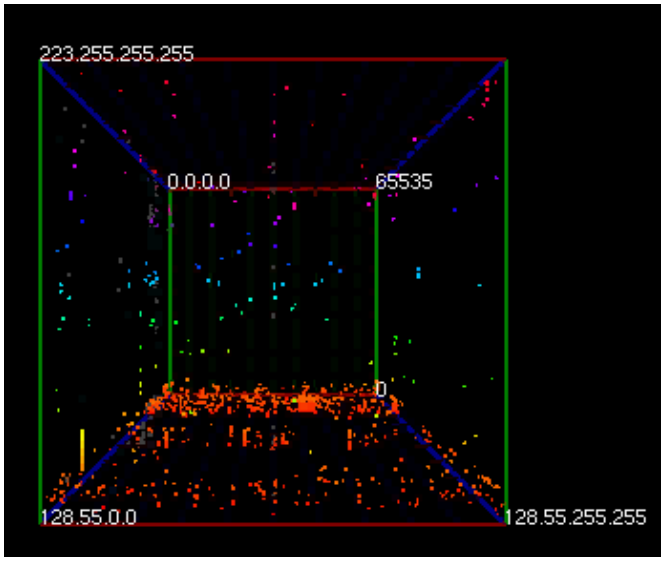


Slika 11: Primer predstavitve s stožčastim grafom

Tak graf lahko uporabimo za preučevanje socialne mreže stranke, ki je osumljena goljufije. Če želimo videti, kako se graf spreminja s časom, lahko dodamo še drsno okno, animacijo ali pa dodaten pogled, ki omogoča prehajanje po času.

Vrteča kocka morebitnih nevarnosti

Vrteča kocka morebitnih nevarnosti (angl. The Spinning Cube of Potential Doom) je bila razvita za opazovanje prometa TCP (angl. Transmission Control Protocol) v omrežju [**53**]. Os x predstavlja naslove v mreži, os y pa vse mogoče naslove, ki generirajo promet. Os Z predstavlja vrata. Vsaka TCP-povezava se prikaže kot točka v 3D-prostoru. Barve točk predstavljajo tip in stanje povezave. Okolje omogoča vrtenje kocke, kar poenostavi iskanje vzorcev (Slika 12).



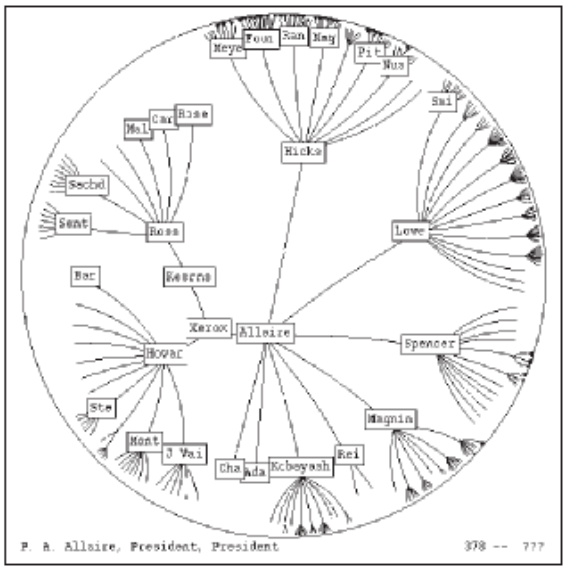
Slika 12: Primer predstavitve z vrtečo kocko

Gre torej za 3D-različico razpršenega prikaza, primernega za odkrivanje razmerij med atributi ter iskanje gruč in zunanjih točk.

Hiperbolični graf

Hiperbolični graf [**36**] [**54**] je primer uporabe principa leč ribjega očesa.[28] Delček podatkov je v fokusu, drugi pa so pomanjšani. Ta možnost je uporabna za prikaz velike količine podatkov (Slika 13).

[28] Leče ribjega očesa (angl. fish eye lenses) povečajo središče oziroma točko, ki nas zanima [**71**]. Povečava pada z razdaljo od središča.



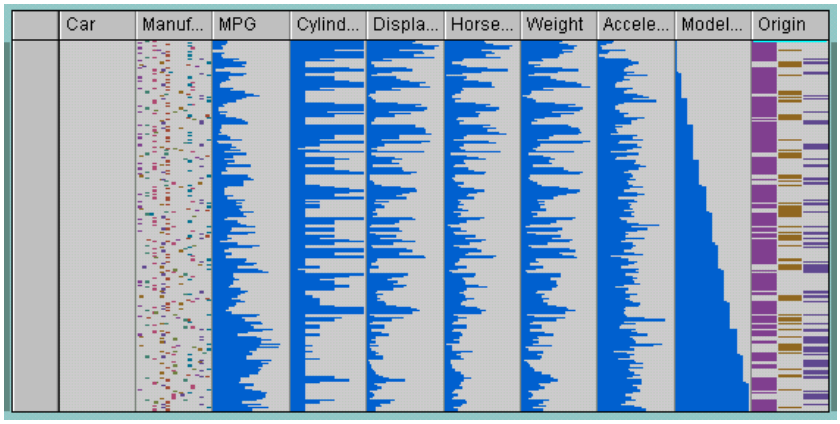
Slika 13: Primer predstavitve s hiperboličnim grafom

V našem primeru velja, da so vozlišča stranke in povezave med njimi transakcije. Velikost in barva vozlišča predstavljata poljubne parametre, ki jih izbere uporabnik. Velikost na primer predstavlja porabljena sredstva, barva pa zanesljivost stranke (ali redno plačuje račune, je nova stranka, ali je bila kdaj vpletena v goljufijo …).

Tak prikaz uporabimo v fazi obravnavanja izjem za preučevanje socialne mreže stranke, ki je osumljena goljufije.

Uporaba tabel

Orodje Evreka (prej znano kot Table Lens) [**55**] omogoča uporabo tabel za prikaz večdimenzionalnih podatkov. Vrstica predstavlja posamezni objekt in stolpci dimenzije. Numerične vrednosti so prikazane z dolžino obarvanega dela določenega polja (traku od leve proti desni), diskretne in nominalne vrednosti pa z barvanjem in delitvijo polja na n enakih delov (Slika 14).



Slika 14: Primer predstavitve s tabelo

Iskanje vzorcev in odvisnosti poteka predvsem z razvrščanjem atributov in s filtriranjem podatkov.

10.6 Model aplikacije

Do zdaj smo spoznali delovanje sistema za upravljanje z goljufijami in ugotovili, kje je lahko vizualizacija v pomoč, ter kako prikazati velike količine večdimenzionalnih podatkov. Imamo torej dovolj znanja, da poskusimo izdelati model aplikacije za vizualno analizo podatkov.

Kateri so najpomembnejši gradniki, pove tudi znana »mantra« iskanja informacij na podlagi vizualizacije, ki se glasi: najprej pregled, povečava in filtriranje, nato podrobnosti na zahtevo [**56**].

Lastnosti dobrega orodja za vizualizacijo so predstavljene v nadaljevanju.

- Razširljivost
  Dodajanje novih načinov vizualizacije mora biti preprosto, na primer predstavitev s paralelnimi koordinatami (glejte razdelek 10.5 Primeri predstavitev; paralelne koordinate) se doda kot nov programski modul.
- Pregled
  Okno uporabniku omogoča pregled nad vsemi podatki. V [**51**] na primer zasledimo podatek, da se analitiki pogosto pritožujejo nad orodji, ki izgubijo pregled nad celoto pri delu s podrobnostmi. Pregled, ki vzdržuje kontekst, mora biti vedno na voljo.
- Interakcija
  Orodje mora omogočati interakcijo med podatki in uporabnikom. Interakcija naj vsebuje:
  - povečavo (priporočeno je dinamično povečevanje in manjšanje natančnosti vseh pogledov; poleg okna za pregled mora biti na voljo okno za natančnejši pogled na izbrano množico podatkov, ločeno okno za nenatančen pregled pa je nujno zaradi ohranitve konteksta; v delu [**30**] je bila

uporabljena povečava prek treh nivojev ali različnih pogledov, ki prikazujejo vedno podrobnejše podatke);

- filtriranje (ker pogosto ne želimo videti vseh podatkov, mora biti za boljšo berljivost omogočeno dinamično filtriranje podatkov, ki so prikazani na zaslonu; v [**57**] je predstavljen primer, kako se filtriranje doseže s preprostim poizvedbenim jezikom; pri filtriranju so lahko v pomoč tudi metode za identifikacijo odvisnosti med posameznimi parametri; eleganten način filtriranja pa je na voljo v orodju VisDB [**58**], kjer se vrednosti spremenljivk poizvedbe nastavljajo z drsnimi gumbi (angl. slider); ni pa nujno, da vedno skrijemo podatke, ki jih uporabnik ne želi videti – lahko jih samo zasenčimo oziroma povečamo njihovo transparentnost; prednost tega je, da ohranimo kontekst, kar poveča možnost, da odkrijemo skrite vzorce in odvisnosti med parametri, po drugi strani pa se zmanjša berljivost oziroma povečuje kompleksnost slike).

- Prikaz relacije
  Značilna grafična predstavitev vsebuje elemente in relacije med njimi. Pomembno je, da so relacije jasno vidne. Predstavitev relacij s črtami je zelo učinkovit način, saj so v vidnem središču (vidni skorji) v možganih posebni mehanizmi za njihovo hitro razpoznavanje [**36**].
- Zgodovina
  Orodje mora omogočati vzdrževanje zgodovine opravil, ki jih je uporabnik izvedel glede podatkov. To omogoča preklic opravil, njihovo ponovitev na osveženih podatkih, prav tako pa skrbi za to, da ne pozabimo, kako smo prišli do rezultatov, in podobno.
- Podrobnosti
  Podrobnosti ne želimo videti v glavnem pogledu, vendar pa morajo biti dosegljive na zahtevo. Dvojni klik elementa v grafu na primer prikliče okno s podrobnostmi, ki morajo biti hitro dosegljive. Na najnižji ravni lahko celo prikažemo dejanske dnevnike s kritičnih elementov omrežja.
- Izbira in osvežitev (angl. brushing and linking)
  Pojem brushing se nanaša na interakcijo med uporabnikom in računalnikom, rezultat pa je neko opravilo v zvezi s podatki. Linking pa pomeni, da se to opravilo odraža v vseh odprtih oknih (vizualnih pogledih). To seveda velja le, kadar so mogoči različni vizualni pogledi nad istimi podatki. Spremembe v enem pogledu se morajo takoj odražati tudi v drugih. Dobro pa je, da je tranzicija vidna – da uporabnik ve, zakaj in kako je prišlo do novega stanja.
- Referenčni model
  Če je le mogoče, mora orodje omogočati izdelavo posnetka običajnega stanja, ki ga nato lahko primerjamo s trenutnim stanjem.

Glavna lastnost, ki jo želimo zagotoviti med načrtovanjem take aplikacije, je, da omogoča preprosto dodajanje modulov, ki implementirajo določen grafični prikaz. Zahteva po različnih grafičnih prikazih izhaja iz razmišljanja, da ni na voljo en sam grafični prikaz, ki bi zadovoljil vse zahteve analitikov in bi bil primeren za vse storitve. Preprosto dodajanje novih modulov pa je nujno za hitro uresničevanje idej oziroma zahtev analitikov in preprosto nadgradnjo aplikacije.

Moduli morajo zadovoljiti vsaj naslednje pogoje:

- Vsak novi prikaz nadgradi (deduje) osnovni razred, ki vsebuje temeljne procedure za prikaz podatkov.
- Struktura vhodnih in izhodnih podatkov (o transakcijah, strankah …) je standardizirana.
- Omogočajo filtriranje in urejanje podatkov, in to tako vizualno (na primer s premikanjem in z razvrščanjem stolpcev v tabeli in brisanjem vozlišč v grafu) kot tudi s poizvedbami.

Kot primer glavnega oziroma začetnega pogleda aplikacije za odkrivanje goljufij uporabimo tabele, kjer so vrednosti posameznih atributov predstavljene z barvnimi trakovi (Slika 15).[29] Na sliki vidimo model in označene glavne značilnosti aplikacije:

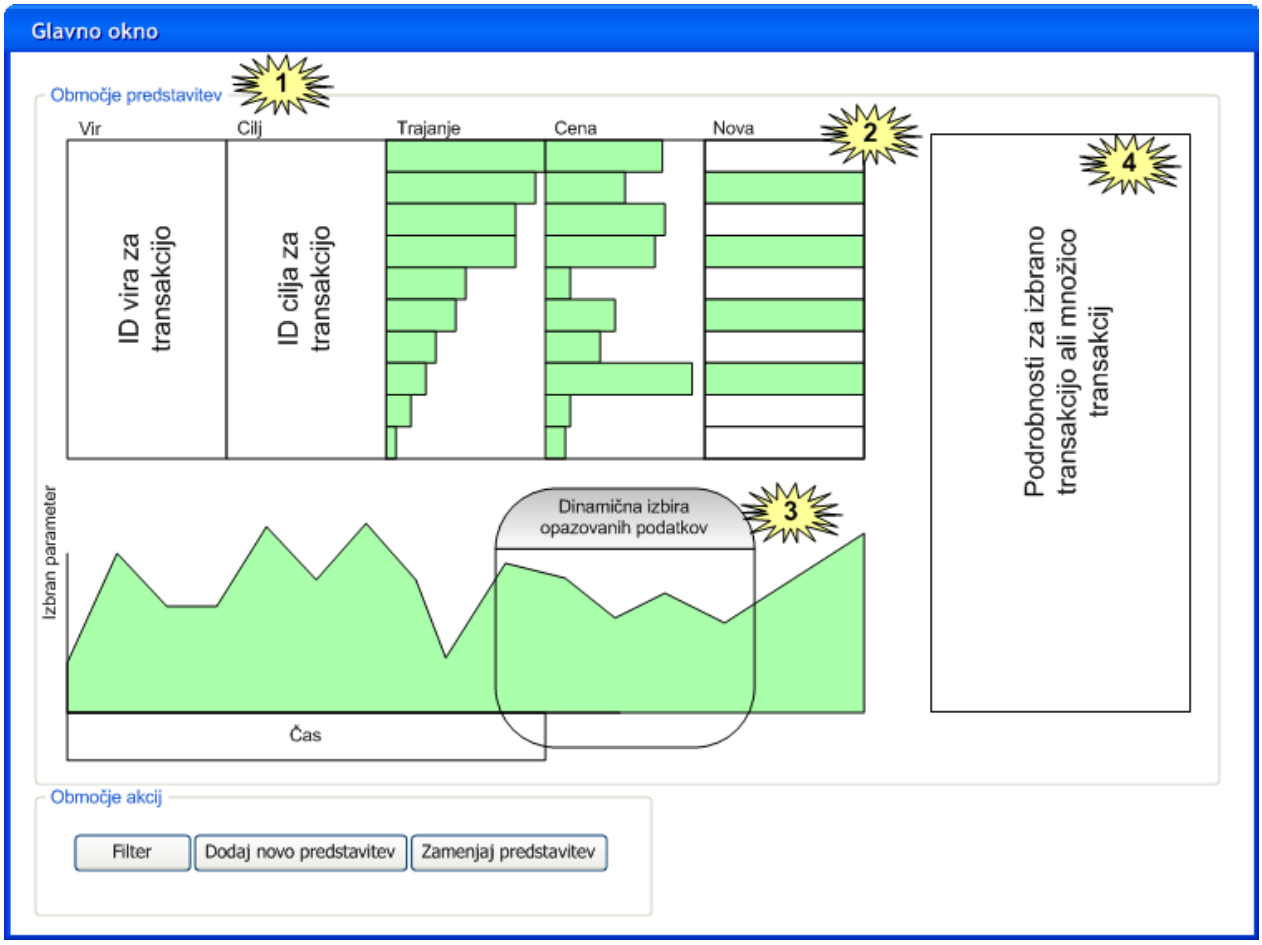
1. Glavno okno je razdeljeno na območje predstavitve in območje opravil. Območje predstavitve je specifično za posamezno predstavitev oziroma pogled. Območje opravil je skupno za vse predstavitve. Omogoča dostop do opravil, kot so filtriranje, spreminjanje in odpiranje novih predstavitev.

2. Predstavitev ne sme biti statična, pač pa dinamična slika, ki jo uporabnik lahko priredi po svoje. V našem primeru dodamo lastnosti, kot so dodajanje atributov (stolpcev) in njihovo premikanje ter razvrščanje in grupiranje po določenih atributih.

3. Želeno je, da je uporabniku omogočeno vizualno filtriranje podatkov. Primer je uporaba premičnega in raztegljivega časovnega okna.

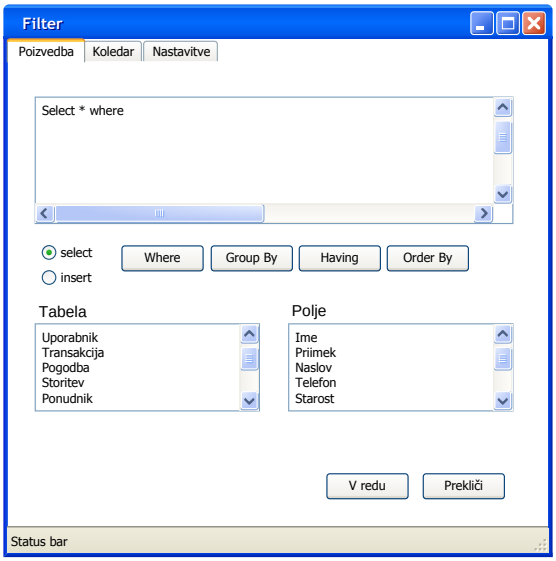
4. Tudi na višji ravni so smiselni povzetki izbranih transakcij, tj. podrobnosti, kot so trajanje, cena, število transakcij in podobno. Podrobnosti se osvežijo, kadar se spremeni množica izbranih podatkov (na primer dvojni klik uporabnika in premik časovnega okna).

[29] Slike za prikaz modela aplikacije so izdelane v orodju Microsoft Office Visio 2007.



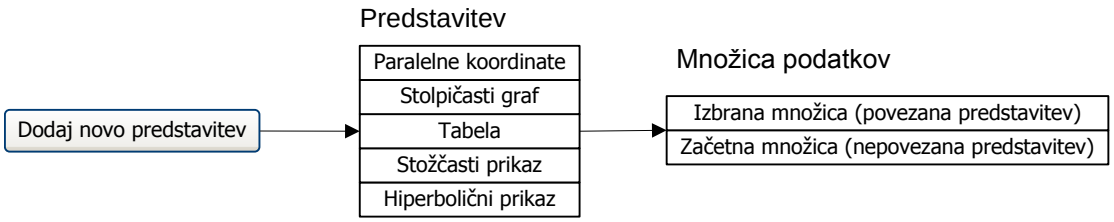
Slika 15: Odkrivanje goljufij – glavno okno

Gumb Filter (območje opravil) odpre okno, v katerem določimo omejitve nad množico podatkov (Slika 16). Uporabimo na primer preproste poizvedbe s strukturiranim povpraševalnim jezikom (angl. Structured Query Language – SQL), ki omogoča filtriranje podatkov in dinamično prirejanje atributov. Kot pri predstavitvah mora biti tudi dodajanje novih filtrov preprosto. Če govorimo o večji organizaciji, je dobro izdelati programski vmesnik (angl. Application Programming Interface – API) za dodajanje novih modulov. Dodamo na primer novi modul za koledar, ki omogoča vizualno časovno filtriranje. Vsak modul je dostopen v ločenem zavihku. Filtri imajo tudi skupne nastavitve (zavihek nastavitve), s katerimi na primer določimo, ali naj se podatki, ki niso izbrani, samo zasenčijo ali se izbrišejo.



Slika 16: Filter

Gumb Dodaj novo predstavitev odpre novo okno z izbrano predstavitvijo. Za vhodne podatke v novo predstavitev lahko uporabimo začetno množico podatkov ali pa le trenutno izbrano podmnožico (Slika 17).

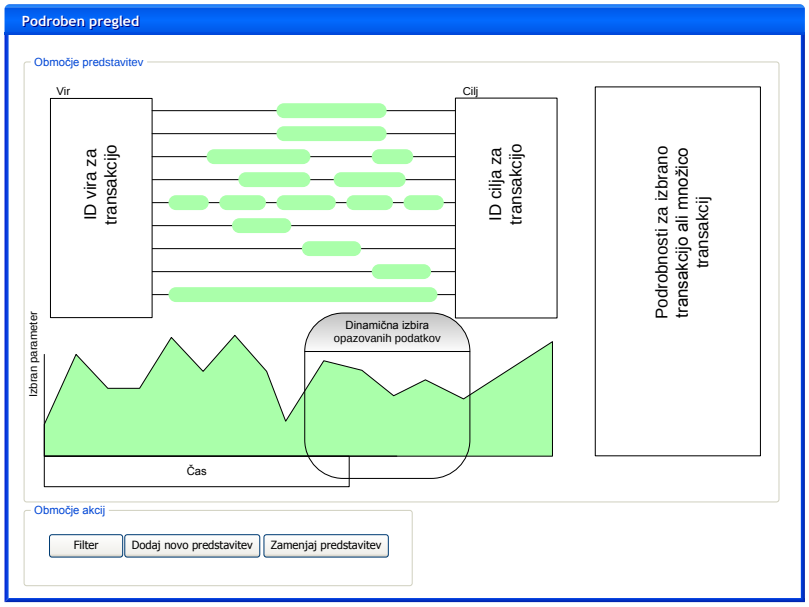


Slika 17: Dodaj novo predstavitev

Izbira slednje pomeni, da se spremembe v prvi predstavitvi odražajo tudi v drugi. V nasprotnem primeru to ne velja, predstavitvi pa sta ločeni. Sprememba množice podatkov je dobrodošla za natančnejšo obdelavo manjše množice.

Gumb Zamenjaj predstavitev le zamenja trenutno predstavitev z novo. Uporabi se ista množica podatkov, filtri pa se ohranijo.

Za manjšo množico podatkov so primerni pogledi, kot je fokus + kontekst prikaza, ki omogoča natančnejšo analizo podatkov (Slika 18). Kot vidimo, je struktura okna identična glavnemu oknu, le predstavitev se zamenja.



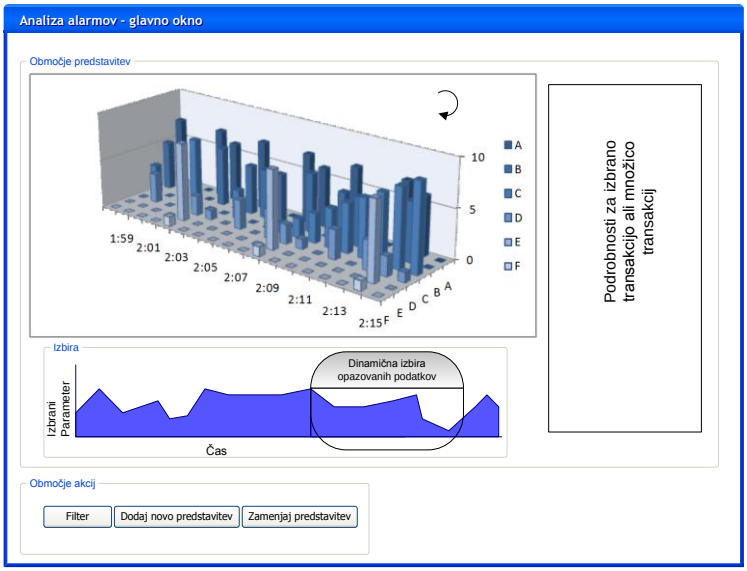
Slika 18: Odkrivanje goljufij – podroben pogled

Interakcijo s podatki v takem pogledu izvedemo z razširljivim »fokusom« območja, premikanja vrstic (transakcij), spreminjanja barve za PRN-klice in podobno.

To je le ena izmed možnosti, uporabnik pa lahko za natančnejšo analizo izbere katerikoli graf, ki ga orodje omogoča. Istočasno je lahko odprtih več med seboj povezanih oken z različnimi predstavitvami, kar prispeva k hitrejšemu odkrivanju vzorcev.

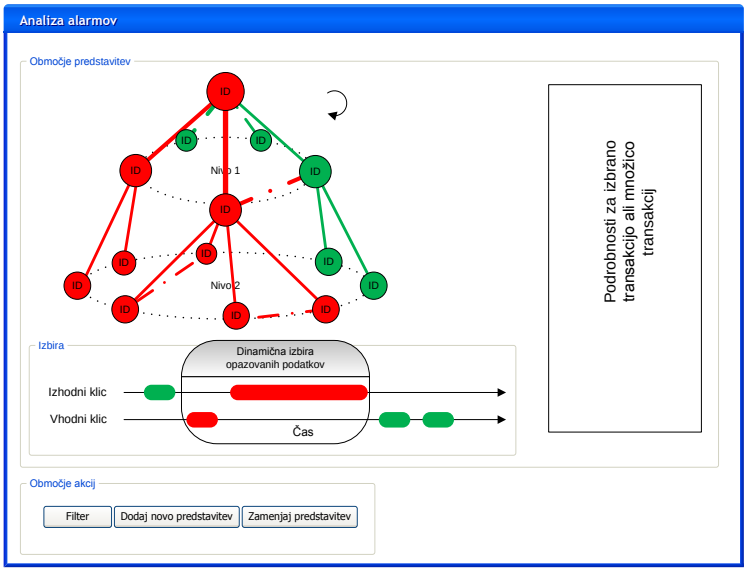
V fazi obravnavanja izjem uporabimo poglede, ki so bolj prilagojeni analizi manjše količine podatkov – alarmov. Slika 19 prikazuje glavni pogled za analizo alarmov, slika 20 pa podrobnejšega.

V glavnem pogledu uporabimo stolpičasti graf. Višina stolpca je kritičnost alarma, os x je čas, os y pa predstavlja vir alarma. Uporabniku, tako kot vedno, omogočimo spremembo teh lastnosti. Uporabi se lahko tudi barva, vendar je treba paziti, da se pri tem ne zmanjša berljivost grafa. Uporabnik tako lahko v realnem času opazuje, kako prihajajo novi alarmi. Poleg vrtenja celotnega grafa je zaželeno tudi dinamično premikanje vrstic, na primer vir A na osi y zamenja mesto z virom B.



Slika 19: Analiza alarmov – glavno okno

Za podrobnejšo analizo tukaj uporabimo stožčasti prikaz. Rdeče obarvana vozlišča predstavljajo stranke, ki so osumljene zlorabe. Vzorce goljufij odkrivamo na podlagi sosedov in lastnosti klicev.



Slika 20: Analiza alarmov – podroben pogled

10.7 Implementacija

Pri implementaciji takega orodja si lahko pomagamo z obstoječimi programskimi vmesniki, jeziki in orodji. Za primere, ki so navedeni v nadaljevanju, smo uporabili:

- Processing [**59**], odprtokodni programski jezik in razvojno okolje, namenjeno razvoju prototipnih aplikacij za delo z grafičnimi prikazi, animacijami in interakcijo;
- Parvis [**60**], orodje za prikaz paralelnih koordinat, ki omogoča vizualizacijo in interakcijo z večdimenzionalnimi podatki, predstavljenimi s paralelnimi koordinatami;
- R [**61**], programski jezik in razvojno okolje, namenjeno statistični obdelavi in grafični predstavitvi podatkov.

Zanimive pa so tudi naslednje rešitve:

- JUNG (angl. Java Universal Network/Graph) [**62**] [**63**], programski vmesnik za modeliranje, analizo in vizualizacijo podatkov, predstavljenih z grafom in mrežo;
- Xmdv [**64**], orodje za interaktivni prikaz večdimenzionalnih podatkov.

Pri razvoju primerov smo upoštevali navodila iz dela [**65**], kjer je opisan proces izdelave orodja za vizualizacijo podatkov. Proces predpisuje upoštevanje naslednjih korakov:

- Zajem (angl. acquire). V tem koraku pridobimo »surove« podatke. V našem primeru se ta korak razlikuje glede na fazo, v kateri smo. Pridobimo jih na primer iz prejšnje faze, posredovalnega sistema ali sistema za zaračunavanje.
- Strukturiranje (angl. parse). Podatke, zbrane iz različnih virov, strukturiramo in kategoriziramo. Najmanjša enota, ki jo prikazuje naša aplikacija, bo posamezni klic. Podatke strukturiramo temu primerno.
- Filtriranje (angl. filter). Odstranimo vse podatke, ki jih ne potrebujemo.
- Obdelava (angl. mine). Podatke obdelamo z matematičnimi metodami (z rudarjenjem podatkov, s statistično obdelavo …). Za našo aplikacijo je primerna predvsem statistična obdelava.
- Predstavitev (angl. represent). Izberemo predstavitev za podatke in implementiramo osnovno različico. Narišemo na primer graf, v katerem vozlišča predstavljajo uporabnike in povezave klice med njimi.
- Prečiščena predstavitev (angl. refine). Izboljšamo osnovno predstavitev za nazornejši in za uporabnika prijaznejši prikaz podatkov. Graf na primer posodobimo tako, da velikost vozlišča prikazuje število klicev in dolžina povezave število klicev med vozlišči. Čim več je klicev med vozlišči, tem manjša je razdalja med njimi.
- Interakcija (angl. interact). Dodamo metode za manipulacijo s podatki, na primer možnost premikanja vozlišč in filtriranja podatkov.

Pri izdelavi končnega izdelka moramo biti pozorni, saj zmožnost prikaza grafa (ali kateri koli drugi pogled) ni dovolj. Algoritem mora biti dovolj zmogljiv za obdelavo velike količine podatkov, ki je značilna za taka okolja.

10.8 Primeri goljufij

V nadaljevanju je predstavljenih nekaj znanih goljufij in vizualizacijskih pristopov, ki so lahko v pomoč pri preprečevanju, odkrivanju ali obravnavanju posamezne goljufije.

10.8.1 Kloniranje identifikacijskih elementov ali kraja identitete

Gre za tehnično goljufijo, kritični element pa so varnostni mehanizmi.

Napadalec na nek način prevzame identiteto običajnega uporabnika. V GSM-okolju je na primer mogoče pridobiti (uloviti) potrebne informacije za kloniranje kartice SIM (angl. Subscriber Identity Module) na daljavo. Treba je dekodirati dva pomembna zaščitna elementa SIM-kartice – IMSI (angl. International Mobile Subscriber Identity) in t. i. Ki ali glavni enkripcijski ključ. Postopek je zapleten, ker je zanj potrebna lažna bazna postaja (angl. Base Transceiver Station – BTS), vendar pa je izvedljiv [**66**].

Podobni primeri so znani iz Indije, kjer zaradi zastarele opreme in prevelike obremenitve sistemov ponekod ne šifrirajo podatkov, ki se prenašajo med mobilnim aparatom in bazno postajo (uporabljajo algoritem A5/0). V takem okolju se pridobivanje varnostnih elementov precej poenostavi [**67**].

Če ima napadalec fizični dostop do SIM-kartice, lahko izdela identično kopijo v slabi uri, in to z zanemarljivim vložkom v opremo. Natančna navodila za kloniranje SIM-kartice so prosto dostopna [**68**].

S premikom v UMTS ta težava izginja, ponovno pa se pojavlja v IP-domeni. Ker so tu sodelujoče naprave mnogo raznovrstnejše in obstaja množica različnih standardov ter načinov identifikacije, se ponuja mnogo več priložnosti za krajo identitete. Veliko storitev VoIP na primer v začetnih nastavitvah nima vklopljenega šifriranja podatkov [**69**], na kar mnogi, ničesar hudega sluteči, uporabniki pogosto pozabijo.

Delovanje

Ko napadalec prevzame identiteto registriranega uporabnika, lahko na njegov račun kliče v tujino ali na PRN-številke. Zaradi kloniranja SIM-kartic je prišlo celo do telefonov, ki so programirani tako, da preklapljajo med različnimi številkami (v [**11**] je naveden primer za 99). Tako se lažje izognejo odkrivanju, saj se promet na nobeni telefonski številki ne spremeni preveč. Leta 2001 je bilo take telefone mogoče kupiti na črnem trgu z nekajmesečno garancijo.

Preprečevanje

Preprečujemo z nadgradnjo in izboljšavo zaščitnih elementov omrežja (na primer z izboljšavo procesa identifikacije naročnika).

Za primer vzemimo kloniranje SIM-kartice, do katere imamo fizični dostop. Klonirati je mogoče kartice, zaščitene z algoritmom COMP128. Odgovor na to pomanjkljivost je bila nadgradnja algoritma COMP128v2. Ta po podatkih, ki so na voljo, za zdaj uspešno preprečuje kloniranje SIM-kartic.

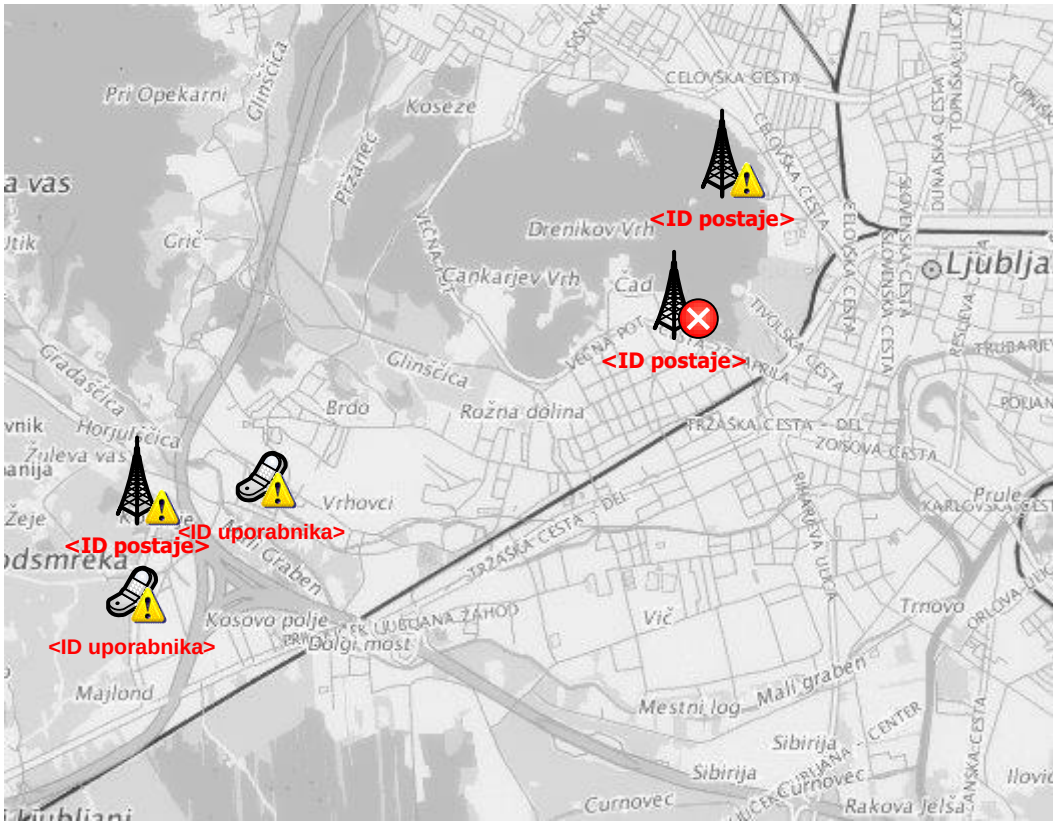
Podobno bo napad z lažno bazno postajo, ki je značilen primer napada ob podpori posrednika (angl. Man-In-The-Middle attack – MITM), v omrežju UMTS preprečen zaradi izboljšave postopka identifikacije. UMTS namreč zahteva obojestransko identifikacijo ter avtentikacijo med mobilno postajo in omrežjem [**70**].

Uporaben primer vizualizacije je predstavitev (približne) geografe lokacije, kjer je prišlo do napake pri identifikaciji bazne ali mobilne postaje. Za bazne postaje že poznamo lokacijo, za mobilne postaje pa uporabimo približno lokacijo, ki jo izračunamo s posebnimi sistemi.[30] Če je bazna postaja zaznala napako, jo označimo z opozorilnim znakom (Slika 21 – prva ikona z leve proti desni). Če gre za napako v komunikaciji z mobilno postajo, uporabimo podatke o približni postaji in jo prikažemo na ustrezni lokaciji z ikono mobilne postaje (Slika 21 – druga ikona). Podobno je, če gre za komunikacijo z lažno bazno postajo, jo predstavimo s posebno ikono bazne postaje (Slika 21 – tretja ikona).

Slika 21: Ikone bazne in mobilne postaje

Jedro take predstavitve bo zemljevid, na katerem so označena mesta kršitev (Slika 22).

[30] Mobitel (http://www.mobitel.si/slo/press/predstavitve/2002/predstavitev1.asp) na primer uporablja Ericssonov sistem za lociranje mobilne postaje MPS 3.0 (angl. Mobile Positioning System).

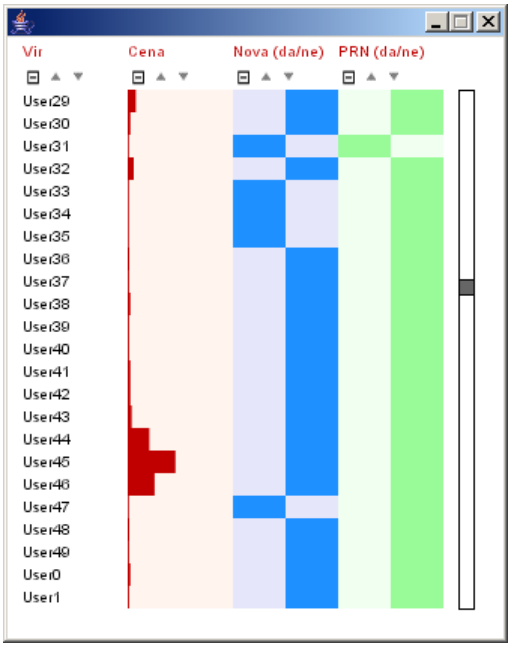


Slika 22: Zemljevid mest kršitev

Odkrivanje

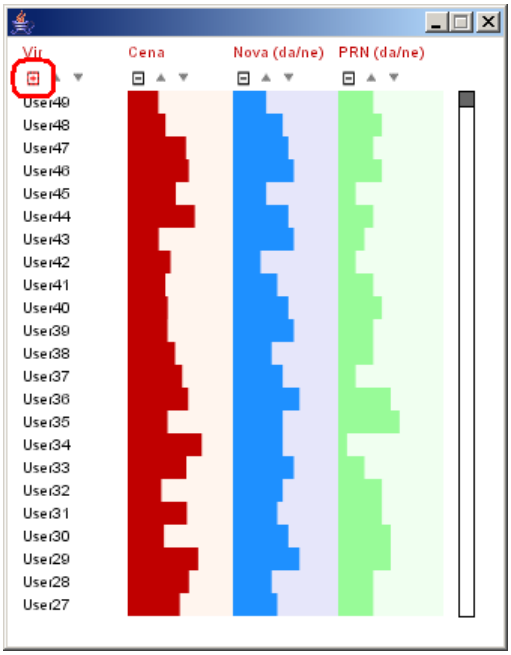
Ker napadalec prevzame identiteto naročnika, je pri odkrivanju takih goljufij glavno vodilo iskanje sprememb v vedenju naročnika. Dodatni znaki so klici na PRN-številke in v tujino. V prej opisanem glavnem pogledu (Slika 15) razvrščamo po atributih Vir, Cena in Nova. Atribut Vir predstavlja identifikacijsko številko vira, cena pa stroške, ki jih je povzročil vir v določenem obdobju. Atribut nova ima vrednosti da ali ne ter pove, ali kombinacija Vir in Cilj že obstaja. Lahko uporabimo tudi atribut Komercialna številka. Ta ima vrednosti da ali ne ter pove, ali je cilj komercialna številka. Iščemo več zaporednih transakcij iz istega vira, ki imajo visoko ceno in atribut Nova postavljen na da. Take transakcije kažejo na morebitno goljufijo.

Za lažje razumevanje postopka si oglejmo primer, predstavljen s prototipom aplikacije (Slika 23). Najprej smo izbrali štiri stolpce, ki jih želimo prikazati: Vir, Cena, Nova in PRN (komercialna številka). V stolpcu Cena so vrednosti predstavljene z močneje obarvanimi trakovi od leve proti desni. Trak, ki prekriva celotno celico, predstavlja največjo vrednost v določenem obdobju. Za stolpca Nova in PRN velja, da če je vrednost atributa da, se močneje obarva leva polovica polja, v nasprotnem primeru pa desna.



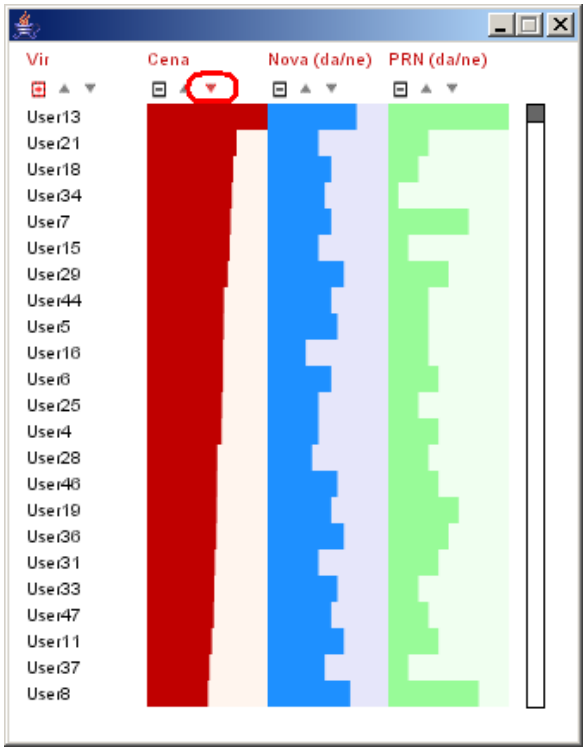
Slika 23: Prototip tabele – začetni izbor

Grupiramo po atributu Vir (Slika 24). Vrednosti binarnih atributov (Nova in PRN) se seštejejo; ne kažejo razmerja med da in ne, pač pa razmerje da z največjim številom seštetih da-jev.



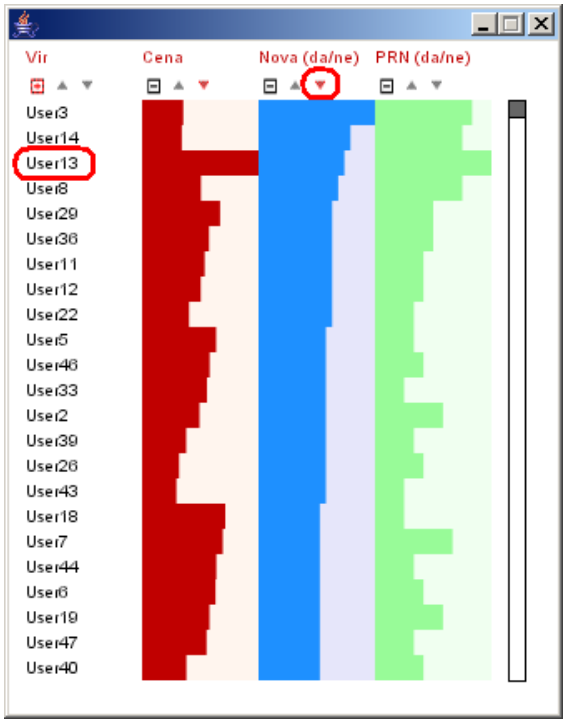
Slika 24: Prototip tabele – grupiranje po atributu Vir

Razvrščamo po atributu Cena (Slika 25).



Slika 25: Prototip tabele – razvrščanje po atributu Cena

Očitno je oseba User13 povzročila največ stroškov in največji je bil delež njenih klicev na PRN-številke. Razvrščamo še po atributu Nova (Slika 26).

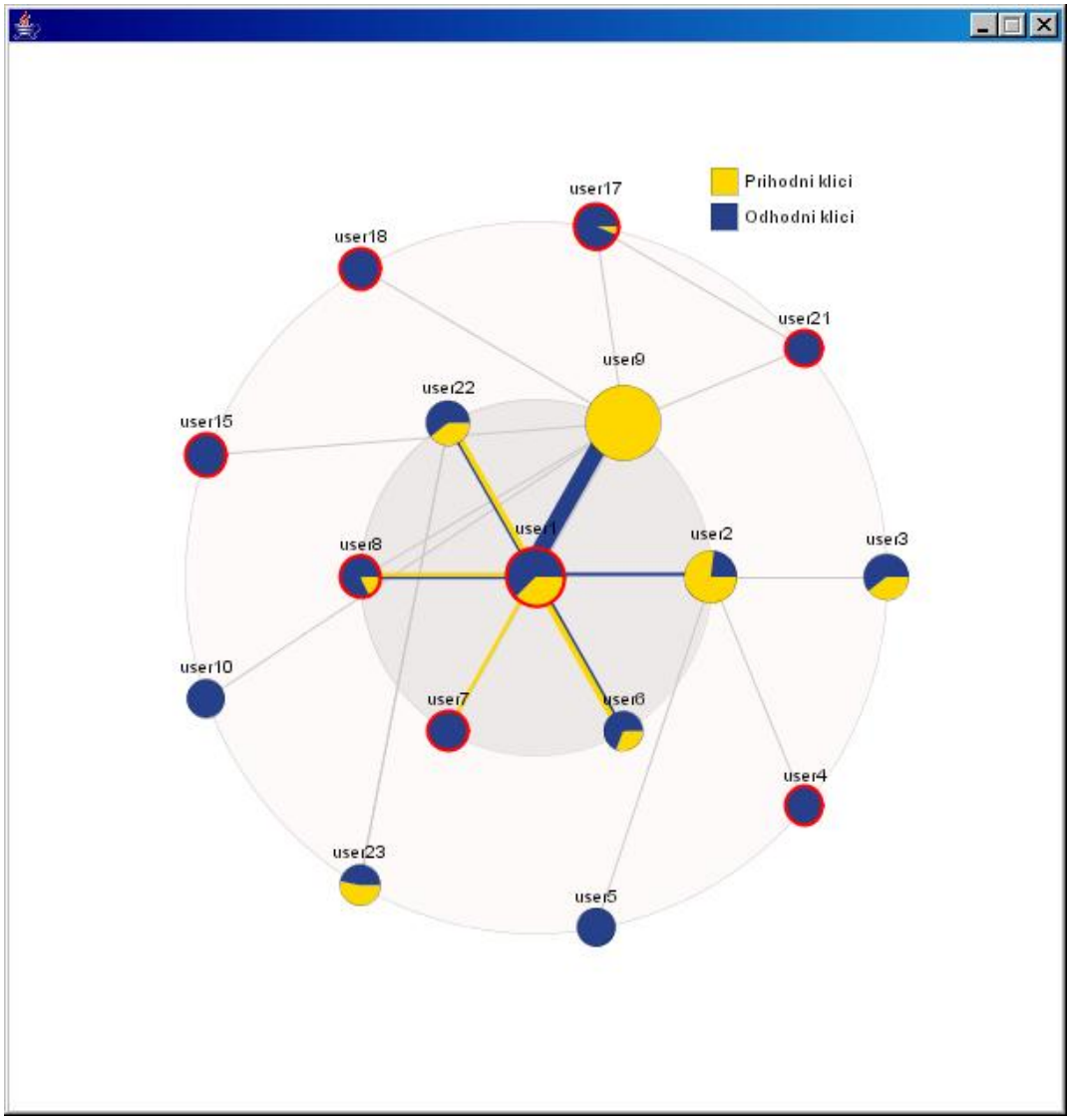


Slika 26: Prototip tabele – razvrščanje po atributu Nova

Kot vidimo, je bil pri opazovani osebi zaznan velik delež klicev na nove številke. Z dvojnim klikom vrstice opazovane osebe osvežimo okno s podrobnostmi in po želji izberemo podrobnejši prikaz za nadaljnjo raziskavo. Glede na spremembo vedenja sta v tem primeru sumljiva tudi uporabnika User3 in User14.

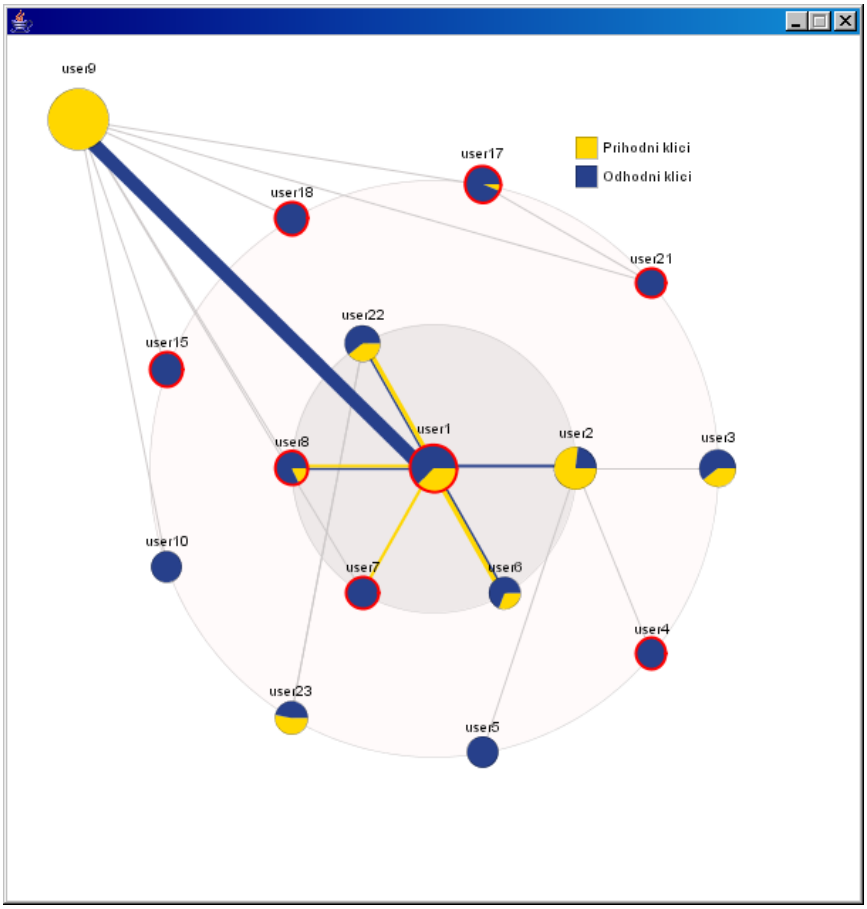
Obravnavanje izjem

Pri zasledovanju incidentov (glejte razdelek 9.1 Načrt delovanja v primeru incidenta; zasledovanje) je pomembno, da pridemo do zaključkov, ki bodo v pomoč pri izboljšanju zdajšnjega sistema. Kot primer uporabe vizualizacije v tej fazi si oglejmo dvodimenzionalno različico prikaza s stožčastim grafom (Slika 27). Vozlišče predstavlja posameznega uporabnika, tortni graf v vozlišču pa razmerje prihodnjih in odhodnih klicev istega uporabnika. Če je vozlišče obrobljeno z rdečo barvo, pomeni, da je bil uporabnik vpleten v goljufijo ali pa da obstaja verjetnost goljufije. Velikost vozlišč ponazarja razmerje med porabljenimi sredstvi posameznih vozlišč. Na začetku analize je v središče grafa postavljen uporabnik, ki je povzročil ravnokar obravnavani incident. V našem primeru je to uporabnik User1 (Slika 27). Sosednja vozlišča središča predstavljajo uporabniki, ki so komunicirali s središčnim. To so sosednja vozlišča prvega nivoja. Odhodni klici (s stališča središča) so predstavljeni z modrimi in prihodnji klici z rumenimi povezavami. Debelina povezav ponazarja razmerje med porabljenimi sredstvi parov vozlišč. Sosednja vozlišča vozliščem prvega nivoja predstavljajo uporabniki, ki so komunicirali z uporabniki, predstavljenimi z vozlišči prvega nivoja. Povezave med vozlišči prvega in drugega nivoja so predstavljene s tanko črto in le ponazarjajo, da je med vozlišči prišlo do komunikacije. Na naslednji sliki (Slika 27) vidimo, da je User1 povzročil razmeroma veliko stroškov s klici na številko uporabnika User9.



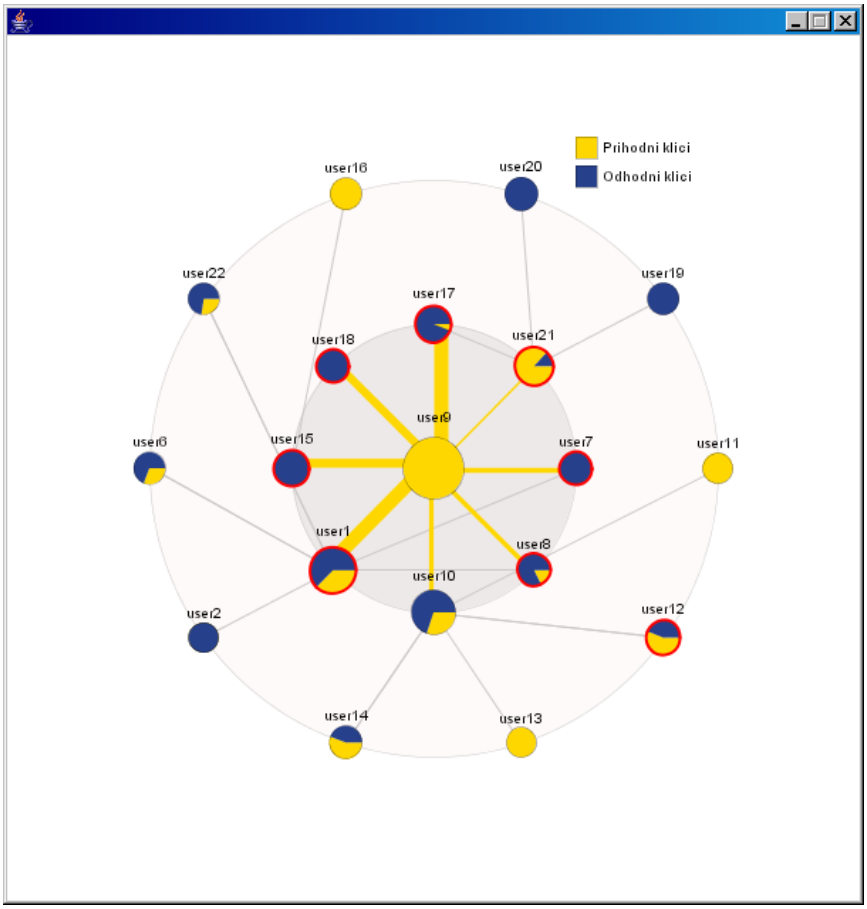
Slika 27: Prototip stožčastega grafa – začetni izbor

Ko natančneje pogledamo, kaj se dogaja z uporabnikom User9, ugotovimo, da so ga klicali še dva »osumljena« uporabnika s prvega nivoja vozlišč in štirje uporabniki z drugega nivoja (Slika 28).



Slika 28: Prototip stožčastega grafa – interakcija

Zdaj izberimo vozlišče User9 za središčno vozlišče. Rezultat je prikazan na naslednji sliki (Slika 29). Tako postane očitno, da je z omenjenim vozliščem nekaj narobe. Kar sedem od osmih kličočih je bilo vpletenih v goljufijo ali osumljenih takega dejanja. To je znak za natančnejšo analizo dogajanja na vozlišču User9.



Slika 29: Prototip stožčastega grafa – sprememba središča

10.8.2 Beige box

Gre za tehnično goljufijo, kritični element pa je oprema v lasti operaterja.

»Beige box« se pogosto obravnava v sklopu t. i. phreakinga, ki označuje včasih aktualnejšo subkulturo, katere pripadniki so preučevali, raziskovali in eksperimentirali s telefonskimi sistemi. Beseda izvira iz angleških besed *phone* (telefon) in *freak* (samovoljen, muhav, igriv …). Pozornost, namenjena telefonskim sistemom, se je v večini primerov preusmerila na internet. Zaradi tega je danes phreaking predvsem le še zgodovinsko dejstvo. Med drugim obstajajo še black, blue in red box, ki pa v današnjih sistemih ne delujejo več.

Predpogoj

Omogočen mora biti dostop do telefonske razdelilne omarice (v bloku, naselju …) ali preprosto do telefonskega kabla (parice) med priključkom in razdelilno omarico.

Predpriprave

Značilna izvedba za »Beige box« je navaden telefon z dvema priključnima sponkama (krokodilčkoma), s katerima se je lahko priključi na telefonski kabel. Treba je le odstraniti zaščito z žice oziroma najti primerno mesto za namestitev priključnih sponk.

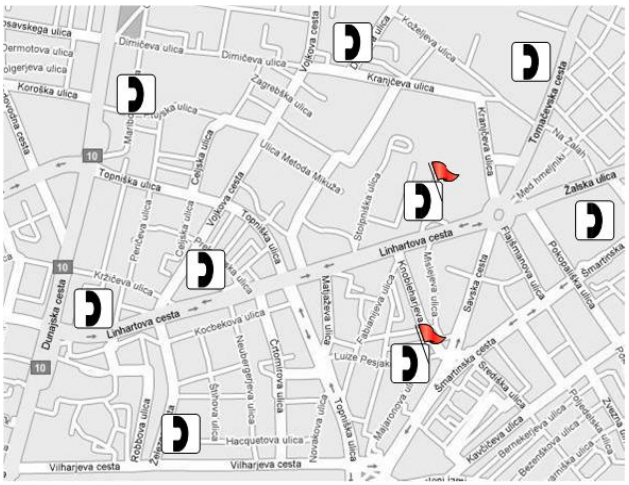
Delovanje

Telefon, priključen na linijo, prevzame identiteto legalnega telefonskega priključka.

Preprečevanje

Primer uporabe vizualizacije lahko ponazorimo z vdori v razdelilne omarice. Tu si lahko pomagamo z zgodovino vdorov, ker predvidevamo, da bo do naslednjega vdora prišlo nekje v bližini, preprosto zaradi lažje dostopnosti omarice goljufu. Identifikacijo naslednjih potencialnih tarč si olajšamo z zemljevidom ulic in razdelilnih omaric, ki so že bile tarče goljufov (Slika 31). Zadnje označimo z rdečo zastavico (Slika 30).

Slika 30: Ikone za razdelilne omarice



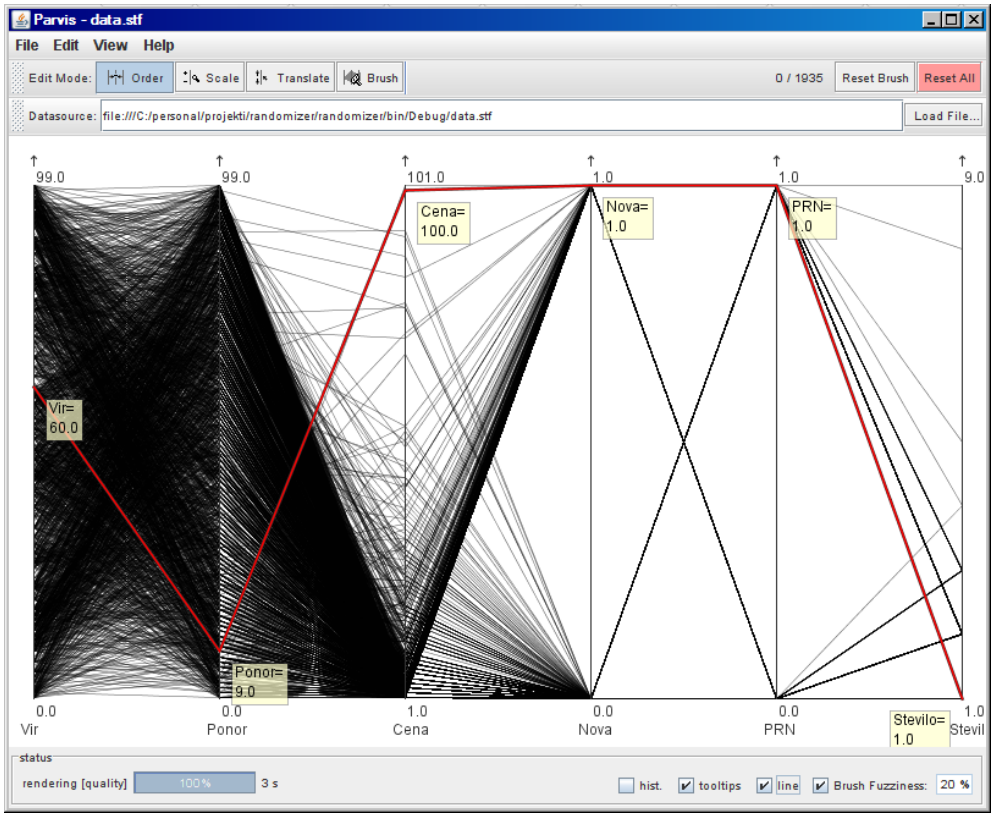
Slika 31: Zemljevid razdelilnih omaric

Omarice v bližini poskusimo bolje zaščititi. Uporabimo lahko varovalna sredstva, kot so boljše ključavnice, kamere, alarmne naprave in občasno nadziranje.

Odkrivanje

Rezultat uporabe »Beige boxa« se kaže kot prevzem identitete uporabnika, na čigar linijo se goljuf priključi. Za odkrivanje goljufov iščemo odstopanja od običajnega vedenja. Če se »Beige box« uporablja vedno na isti številki, lahko pričakujemo pritožbe stranke zaradi previsokega zneska na računu. To je opozorilo, da naj si operater pri stranki natančneje ogleda inštalacijo. Če je goljuf spretnejši in uporablja več številk, je goljufijo težko odkriti, pomagamo pa si lahko z iskanjem vzorcev med strankami.

Računi z izpiskom vseh klicanih številk veliko prispevajo k odkrivanju takih goljufij, pri katerem lahko uporabimo prikaz s paralelnimi koordinatami. Najprej prikažemo celoten promet iz obdobja, ki nas zanima (Slika 32).

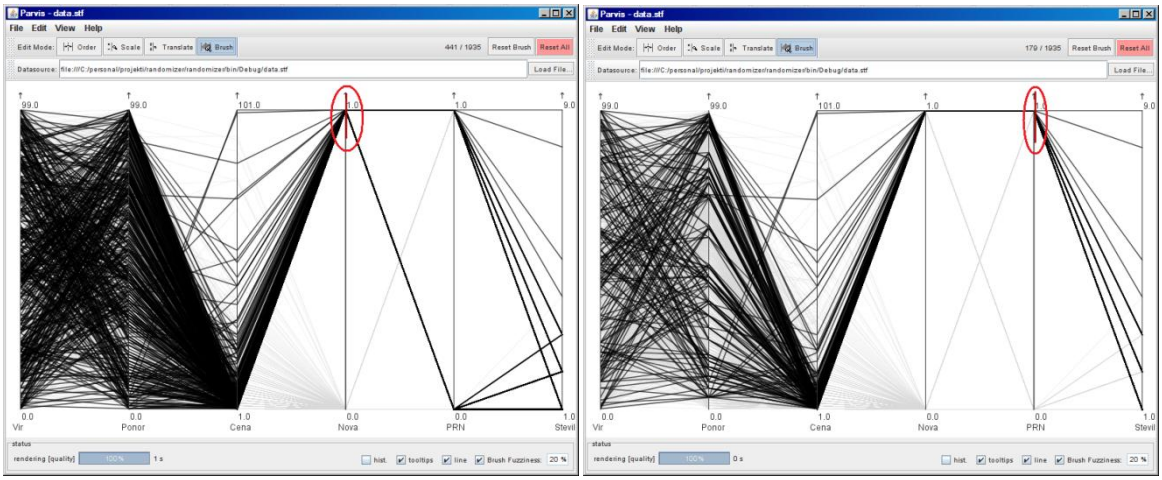


Slika 32: Paralelne koordinate – začetni izbor

Na sliki 32 je značilen prikaz s paralelnimi koordinatami. Izbrane koordinate (ki jih lahko dodajamo in odstranjujemo, če je treba) so identifikacijska številka kličočega (koordinata Vir), identifikacijska številka klicanega (koordinata Ponor), cena vseh klicev iz vira do ponora v izbranem obdobju (koordinata Cena); do klica med virom in ponorom je prvič (v celotni zgodovini obeh računov) prišlo v izbranem obdobju (koordinata Nova, ki ima lahko vrednosti da-1 in ne-0), ponor je komercialna številka (koordinata PRN,

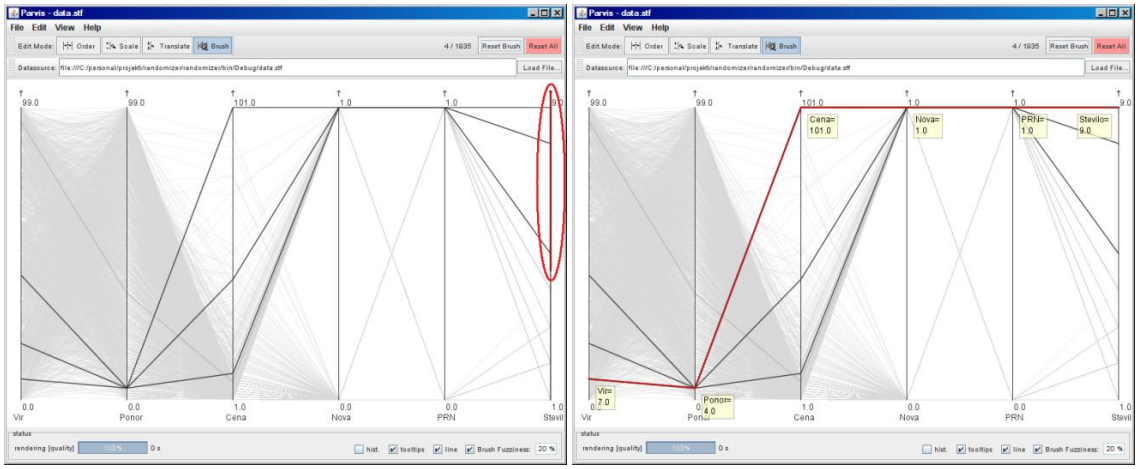
kot Nova ima vrednosti da/ne) in število klicev od vira do ponora v izbranem obdobju (koordinata Število). Rdeče obarvana črta na zaslonu je naključni zapis z vira 60 na ponor 9. Zanj velja, da je skupna cena klicev 100 enot, številka je bila prvič klicana v izbranem obdobju, ponor je komercialna številka, med virom in ponorom pa je bil v izbranem obdobju izveden samo en klic.

Oglejmo si primer analize odkrivanja obravnavane goljufije. Iščemo torej odstopanje od običajnega vedenja uporabnika. Ker se za take goljufije običajno uporabi več številk, iščemo podobne spremembe v vedenju več uporabnikov. Najprej se omejimo na zapise, ki predstavljajo klice na novo številko (Slika 33, levo), in nato še na klice na komercialno številko (Slika 33, desno). Neizbrani zapisi se zasenčijo.



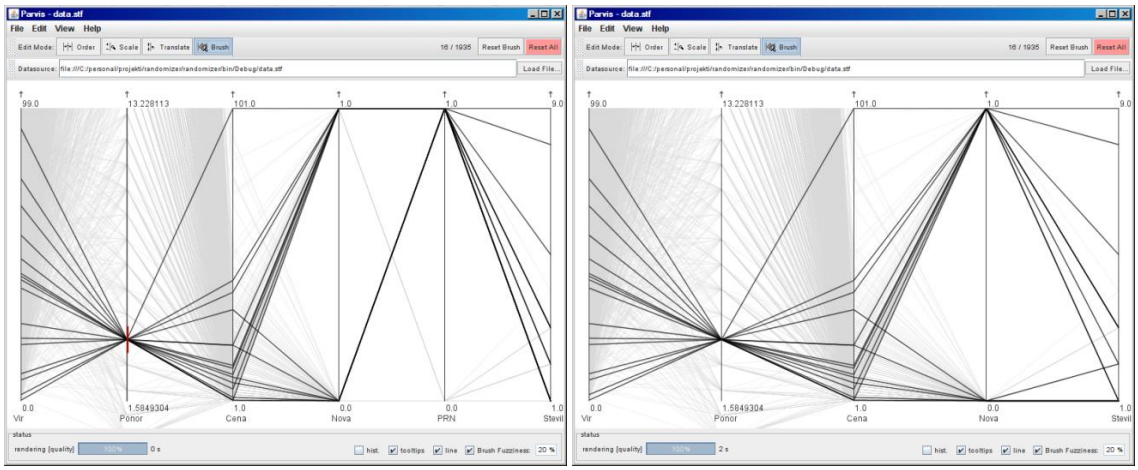
Slika 33: Paralelne koordinate – omejitev po novi in komercialni številki

Kot je bilo mogoče pričakovati, je še vedno veliko zapisov, ki ustrezajo izbranim kriterijem. Na voljo sta še koordinati Cena in Število. Izberimo tiste z večjim številom klicev (Slika 34, levo).



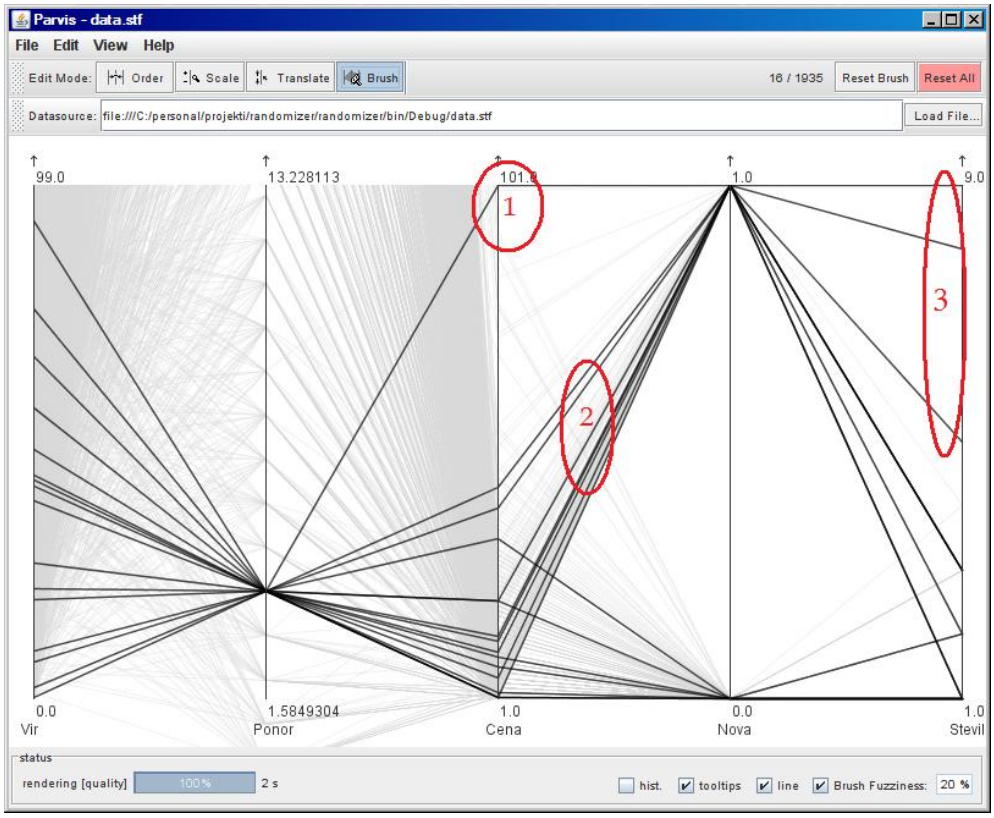
Slika 34: Paralelne koordinate – omejitev po številu klicev

Kot vidimo na sliki 34 (desno), je skupna točka vseh zapisov ponor z identifikacijsko številko 4. Zbrišimo vse do zdaj opredeljene omejitve. S povečavo koordinatne osi Ponor in z omejitvijo prikaza na vrednost 4 prikažemo vse zapise omenjenega ponora (Slika 35, levo). Koordinatno os PRN lahko zdaj odstranimo, saj ne prinaša dodatnih informacij. Vemo namreč, da je izbrana številka komercialna (Slika 35, desno).



Slika 35: Paralelne koordinate – omejitev ponora in izbris osi

Na končnem prikazu (Slika 36) vidimo, da je izbrana številka prvič klicana v večini primerov (Slika 36, oznaka 2), ima zapis z najvišjo skupno ceno (Slika 36, oznaka 1) in število klicev v samem vrhu za določeno obdobje (Slika 36, oznaka 3).



Slika 36: Paralelne koordinate – rezultat

Na podlagi take analize lahko zaključimo, da obstaja sum goljufije pri klicih na ponor 4. Sum potrdimo ali ovržemo z natančnejšo analizo.

Obravnavanje izjem

Pri razdelilnih omaricah lahko uporabimo enak pogled kot v fazi preprečevanja, saj omogoča grupiranje zlorab, ki jih zaradi bližine lahko pripišemo istemu goljufu oziroma lahko predpostavimo, da so med seboj povezane. Vizualizacija je v pomoč pri določitvi naslednje tarče ter omogoča identifikacijo in posledično kaznovanje goljufa.

10.8.3 Parazitni programi za samodejno klicanje

Gre za tehnično goljufijo, kritični elementi pa so oprema v lasti operaterja in zaposleni pri operaterju.

Parazitni program je program ali naprava z zmožnostjo klicanja naključne ali prednastavljene množice telefonskih številk. Druge zahteve so samodejno klicanje (brez posredovanja uporabnika) in zmožnost vzdrževanja zveze za določen čas.

Predpriprave

Napadalec pripravi parazitni program za samodejno klicanje (angl. autodialer). Ta je lahko v obliki naprave, ki se fizično priključi na linijo in v intervalih kliče PRN-številko (na primer vsako uro za pet minut).

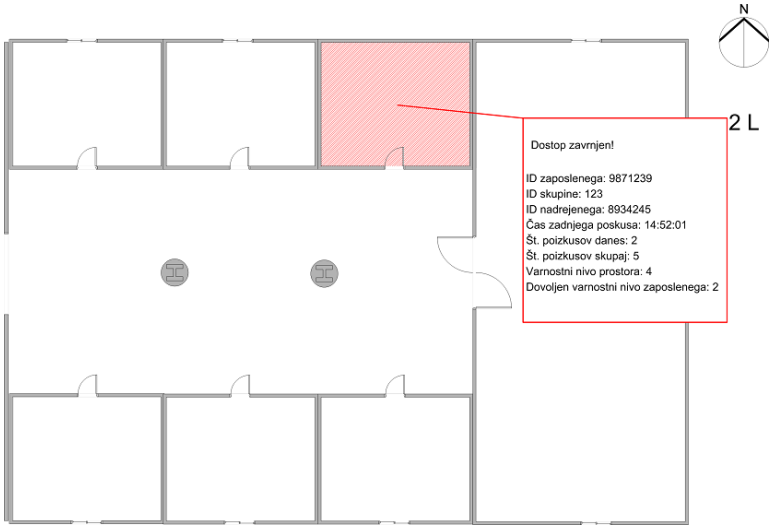
Delovanje

Zaposleni pri telefonskem operaterju napravo podtakne v operaterjevih prostorih, za nagrado pa prejema delež dobička iz PRS. Podtaknjeno napravo je zaradi intervalov in notranjih sodelavcev težko odkriti. Tako lahko deluje mesece in povzroči veliko škode.

Preprečevanje

Parazitne programe, ki kličejo PRN-številke v določenih intervalih, je praviloma težko odkriti. Seveda pa obstajajo tudi izjeme, odvisno od tega, koliko truda in raziskovanja je goljuf vložil v podvig. Na primer v [**11**] omenjen parazitni program, ki je omogočil preslepitev FMS tako, da so bili intervali klicanja vedno krajši od meje, ki jo je FMS označil za sumljivo. Take programe, ki so izdelani na podlagi notranjih informacij, je zelo težko odkriti.

Goljufijo, pri kateri se naprava podtakne v operaterjevih prostorih, lahko preprečimo s strožjim nadzorom nad dostopom do opreme in prostorov. Sem spada tudi natančna obravnava zavrnjenih dostopov. Če je zaposleni poskusil vstopiti v prostore, ki zahtevajo višjo raven varnosti, kot je omogočena, je to znak za natančnejšo obravnavo. Pomagamo si lahko s prikazom načrta prostorov in z alarmi s podrobnostmi, kadar pride do zavrnjenega dostopa (Slika 37).



Slika 37: Načrt prostorov za prikaz zavrnjenih **dostopov**

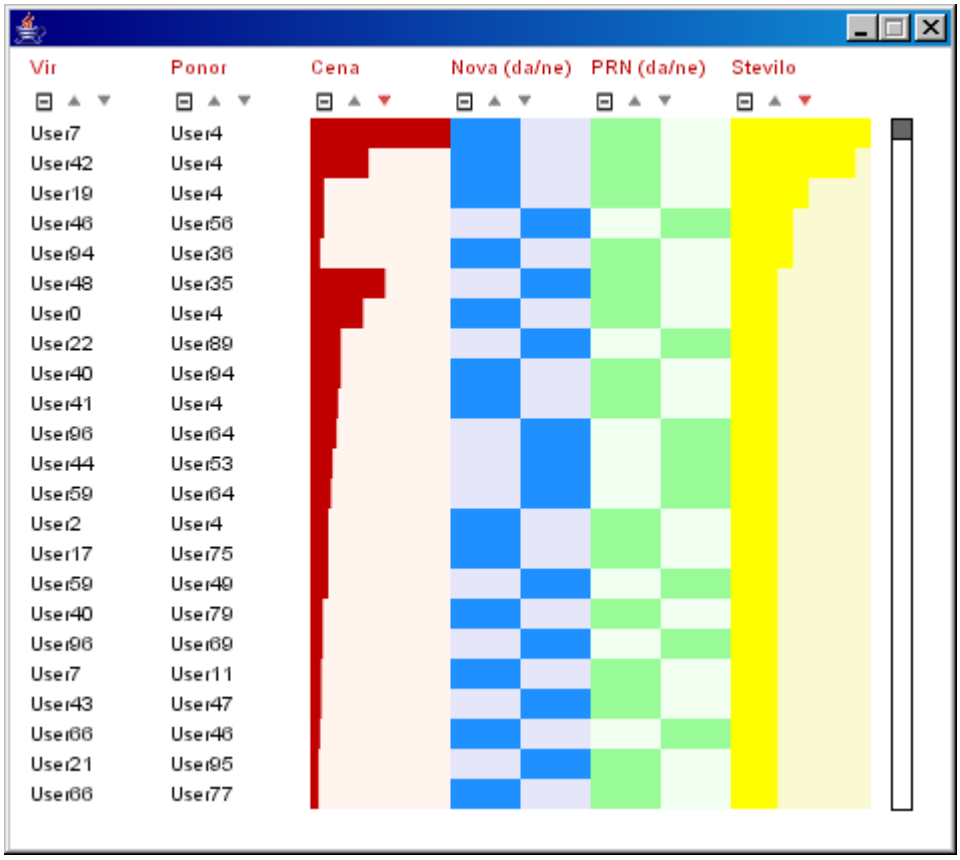
Odkrivanje

Simptomi so pogosti kratki klici in klici na PRN-številke.

Primerno orodje za odkrivanje takih goljufij so spet tabele. Prikažemo stolpce Vir, Ponor, Cena, Nova, PRN in Število. Stolpec Število predstavlja število klicev med virom in ponorom v določenem intervalu (Slika 38). Razvrstimo stolpca Cena in Število klicev.

Klici med virom User7 in ponorom User4 so sumljivi, ker:

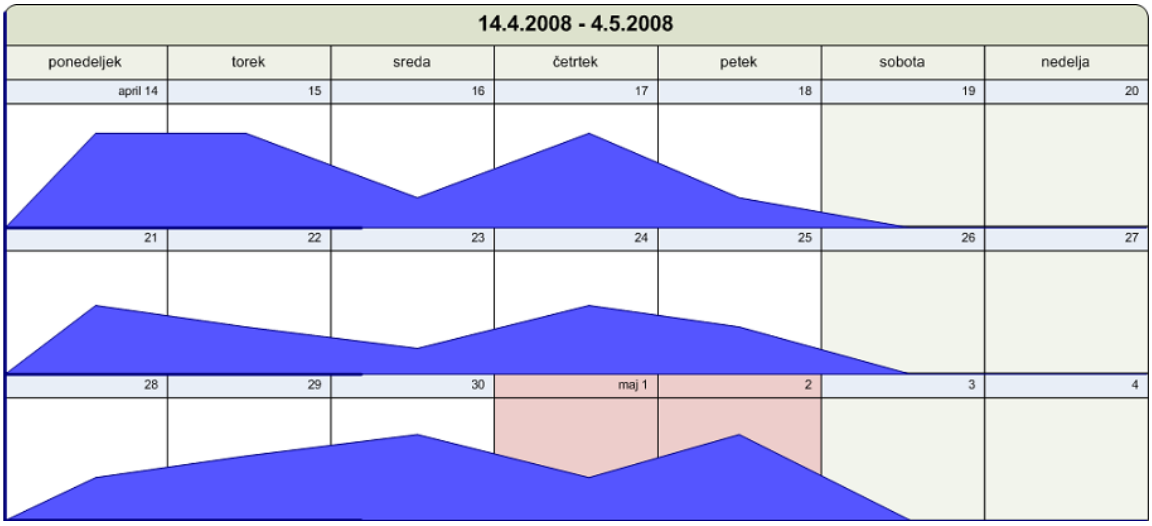
- imajo najvišjo skupno ceno v izbranem obdobju;
- je bila povezava med virom in ponorom prvič vzpostavljena v izbranem obdobju;
- je ponor PRN-številka;
- je bilo najvišje skupno število klicev v izbranem obdobju.



Slika 38: Prototip tabele – iskanje parazitnih programov

Obravnavanje izjem

Za potrditev suma najprej preučimo vedenje naročnika. Ker gre za razmeroma malo podatkov, so za predstavitev primerni preprosti grafi. Na sliki 39 je predstavljeno število klicev, razporejenih po dnevih v tednu. Predpostavimo, da je bil avtor parazitnega programa dovolj prebrisan in je nastavil različno število klicev za vsak dan in nič klicev ob koncu tedna. Iz primera na sliki je razvidno, da je pozabil na praznike, ki so dela prosti dnevi. Taki ključi samo še potrdijo verjetnost goljufije.



Slika 39: Graf za primerjavo števila klicev po dnevih v tednu

10.8.4 Zloraba dodatnih funkcij zasebne naročniške centrale

Gre za tehnično goljufijo, kritični element pa so varnostni mehanizmi.

Predpogoj

Zasebna naročniška centrala (angl. Private Branch eXchange – PBX)[31] mora omogočati klicanje iz centrale skozi zunanjo linijo (angl. Direct Inward System Access – DISA). Oseba, ki kliče, plača samo klic do centrale.

Predpriprave

Najprej mora napadalec ugotoviti, katero številko poklicati za dostop do linije DISA. Tu si pomaga s splošno dostopno dokumentacijo o sistemu, z javno dosegljivimi številkami in ugibanjem. Dostop do linije

[31] Tri najbolj razširjene hišne centrale so Centrex, KTS in PBX.

DISA je običajno zaščiten z geslom. Izkaže se, da veliko skrbnikov sistema ne nastavi novega gesla in pusti privzeto vrednost, ki jo napadalec lahko pridobi brez posebnih težav.[32] Druga možnost je poizkušanje. Za primer vzemimo sistem, ki za geslo uporablja samo štiri znake. Napadalec preizkusi le najpogostejše (npr. 1111, 0000, 1234 …), in če mu ne uspe, nadaljuje z naslednjo telefonsko številko. Čeprav je tak pristop preprost, je velikokrat zelo uspešen.

Delovanje

Ko napadalec vstopi v sistem, lahko kliče na račun ustanove, ki ima v lasti napadeni PBX. Kadar je v napadenem sistemu veliko prometa, pogosto mine veliko časa, preden se take goljufije odkrijejo. Če je napadalec previden in ne povzroči veliko škode naenkrat, ni razloga, da bi tako goljufijo sploh kdaj odkrili, še posebej, kadar so PBX-centrale v zasebni lasti, kjer lastniki praviloma ne namenijo veliko pozornosti odkrivanju in preprečevanju goljufij.

Preprečevanje

Za zasebno centralo so navadno odgovorni lastniki, in ne operater. Operater (zaradi dobrih odnosov z naročniki) lahko zasleduje spremembe v vedenju in nenavadne dogodke (klice PRN-številk) ter o tem diskretno obvesti stranko.

Take zlorabe preprečujemo predvsem z izobraževanjem lastnikov naročniških central tako, da so sposobni sami poskrbeti za varnost v svojem sistemu. Pomembno je tudi redno obveščanje o novih goljufijah in načinih preprečevanja.

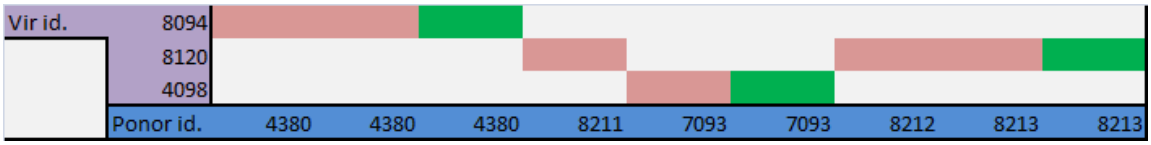
Za primer vizualizacije vzemimo prikaz napačno vpisanih gesel. Potrebujemo podatke o viru oziroma številki, s katere je klical uporabnik, ki je vtipkal napačno geslo, in podatke o ponoru oziroma številki za dostop do linije DISA. Prikazati želimo izključno napačno vpisana gesla za dostop do linije DISA.

Tabela je predstavljena na spodnji sliki (Slika 40). Na levi strani so identifikacijske številke vira. Vsaka vrstica (razen zadnje, ki predstavlja identifikacijsko številko ponora) predstavlja dejanja vira. Najnovejše dejanje je prikazano na skrajni desni.

Ločimo tri vrste dejanj, ki so predstavljene z barvo polja:

- Rdeče polje. Uporabnik (vir) je vtipkal napačno geslo za dostop do linije DISA (ponor).
- Zeleno polje. Uporabnik je vtipkal pravilno geslo.
- Belo polje. Ni dejanja uporabnika.

[32] Odličen vir za take informacije je internet. Primer strani s seznamom privzetih gesel je na http://www.phenoelit-us.org/dpl/dpl.html (13. 3. 2008).

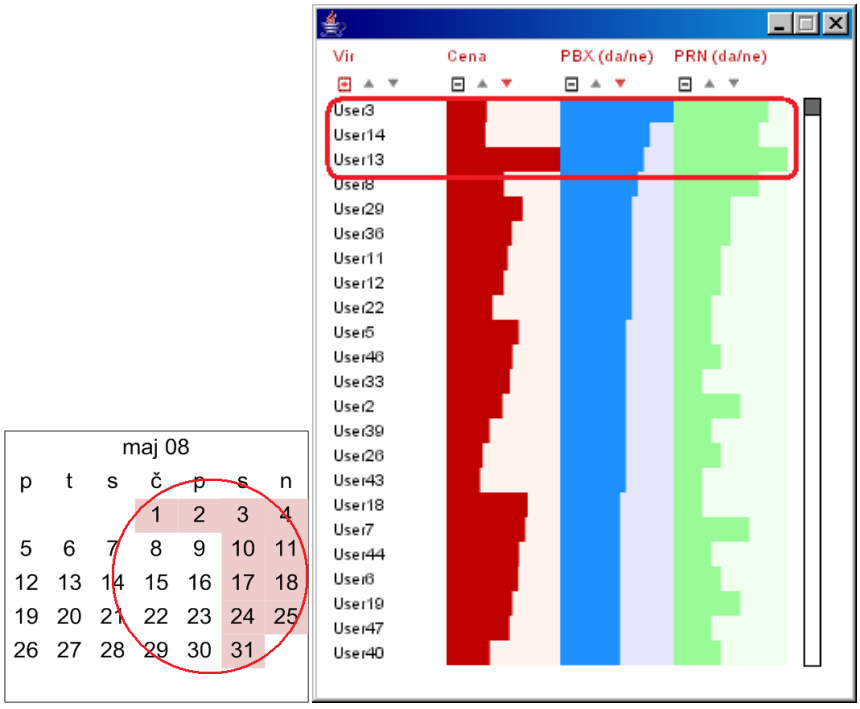


Slika 40: Tabela zavrnjenih dostopov do linije DISA

V našem primeru je sumljiv uporabnik 8120, ker je večkrat vpisal napačno geslo na različnih številkah za dostop do linije DISA (8211, 8212 in 8213).

Odkrivanje

Znamenja zlorabe hišne centrale so predvsem dejavnost med dela prostimi dnevi, klici v tujino in klici PRN-številk. Po drugi strani pa so dolgi klici v tujino zunaj običajnega delavnega časa značilni za podjetja, ki sodelujejo s tujino oziroma prodajajo svoje storitve v tujino, zato je nujna določena previdnost. Podobno so tudi klici komercialnih številk nekaj običajnega, če se na komercialni številki ponujajo na primer svetovalne storitve. Spet si lahko pomagamo s tabelami, kjer s filtrom opredelimo, da opazujemo samo dela proste dneve (Slika 41, levo), grupiramo po atributu Vir ter razvrstimo po atributih Cena in PBX. Atribut PRN ima lahko vrednosti da ali ne in pove, ali je vir hišna centrala. Na sliki 41 (desno) vidimo, da so zanimivi predvsem prvi trije uporabniki, ki so iz hišne centrale opravili razmeroma visok delež klicev komercialne številke.



Slika 41: Prototip tabele – zloraba hišne centrale

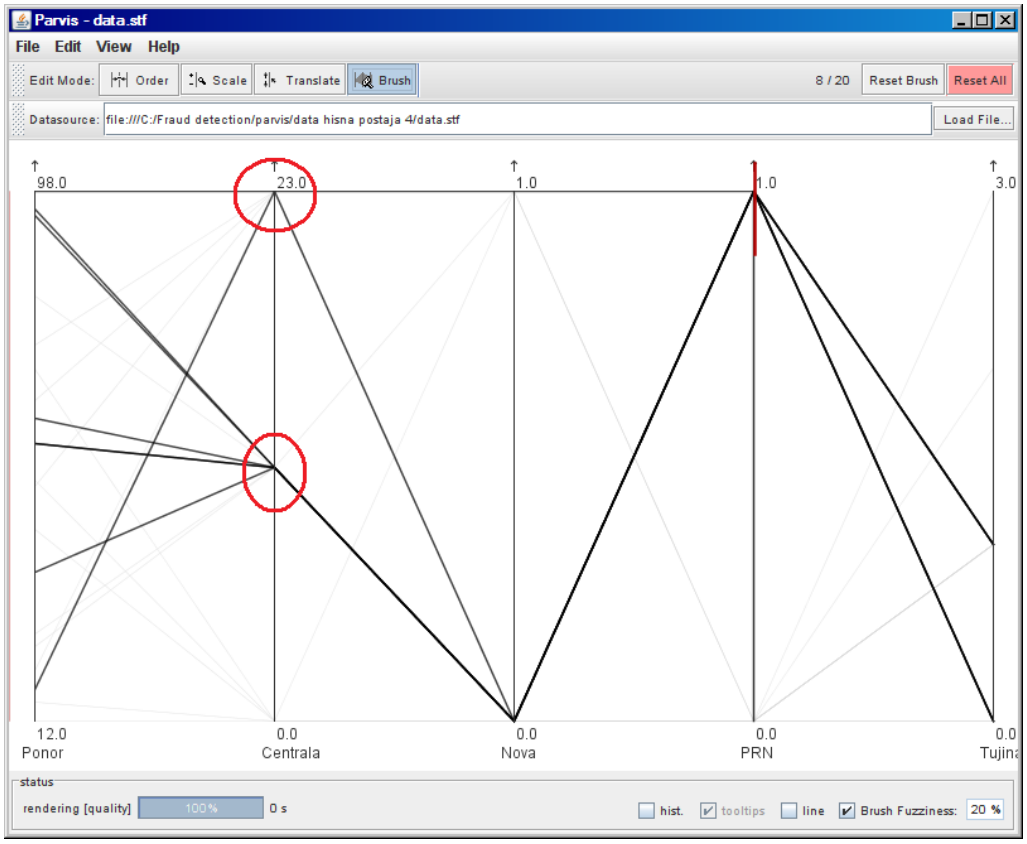
Obravnavanje izjem

V fazo dobimo podatke o viru nenavadnega prometa prek hišne postaje. Tu sum potrdimo oziroma zavrnemo in podatke o primeru posredujemo lastniku hišne postaje. Koristno je, da se tudi pri običajnem prometu pošiljajo poročila prometa v določenih obdobjih.

Sum potrdimo z natančnejšo analizo prometa pri osumljenem viru. S pogledom paralelnih koordinat preučimo vedenje vira.

Na sliki 42 je predstavljen samo promet osumljenega uporabnika. Uporabimo naslednje koordinate:

- Ponor. Identifikacijska številka ponora.
- Centrala. Identifikacijska številka centrale.
- Nova. Podatek, ali se je v izbranem obdobju prvič klicalo na ponor.
- PRN. Podatek, ali gre za klic PRN-številke.
- Tujina. Število klicev v tujino.



Slika 42: Paralelne koordinate – zloraba hišne centrale

Zanimivo je predvsem dejstvo, da je uporabnik iz osumljenega vira izvedel veliko klicev različnih PRN-številk in pri tem uporabljal dve različni hišni centrali.

10.8.5 Zloraba predala za glasovno pošto

Gre za tehnično goljufijo, kritični elementi pa so varnostni mehanizmi in postopki operaterja.

Predpogoj

Telefonski operater napadenega mora omogočati preusmerjanje neodgovorjenih klicev v telefonski predal za glasovno pošto (angl. voice mailbox). Telefonski operater napadalca mora omogočati klicanje na stroške tretje osebe in operater, ki preverja, ali tretja oseba sprejme klic, mora biti avtomatiziran (če prepozna besede, kot so *da*, *ja* in *sprejmem*, samodejno sprejme klic).

Predpriprave

Z ugibanjem gesla (zakaj je to preprosto, je bilo opisano že pri prejšnji goljufiji) se vdre v telefonski predal in zamenja sporočilo za sprejem klica v predalu. Novo sporočilo se glasi nekako tako; »Da, da, da, da, sprejmem stroške.«

Delovanje

V času, ko predvidevamo, da napadeni ne bo odgovarjal na klice (ponoči, ob koncu tedna in med počitnicami), se številka uporabi za klicanje na stroške tretje osebe. Ko avtomatizirani operater prepozna besedi, kot sta *da* in *sprejmem*, dovoli klic na stroške klicanega.

Preprečevanje

Take goljufije lahko preprečimo predvsem s poostritvijo politike kompleksnosti in obnavljanja gesel za dostop do glasovne pošte. V fazi preprečevanja gre za isti problem kot v prejšnjem primeru, uporabimo pa lahko enak pristop za iskanje uporabnikov, ki ugibajo gesla.

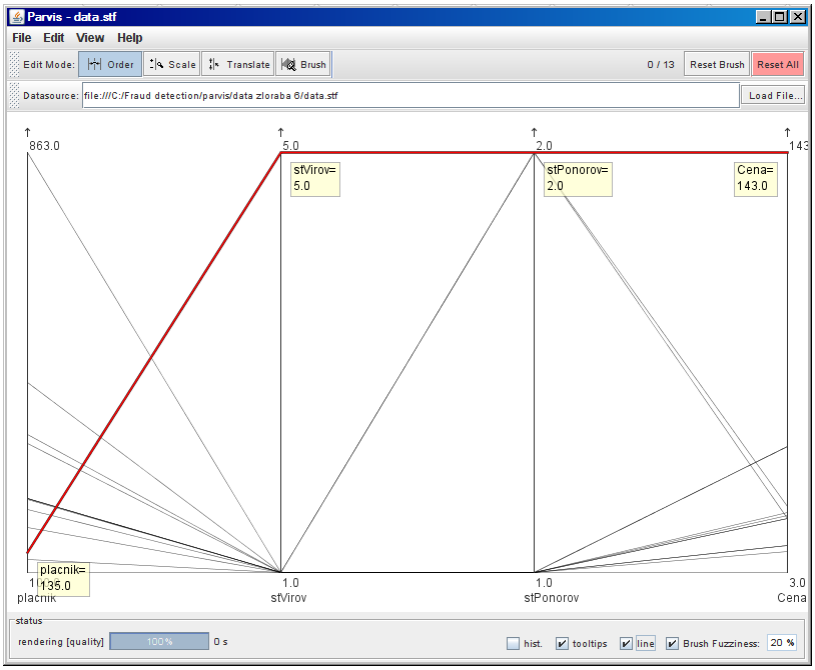
Odkrivanje

Vzorci, ki izdajajo tako goljufijo, so povečano število klicev ob nenavadnem času (ponoči, med prazniki in počitnicami …), večja količina klicev na stroške tretje osebe (ki je enaka za več virov) ter klici v tujino ali klici komercialnih številk.

Za odkrivanje uporabimo paralelne koordinate. Najprej omejimo prikaz na transakcije, kjer je tip plačnika tretja oseba (Slika 43), uporabimo SQL-filter. Rezultat poizvedbe prikažemo v pogledu paralelnih koordinat (Slika 44). Če ima isti plačnik večje število virov in ciljev, je to znamenje za natančnejšo raziskavo.

```
SELECT    [Id placnika] AS 'placnik'
          ,COUNT(DISTINCT([Id vira])) AS 'stVirov'
          ,COUNT(DISTINCT([Id ponora])) AS 'stPonorov'
          ,SUM([cena]) AS 'cena'
FROM      [Transakcija 3April2008]
WHERE     [Tip placila] LIKE 'tretja oseba'
GROUP BY [Id placnika]
```

Slika 43: Poizvedba SQL



Slika 44: Paralelne koordinate – zloraba predala za glasovno pošto

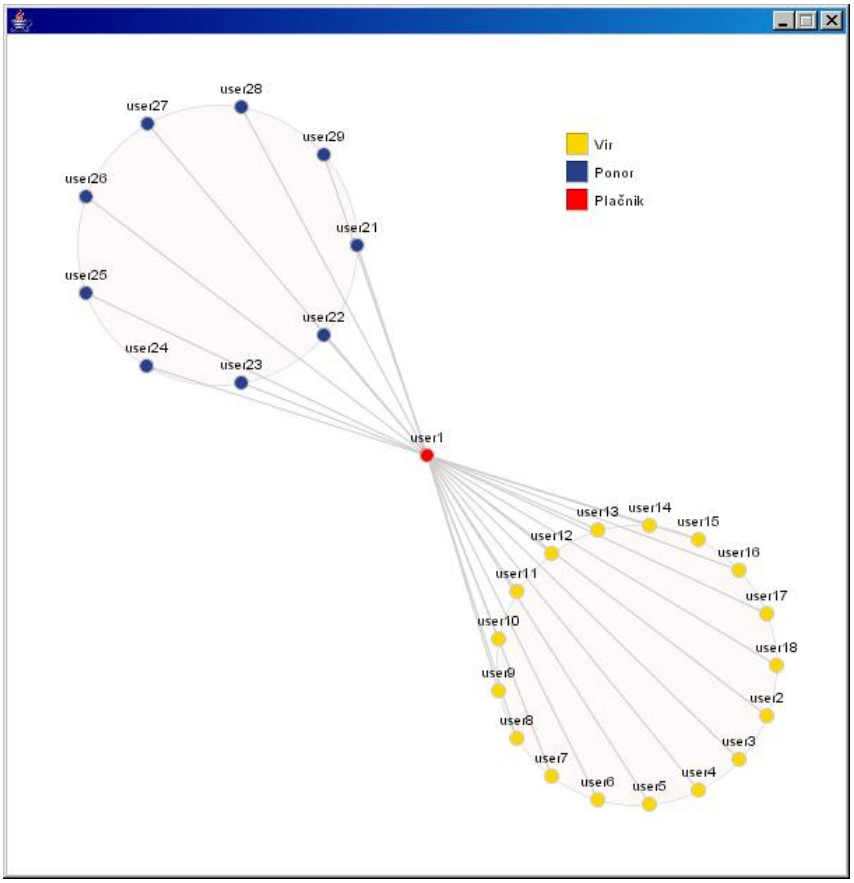
Na sliki 44 so uporabljene naslednje koordinate:

- Plačnik. Identifikacijska številka plačnika tipa tretja oseba (glejte SQL-poizvedbo).
- StVirov. Vsota različnih virov, ki so za plačnika uporabili isto osebo.
- StPonorov. Vsota različnih ponorov klicev, pri katerih je plačnik ista oseba.
- Cena. Skupna cena, ki jo je plačala tretja oseba – plačnik.

Obravnavanje izjem

V tej fazi dobimo podatke o tretji osebi, ki je plačala veliko klicev. Da potrdimo sum, podatke predstavimo še z grafom. Prikaz na sliki 45 ponazarja razmerje med viri in ponori klicev. Na običajni sliki

bi bil samo eden ali dva vira. Če je treba, graf obogatimo s prikazom lastnosti, kot so komercialna številka, nova številka, cena klicev, število klicev in podobno. Z dvojnim klikom povezave ali vozlišča pa prikažemo podrobnosti.



Slika 45: Predstavitev z grafom – zloraba predala za glasovno pošto

10.8.6 Posredovanje klicev brez vednosti lastnika številke

Gre za netehnično goljufijo, kritični elementi pa so oprema v lasti uporabnika in uporabniki.

Predpogoj

Telefonski operater napadenega mora omogočati posredovanje klicev (angl. call forwarding) na drugo številko in klicanje na stroške klicanega (angl. collect call).

Predpriprave

Najprej je treba lastnika številke prepričati, da vtipka številko za posredovanje klicev (navadno *72 za operaterje v ZDA) in številko, na katero želi napadalec prejemati klice. Prepričati lastnika, da to stori, ni tako težko, kot bi si morda mislili. Dovolj je, da se napadalec izdaja za telefonskega operaterja, ki preverja telefonski sistem. Drugi preizkušeni način je, da stopi do žrtve in prosi za klic pod pretvezo, da se mu je pokvaril avtomobil in da želi poklicati servis. Ko mu ta dovoli klicati (večina ljudi bi to dovolila), lahko kar sam vtipka številko za preusmeritev.

Delovanje

Napadalec sporoči sodelavcem v tujini, naj ga pokličejo na številko, s katere je preusmeril klice. Stroške klicanja sprejme napadalec s svoje številke, dejanska številka, za katero bo prišel račun, pa je preusmerjena številka.

Preprečevanje

Veliko klicev na stroške klicanega, pri katerih je prišlo do posredovanja klicev z iste številke, je namenjenih za opozorilo, da obstaja možnost goljufije.

Goljufijo preprečimo tako, da zaščitimo aktiviranje posredovanja klicev z geslom, ki ga pozna le naročnik. Druga možnost je sprememba politike zaračunavanja klicev. Posredovani klici se plačajo za številko, na katero preusmerimo klice.

Z vizualizacijo si v fazi preprečevanja ne moremo pomagati, saj se pri vzpostavitvi goljufije ne kršijo nobeni varnostni mehanizmi, najuspešnejše sredstvo za preprečevanje takih goljufij pa je izobraževanje naročnikov.

Odkrivanje

Ker so znaki enaki kot pri prejšnji zlorabi, je tudi identifikacija enaka. Opazujemo torej atribut Tip plačila.

Obravnavanje izjem

Tudi v tej fazi lahko uporabimo postopek iz prejšnjega primera.

10.8.7 Klicanje na stroške tretje osebe brez njenega soglasja

Gre za netehnično goljufijo, kritični elementi pa so postopki operaterja in uporabniki.

Predpogoj

Telefonski operater omogoča klicanje na stroške tretje osebe (angl. third party billing).

Predpriprave

Napadalec iz telefonskega imenika izbere naključno osebo. Pokliče izbrano številko in izbere plačilo na stroške tretje osebe. Operaterju se predstavi kot oseba iz telefonskega imenika in pove, da želi plačati prek domače telefonske številke.

Delovanje

Tretja oseba, ki sprejme klic (na domači številki), bo navadno potrdila, da sprejme stroške.

Razlogi so naslednji:

- osebe, ki je navedena v imeniku, ni doma;
- oseba ima sorodnika z istim imenom;
- nesporazum – oseba ne razume operaterja.

Preprečevanje

Večino takih goljufij odkrijemo in preprečimo z izboljšavo postopka identifikacije kličočega. Zahtevamo na primer, da poleg imena navede tudi datum rojstva. Tako bo tretja oseba vedela, da je dovolila klic pravi osebi. Veliko pa prispevajo že opozorila tretji osebi, da pri takih zahtevah obstaja možnost prevare.

Ker se ne kršijo nobeni varnosti mehanizmi, ni ustrezne vizualizacije.

Odkrivanje

Odkrivanje take goljufije je praktično nemogoče, ker je plačnik naključna oseba, ki se ne ponavlja. Z ustreznimi varnostnimi mehanizmi za identifikacijo kličočega pa lahko take goljufije preprečimo.

Obravnavanje izjem

Obravnava takih goljufij je v večini primerov neuspešna, ker gre za klice iz telefonske govorilnice, pri čemer se uspešno zakrije identiteta kličočega. Edina sled, ki jo lahko uporabimo (če tarča oziroma plačnik ugotovi, da je znesek na računu previsok), je številka, ki jo je goljuf klical.

10.8.8 Sklenitev pogodbe z lažno identifikacijo

Gre za netehnično goljufijo, kritični elementi pa so postopki operaterja.

Predpriprave

Sklenitev pogodbe z lažno identifikacijo (angl. subscription fraud) pomeni, da goljuf uporabi lažno identifikacijo pri sklenitvi naročniške pogodbe s telefonskim operaterjem. To je težje izpeljati pri nas kot pa na primer v ZDA, kjer ima vsaka od petdesetih držav drugačen osebni dokument. Ker oseba, ki

sprejema naročnine, ne pozna vseh različic osebnega dokumenta, je mogoče uporabiti tudi slabše ponaredke.

Sklenitev pogodbe z lažno identifikacijo je lahko posledica kraje identitete (angl. identity theft). V tem primeru napadalec prevzame identiteto tretje osebe. Kraja identitete je že nekaj let v porastu. Dober pokazatelj porasta tega problema je pojav specializiranih podjetij za preprečevanje take kraje.[33]

Delovanje

Napadalec, če mu uspe skleniti naročnino, ne namerava plačati mesečnih obveznosti. V večini primerov lahko kliče mesec dni brezplačno. Ko operater opazi, da račun, ki je običajno visok, ni bil plačan, kaj hitro onemogoči nadaljnjo uporabo.

Pri mobilnih operaterjih včasih (zdaj naj bi bili že bolje usklajeni) tudi to ni zadostovalo, saj je bilo telefon še nekaj časa mogoče uporabljati pri operaterjih v drugih državah.

Preprečevanje

Logična rešitev za znižanje teh vrst goljufije bi bila poostritev pogojev za sklenitev pogodbe, na primer natančnejše preverjanje identitete prihodnjega naročnika, omejitve v prvem mesecu naročniškega razmerja, promocija predplačniških razmerij ali neposredna obremenitev bančnega računa. Vendar je to dvorezen meč za telefonske operaterje. Njihov cilj je namreč pridobiti kar se da veliko naročnikov (sklenitev naročnine ne sme biti zapleten postopek) in jim dovoliti, da zapravijo toliko, kolikor želijo (nočejo jih omejevati pri zgornji meji porabe).

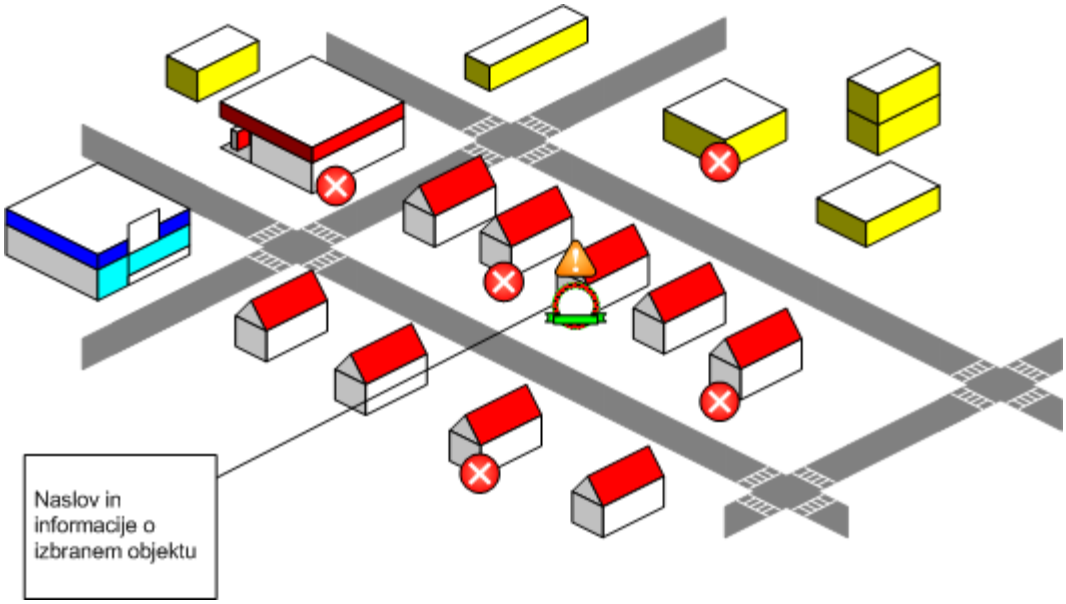
Če je goljuf že kdaj zagrešil tako goljufijo in poizkuša znova skleniti naročniško razmerje z drugo lažno (ali pa pravo) identiteto, ga lahko odkrijemo po vzorcu številk, ki jih kliče oziroma ki kličejo njega (angl. fingerprint). Obstaja velika verjetnost, da bo goljuf še naprej klical iste številke [**9**], torej prijatelje, sodelavce itd. Dovolj je, da si zapomnimo pet najpogostejših vhodnih in izhodnih številk vseh odkritih goljufov in vzorec primerjamo z novimi naročniki. Tako lahko hitro odkrijemo poizkuse novih goljufij starih goljufov.

Na splošno velja, da je tako goljufijo lažje preprečiti, kadar govorimo o fiksni telefoniji, saj nas isti naslov opozori na morebitno zgodovino goljufij, rizične sostanovalce ali sorodnike in podobno.

Za preprečevanje uporabimo predstavitev z mapo iskane lokacije (Slika 46). Tu so podane informacije o objektu na naslovu in informacije o že odkritih goljufijah ali sumih goljufije v okolici. Če goljuf uporabi pravi naslov, so znaki že znane zlorabe v okolici ali na istem naslovu. Če goljuf poda lažni naslov, so znaki nepoznavanje goljufa z objektom na tem naslovu (ali gre za stanovanjsko hišo, blok …) ali neujemanje podanih podatkov z dejanskimi (na primer na naslovu ni družine s podanim priimkom).

---

[33] V kraju Tempe v Arizoni je na primer podjetje LifeLock, ki za devet dolarjev na mesec (http://www.lifelock.com, 13. 11. 2007) varuje posameznike pred krajo identitete.



Slika 46: Mapa iskane lokacije

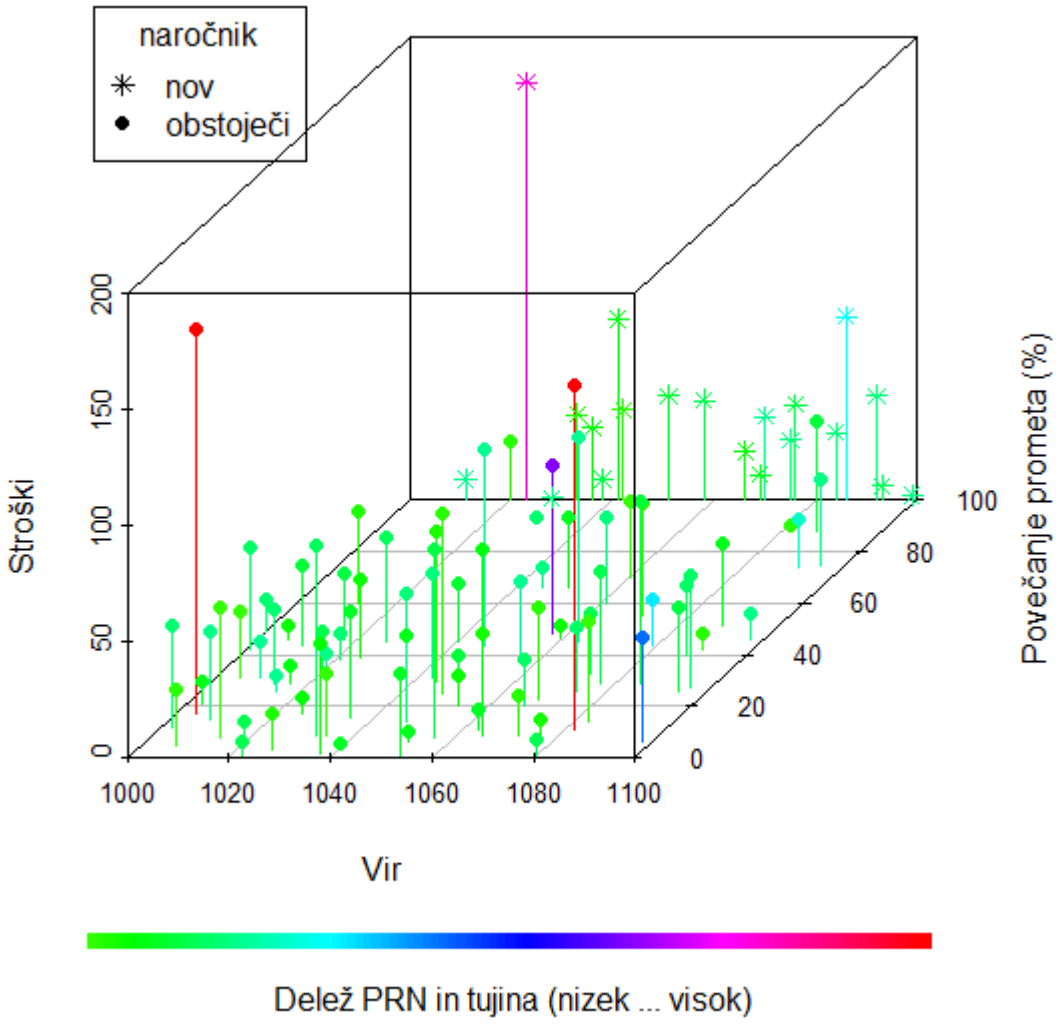
Operater, ki sklepa razmerja, odkrije goljufa z vsakdanjimi vprašanji, s katerimi poizveduje o tem, ali stanujete v stanovanjski hiši, o tem, kdo še živi na tem naslovu, in podobno. Če odkrije neskladnosti v odgovorih ali pa vidi, da so bile na tem naslovu že odkrite goljufije, se ustrezno odzove.

Odkrivanje

Znak, da je z naročnikom nekaj narobe, je, da se v prvem mesecu naročniškega razmerja opravi nadpovprečno veliko prometa. Samo po sebi to ni dokaz, da gre za goljufijo, vendar pa je dober znak za operaterja, da preveri, kaj se dogaja z naročnikom.

Taka goljufija se odkrije najpozneje v prvem mesecu, ko naročnik ne plača svojih obveznosti.

Goljufijo lahko odkrivamo z razpršenim 3D-grafom. V našem primeru (Slika 47) smo za os x izbrali identifikacijsko številko vira, y pa predstavlja povečanje prometa v primerjavi s prejšnjim obdobjem in os z stroške, ki so nastali v tem plačilnem obdobju. Dodatni dimenziji predstavljata barva in oblika točke. Barvna shema od zelene do rdeče predstavlja odstotek klicev komercialnih številk ali številk v tujini. Če takih klicev ni ali pa jih je malo, se zadržujemo na zeleni strani spektra, z višanjem odstotka takih klicev pa se premikamo k rdečemu delu.



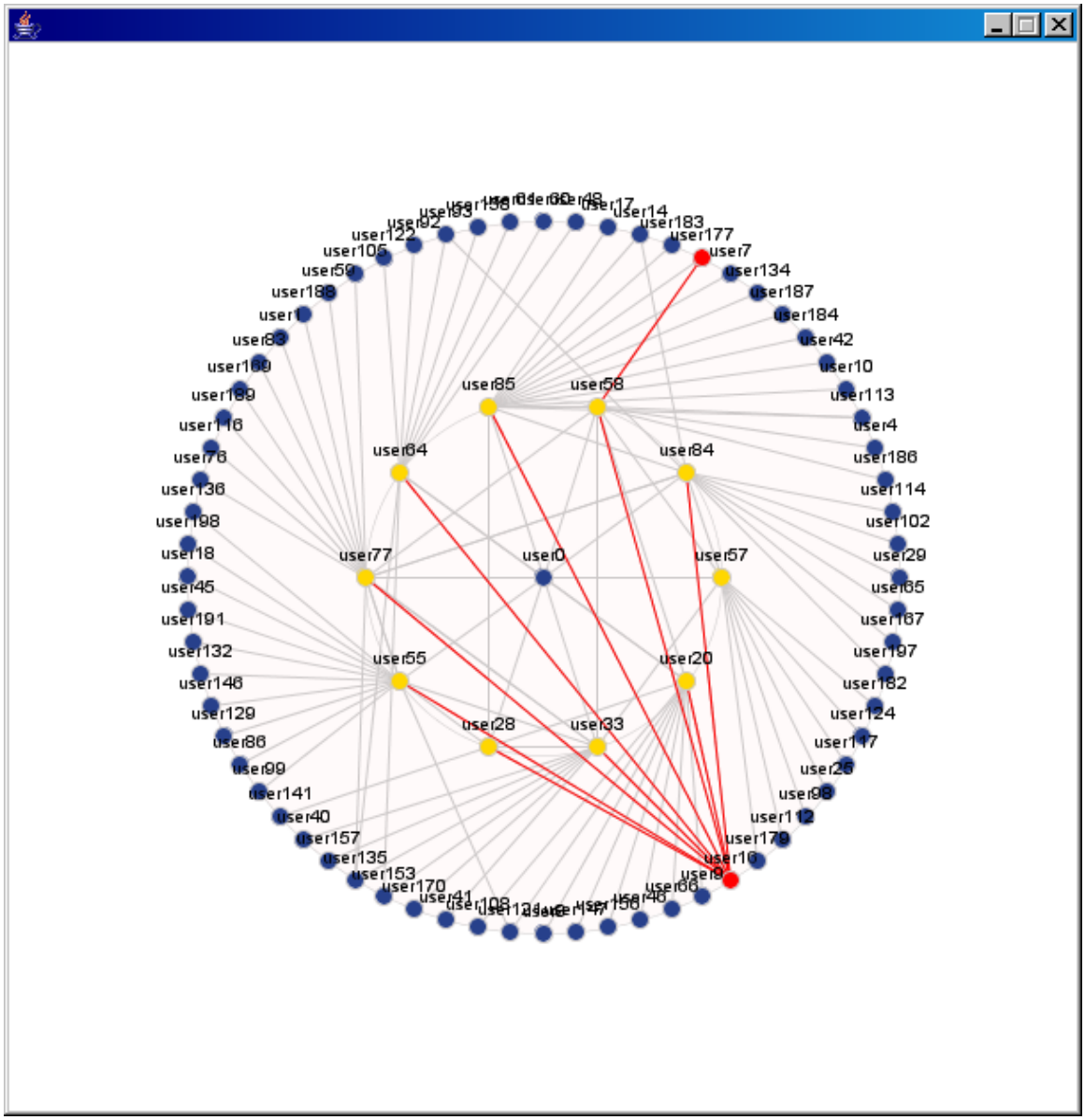
Slika 47: Razpršeni 3D-graf – povečanje prometa

Zanimivi so predvsem viri z velikim povečanjem prometa in visokimi stroški. Samo povečanje prometa za nove naročnike ni zanimivo, ker bo vedno stoodstotno (zgodovina ne obstaja). So pa zanimivi novi naročniki, ki so povzročili izjemno visoke stroške.

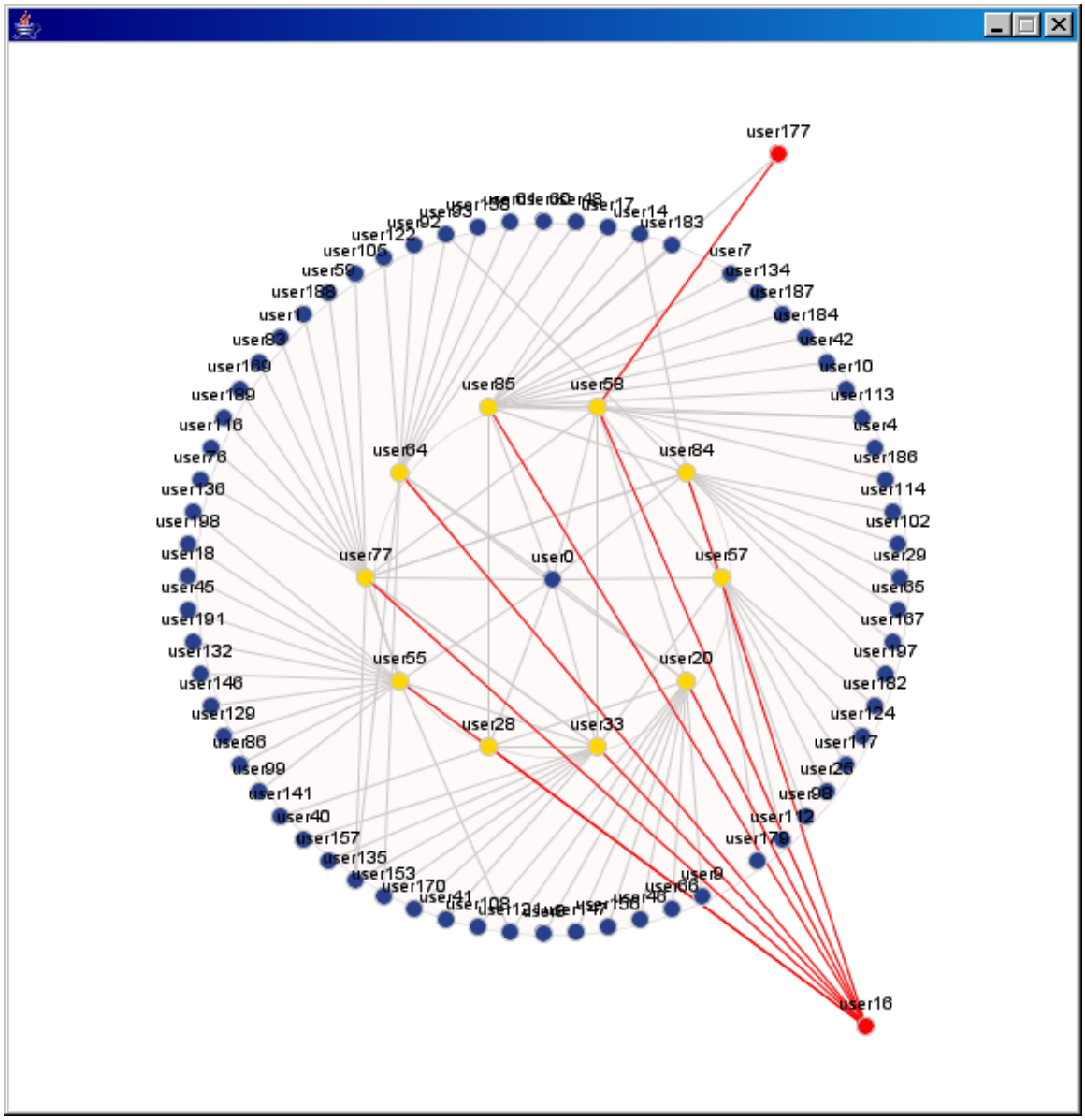
Obravnavanje izjem

Pri obravnavanju suma opisane goljufije je vizualizacija lahko v pomoč pri odkrivanju goljufov, ki so take goljufije že izpeljali. Ko so odkriti (najverjetneje takrat, ko ne plačajo svojih obveznosti), si operater zapomni njihov vzorec vedenja. Ker pričakujemo podoben vzorec tudi pri ponovitvi goljufije, ga lahko uporabimo kot orodje za potrditev suma goljufije.

Na sliki 48 je graf uporabnikov, ki si izmenjujejo klice z osumljenim. Vozlišča predstavljajo uporabnike in povezave klice med njimi. V središče smo postavili osumljenega uporabnika, na prvo krožnico od vozlišča pa uporabnike, s katerimi je osumljeni komuniciral. Na drugo (zunanjo) krožnico so postavljeni uporabniki, ki so komunicirali z uporabniki na prvi krožnici. Uporabniki, pri katerih smo v preteklosti odkrili goljufije, so predstavljeni z rdečimi vozlišči, rdeče povezave iz teh vozlišč pa ponazarjajo odhodne klice. S premikanjem omenjenih vozlišč (Slika 49) lahko izboljšamo sliko in natančneje predstavimo, kam kažejo povezave. Zanimivo je predvsem vozlišče User16, ki je komuniciralo s skoraj identično skupino uporabnikov. V našem primeru lahko z veliko verjetnostjo zaključimo, da gre za istega uporabnika.



Slika 48: Graf osumljenih uporabnikov – začetno stanje



Slika 49: Graf osumljenih uporabnikov – interakcija

Zanimivo je predvsem vozlišče User16, ki je komuniciralo s skoraj identično skupino uporabnikov. V našem primeru lahko z veliko verjetnostjo zaključimo, da gre za istega uporabnika.

10.8.9 Kraja

Gre za netehnično goljufijo, kritični element pa je oprema uporabnika.

Predpriprave

Napadalec stranki ukrade terminal, telefonsko kartico za telefonske govorilnice, telefonske kartice z identifikacijsko številko (angl. remote memory phonecards)[34] ali kakršen koli drugi identifikacijski element, ki dovoljuje klicanje na račun druge osebe.

Delovanje

Napadalec lahko z ukradeno opremo ali informacijo kliče na račun ogoljufane osebe. Pri kraji lahko operater, ko je obveščen, klicanje običajno takoj onemogoči. Čeprav kraje niso najdobičkonosnejše, so med najpogostejšimi goljufijami v manj razvitih državah.

Preprečevanje

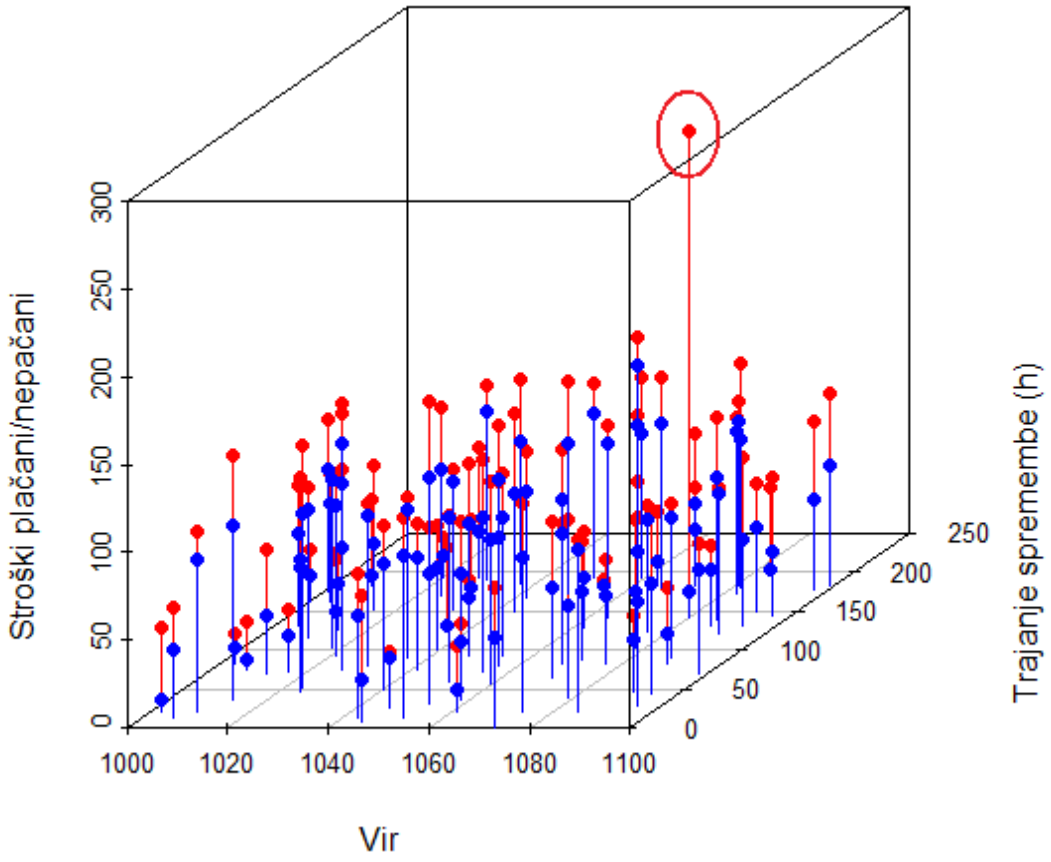
Krajo lahko prepreči le uporabnik sam, največ, kar lahko naredi operater, pa je, da uporabnike izobražuje. Vizualizacija v tem primeru ne more biti v pomoč.

Odkrivanje

Pri odkrivanju iščemo izjeme in spremembe v vedenju naročnika. Znaki so enaki kot pri prej omenjeni goljufiji (glejte razdelek 10.8.1 Kloniranje identifikacijskih elementov ali kraja identitete). Uporabimo lahko prej omenjeno metodo.

Pri odkrivanju je lahko v pomoč tudi razpršeni 3D-graf. Na sliki 50 so prikazani uporabniki, ki so v neki točki spremenili vedenje. To pomeni, da ne kličejo več enakih številk kot prej (z izjemo nekaterih številk, kot so informacije, podpora uporabnikom in podobno). Zanimajo nas atributi, kot so identifikacijska številka vira (os x), koliko časa je minilo od odkrivanja spremembe vedenja (os y), plačani stroški prejšnjega obračunskega obdobja in neplačani stroški trenutnega obračunskega obdobja. Pri vsaki točki modri del predstavlja plačane stroške in rdeči neplačane. Označena točka na sliki predstavlja sumljivega uporabnika, ki izstopa predvsem po neplačanih stroških.

[34] To so kartice, na katerih je napisana identifikacijska številka, ki predstavlja omejeni kredit. Uporabnik jo prebere centrali, preden lahko opravi klic. Informacije s telefonske kartice je mogoče pridobiti s prisluškovanjem, z opazovanjem (s kamerami s povečavo) ali s krajo.

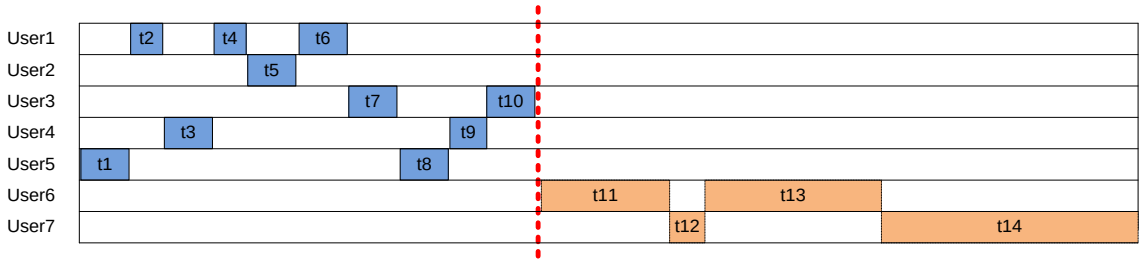


Slika 50: Razpršeni 3D-graf – sprememba vedenja

V tem primeru je atribut Vir nekoliko odvečen, saj ga lahko dobimo na podlagi podrobnosti, ki so na primer dostopne s premikom kazalca miške na omenjeno točko. Tako bi bil enako uporaben že razpršeni 2D-graf.

Obravnavanje izjem

V fazi obravnave dobimo podatke o naročniku, kot so čas spremembe vedenja in časi klicev. Z vizualizacijo na sliki 51 dobimo natančnejšo predstavo o vedenju osumljenega naročnika. Vrstice tabele predstavljajo ponore, rdeča vertikalna črta pa mesto, kjer se je vedenje spremenilo. Na sliki je prikazan zgoščen pogled (kakor da so se klici odvijali drug za drugim), če je treba, pa pogled razširimo z realnim prikazom časa med klici. Prednost prvega je več podatkov na zaslonu, prednost drugega pa boljša predstava vzorcev klicanja.



Slika 51: Tabele – sprememba vedenja

10.8.10 Ustanovitev ponudnika storitev VoIP z namenom goljufije

Gre za netehnično goljufijo, kritični elementi pa so postopki operaterja.

Predpriprave

Ustanovi se nov ponudnik storitev VoIP, novo podjetje, ki deluje kot legalni ponudnik storitev VoIP.

Delovanje

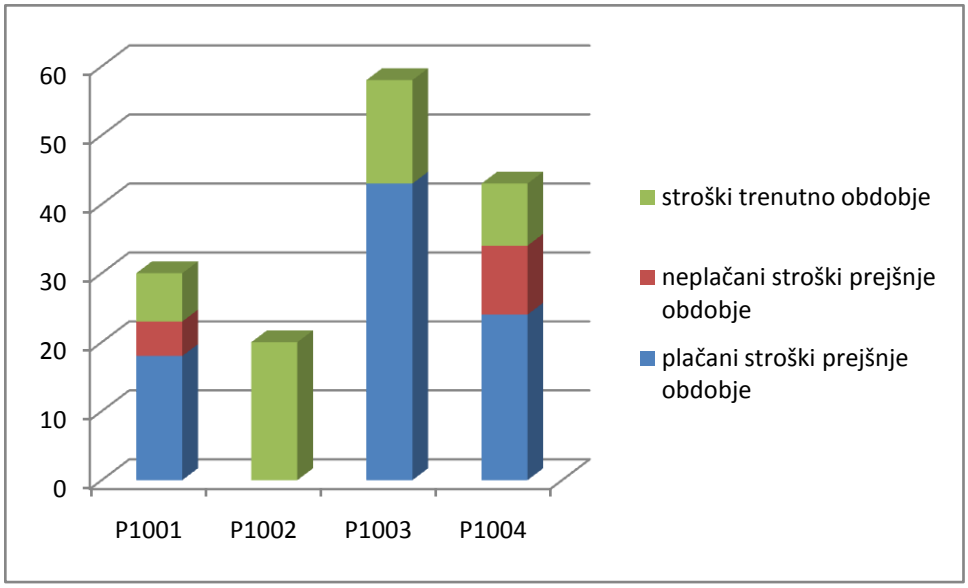
Ker ustanovitev takega podjetja ne zahteva prevelikih vložkov (vsaj ne v primerjavi s klasično telefonijo; za postavitev ogrodja omrežja ponudnika storitev, ki je namenjeno omejenemu število uporabnikov, bi potrebovali nekaj tisoč evrov), si lahko posamezniki ali kriminalne združbe to privoščijo. Ko operaterji (običajno iz tujine) zahtevajo povrnitev stroškov za opravljene storitve, ta podjetja hitro izginejo.

Preprečevanje

Znak, da je prišlo do goljufije, je predvsem neplačevanje računov na strani ponudnika storitev VoIP. Preprečimo jo lahko z natančnejšim preverjanem kredibilnosti prihodnjih poslovnih partnerjev in s strožjimi pogoji poravnavanja obveznosti v prvih mesecih na novo vzpostavljenega poslovnega razmerja. Omejimo lahko na primer število neplačanih prenesenih minut za ponudnike brez potrjene kredibilnosti. Če ponudnik redno plačuje svoje obveznosti, povečamo njegovo mejno vrednost, pri čemer ne potrebujemo posebne vizualizacije.

Odkrivanje

Simptom je čedalje večji dolg ponudnika. Visok delež neplačanih stroškov pove, da obstaja sum goljufije. Ker rizičnih ponudnikov ni veliko, si pri odkrivanju lahko pomagamo s preprostim paličnim grafom (Slika 52).



Slika 52: Palični graf – dolgovi ponudnikov

Identifikacijska številka ponudnika je predstavljena na osi x, stroški iz prejšnjega in trenutnega obdobja pa so predstavljeni z različnimi barvami.

Obravnavanje izjem

V fazi obravnavanja izjem izterjamo plačilo oziroma prekinemo dobavo storitev. Ker gre za očitne kršitve poslovnih pravil, v tej fazi ne potrebujemo posebne vizualizacije.

11 Zaključek

Zdaj lahko odgovorimo na vprašanje iz uvoda – ali in kako lahko vizualizacija prispeva k upravljanju z goljufijami. Da je lahko v pomoč, je bilo nedvoumno potrjeno. Prednosti vizualizacije je več (uporaba izjemnih zmožnosti človeškega vida, učinkovitejša analiza umazanih in tudi nehomogenih podatkov …), vse pa prispevajo dodaten pogled na problematiko, s katero se srečujemo pri upravljanju z goljufijami. Odprto pa ostaja vprašanje, v kolikšni meri je lahko v pomoč. Nedvomno velja, da ne more nadomestiti drugih metod za analizo podatkov, pa tudi, da so na voljo zelo dobri sistemi za upravljanje z goljufijami, ki ne temeljijo na vizualizacijskih metodah za obdelavo podatkov. Torej brez zadržkov lahko rečemo, da vizualizacija ni kritični del sistema, je pa dobrodošel pripomoček. Uporabnost je odvisna tudi od preferenc analitika, kajti nekaterim je vizualizacija bližje oziroma je zanje lažje razumljiva kot za druge. O tem, kako je vizualizacija v pomoč, smo že veliko govorili, na splošno velja, da je v fazi preprečevanja goljufij v pomoč pri analiziranju povratne informacije z zaščitnih elementov, v fazi odkrivanja je v pomoč pri analiziranju velike količine podatkov, v fazi obravnave izjem pa je v pomoč pri analiziranju alarma. Ugotovitve iz magistrske naloge kažejo, da je odgovor pritrdilen; uporaba vizualizacije pri upravljanju z goljufijami je dobrodošla in zaželena.

Pri tem pa se moramo zavedati, da vizualizacijsko orodje ne sme biti statično, ki bi bilo prednastavljeno za uporabo omejene množice togih prikazov, ki ne dopuščajo posebne interakcije analitikov s podatki. Da je orodje uporabno, mora biti izjemno dinamično, analitiku mora ponujati široko paleto pogledov, ki lahko delujejo sočasno in povezano ter temeljijo na skupnih pravilih za filtriranje in interakcijo s podatki. Razvoj takega orodja pomeni določeno investicijo in mora biti opravljen v tesnem sodelovanju z analitiki, ki ga bodo uporabljali. Ker gre za kompleksno orodje, je pogosto težko upravičiti investicijo oziroma najti dovolj interesa med udeleženci, vendar pa trendi porasta škode, ki jo povzročajo goljufije ter velika konkurenca med operaterji, govorijo v prid razvoju takih orodij.

Na podlagi definicije sistema za upravljanje z goljufijami z začetka magistrske naloge in ugotovitev, do katerih smo prišli, lahko izpeljemo naslednjo »dopolnjeno« definicijo, ki vključuje tudi orodja za vizualizacijo podatkov:

Telekomunikacijski sistem za upravljanje z goljufijami je avtomatizirano orodje za preprečevanje, odkrivanje in obravnavanje goljufij. Običajno ima napredni grafični vmesnik, ki vključuje orodja za ročno raziskavo. Pri slednjih se zaradi lažjega obvladovanje podatkov in omejitev ročne analize priporoča uporaba tehnik vizualizacije podatkov.

12 Literatura in viri

[1] K. Cox, S. Eick, G. Wills, and R. Brachman, *Visual Data Mining: Recognizing Telephone Calling Fraud*. Naperville, Illinois: Kluwer Academic Publishers, 1997.

[2] IPDR Organization, *Network Data Management – Usage (NDM-U) For IP-Based Services Service Specification – Voice over IP (VoIP)*. Nantucket, Massachusetts: IPDR Organization, 2002.

[3] A. Trickey, *Simply SS7*. Milpitas, California: SS8 Networks, 2002.

[4] E. Gadaix, *GSM and 3G Security*. Singapore: Black Hat. Conference Singapore, 2001.

[5] J. C. Foster, V. Osipov, N. Bhalla, and N. Heinen, *Buffer Overflow Attacks: Detect, Exploit, Prevent*. ZDA: Syngress Publishing, 2005.

[6] Sipera VIPER Lab, *Report on VoIP Vulnerabilities in WiFi/Dual-mode Phones: Threat Advisories from Sipera VIPER Lab*. Richardson, Texas: Sipera Systems, 2007.

[7] O. A. Abidogun, *Data Mining, Fraud Detection and Mobile Telecommunications: Call Pattern Analysis with Unsupervised Neural Networks*. Cape Town, Južna Afrika: University of the Western Cape, 2005.

[8] R. Horak, *Webster's New World® Telecom Dictionary*. Indianapolis, Indiana: Wiley Publishing, 2007.

[9] R. J. Bolton and D. J. Hand, *Statistical Fraud Detection: A Review*. London, Anglija: Imperial College, 2002.

[10] M. H. Cahill, D. Lambert, J. C. Pinheiro, and D. X. Sun, *Detecting Fraud in the Real World*. ZDA: Technical report, Bell Labs, Lucent Technologies, 2000.

[11] Cerebrus Solutions Limited, *Fraud Primer*. Burlington, Massachusetts: Cerebrus Solutions Limited, 2001.

[12] Communications Fraud Control Association, *Global Telecom Revenues Increase 12% and Fraud Increases 52% from 2003-2005*. Phoenix, Arizona: Communications Fraud Control Association, 2006.

[13] R. Jacobs and I. Booth, *Telecommunications Fraud*. Nairobi, Kenya: Dimension Data, 2007.

[14] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. ZDA: John Wiley & Sons, 2002.

[15] J. H. Van Heerden, *Detecting Fraud in Cellular Telephone Networks*. Stellenbosch, Južna Afrika: University of Stellenbosch, 2005.

[16] H. Kvarnström, E. Lundin, and E. Jonsson, *Combining fraud and intrusion detection - meeting new requirements*. Gothenburg, Švedska: Chalmers University of Technology, 2000.

[17] B. Bihina, *A fraud detection model for Next-Generation Networks*. Champagne Castle, Južna Afrika: Southern African Telecommunication Networks and Applications Conference 2005, 2005.

[18] Dimension Data, *Dimension Data Develops Anti-Fraud Solution for Telcos*. Johannesburg, Južna Afrika: Dimension Data, 2004.

[19] D. Lloyd, *International Roaming Fraud Trends & Prevention Techniques*. Minneapolis, Minnesota: Fair Isaac Corporation, 2003.

[20] H. Kvarnström, *Intrusion and Fraud Detection*. Göteborg, Švedska: SWITS IV Seminar, Vadstena, 2004.

[21] L. Šolc, *Varnost v mobilnem telefonskem omrežju tretje generacije*. Brdo pri Kranju, Slovenija: Štirinajsta delavnica VITEL, 2003.

[22] W. Mazurczyk and Z. Kotulski, *Lightweight security mechanism for PSTN-VoIP cooperation*. Varšava, Poljska: Warsaw University of Technology, 2006.

[23] N. R. Wyler, B. Potter, and C. Hurley, *Aggressive Network Self-Defense*. Rockland, Massachusetts: Syngress Publishing, 2005.

[24] L. Spitzner, *Honeypots: Tracking Hackers*. Boston, Massachusetts: Addison Wesley, 2002.

[25] D. De Capite, *Self-Defending Networks: The Next Generation of Network Security*. Upper Saddle River, New Jersey: Cisco Press, 2006.

[26] P. A. Estévez, C. M. Held, and C. A. Perez, *Subscription Fraud Prevention in Telecommunications using Fuzzy Rules and Neural Networks*. Santiago, Chile: University of Chile, 2005.

[27] B. Bihina, E. Jan, and O. Martin, *Using the IPDR standard for NGN billing and fraud detection*. Sandton, Južna Afrika: Fifth Annual Information Security South Africa Conference, 2005.

[28] International Engineering Consortium, *Fraud Analysis in IP and Next-Generation Networks*. Chicago, Illinois: International Engineering Consortium, 2007.

[29] D. Alessandri, C. Cachin, M. Dacier, O. Deak, and K. Julisch, *Towards a Taxonomy of Intrusion Detection Systems and Attacks*. Zurich, Nemčija: IBM Zurich Research Laboratory, 2001.

[30] K. Lakkaraju, W. Yurcik, R. Bearavolu, and A. J. Lee, *NVisionIP: An Interactive Network Flow Visualization Tool for Security*. Illinois: University of Illinois, 2004.

[31] J. Riordan, *Intrusion Detection*. Zürich, Švica: CNEC-Symposium, 2002.

[32] T. R. Osborne, *Building an Incident Response Program To Suit Your Business*. Bethesda, Maryland: SANS Institute, 2001.

[33] A. Chuvakin and C. Peikari, *Security Warrior*. Sebastopol, California: O'Reilly, 2004.

[34] M. Schiffman, *Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios*. New York, New York: McGraw-Hill, 2001.

[35] R. Albertoni, A. Bertone, U. Demšar, M. De Martino, and H. Hauska, *Knowledge Extraction by Visual Data Mining of Metadata in Site Planning*. Stockholm, Švedska: Scandinavian Research Conference on Geographical Information Science, 2003.

[36] C. Ware, *Information Visualization : Perception for Design*. San Francisco, California: Elsevier, 2004.

[37] T. Munzner, *H3: Laying Out Large Directed Graphs in 3D Hyperbolic Space*. Phoenix, Arizona: IEEE Symposium on Information Visualization, 1997.

[38] E. Kleiberg, H. Wetering, and J. J. Wijk, *Botanical Visualization of Huge Hierarchies*. Eindhoven, Nizozemska: Eindhoven University of Technology, 2001.

[39] S. T. Teoh and K.-L. Ma, *RINGS: A Technique for Visualizing Large Hierarchies*. Davis, California: University of California, 2002.

[40] J. Seo and B. Shneiderman, *Interactive Exploration of Multidimensional Microarray Data: Scatterplot Ordering, Gene Ontology Browser, and Profile Search*. College Park, Maryland: University of Maryland, 2003.

[41] E. Kandogan, *Star Coordinates: A Multi-dimensional Visualization Technique with Uniform Treatment of Dimensions*. Salt Lake City, Utah: IEEE Information Visualization Symposium, 2000.

[42] M. Hearst, *Information Visualization and Presentation*. Berkeley, California: University of California, 2004.

[43] P. C. Saunders and V. Interrante, *An Investigation into Color Preference for Color Palette Selection in Multivariate Visualization*. Minneapolis, Minnesota: University of Minnesota, 2005.

[44] C. G. Healey, *Choosing Effective Colours for Data Visualization*. San Francisco, California: 7th conference on Visualization '96, 1996.

[45] E. R. Tufte, *Envisioning Information*. Cheshire, Connecticut: Graphics Press, 1998.

[46] D. D. Woods and J. C. Watts, *Handbook of Human-Computer Interaction: How not to have to navigate through too many displays*. Amsterdam, Nizozemska: Elsevier Science, 1997.

[47] P. Irani, M. Tingley, and C. Ware, *Using Perceptual Syntax to Enhance Semantic Content in Diagrams*. Washington, District of Columbia: IEEE Computer Graphics and Applications, Vol. 21, 2001.

[48] S.-T. Teoh, S. Ranjan, A. Nucci, and C. Chuah, *BGP Eye: A New Visualization Tool for Realtime Detection and Analysis of BGP Anomalies*. Alexandria, Virginia: 3rd International Workshop on Visualization for Computer Security, 2006.

[49] M. Q. Wang, A. Woodruff, and A. Kuchinsky, *Guidelines for Using Multiple Views in Information Visualization*. Palermo, Italija: Working conference on Advanced visual interfaces, 2000.

[50] AIS SpA, *The VisualMine Image Gallery*. Milano, Italija: AIS SpA, 2008.

[51] J. R. Goodall, W. G. Lutters, P. Rheingans, and A. Komlodi, *Preserving the Big Picture: Visual Network Traffic Analysis with TNV*. Minneapolis, Minnesota: IEEE Visualization for Computer Security, 2005.

[52] K. R. Quinn, *Data Visualization: Gaining Perspective*. New York, New York: Information Builders, 2006.

[53] S. Lau, *The Spinning Cube of Potential Doom*. San Francisco, California: Lawrence Berkeley National Laboratory, 2003.

[54] V. Batagelj, E. Pavletič, M. Zaveršnik, and S. Korenjak, *Clustering Large Datasets and Visualizations of Large Hierarchies and Pyramids Symbolic Data Analysis Approach*. Lyon, Francija: Workshop on Symbolic Data Analysis: Theory, Software and Applications for Knowledge Mining, 2000.

[55] A. Kobsa, *An Empirical Comparison of Three Commercial Information Visualization Systems*. San Diego, California: IEEE Symposium on Information Visualization, 2001.

[56] B. Shneiderman, *The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations*. College Park, Maryland: University of Maryland, 1996.

[57] K. Stockinger, J. Shalf, K. Wu, and W. Bethel, *Query-Driven Visualization of Large Data Sets*. Berkeley, California: University of California, 2005.

[58] D. A. Keim and H.-P. Kriegel, *VisDB: Database Exploration Using Multidimensional Visualization* . Washington, District of Columbia: IEEE Computer Graphics and Applications, 1994.

[59] B. Fry and C. Reas. (2008) Processing. [Online]. http://processing.org/

[60] F. Ledermann. (2008) Parvis. [Online]. http://home.subnet.at/flo/mv/parvis/

[61] R. Ihaka and R. Gentleman. (2008) R Project. [Online]. http://www.r-project.org/

[62] J. O'Madadhain, D. Fisher, T. Nelson, S. White, and Y.-B. Boey. (2008) JUNG. [Online]. http://jung.sourceforge.net/

[63] J. O'Madadhain, D. Fisher, P. Smyth, S. White, and Y.-B. Boey, *Analysis and Visualization of Network Data using JUNG*. ZDA: Journal of Statistical Software, 2005.

[64] M. Ward and E. Rundensteiner. (2008) Xmdv Tool. [Online]. http://davis.wpi.edu/~xmdv/

[65] B. Fry, *Visualizing data*. Sebastopol, California: O'Reilly Media, 2007.

[66] J. Quirke, *Security in the GSM system*. Australija: AusMobile, 2004.

[67] Spy Blog, *Iraq insurgents intercepting British soldiers' mobile phone data - hype?*. Združeno kraljestvo Velike Britanije in Severne Irske: Spy Blog, 2006.

[68] Gsm Solutions, *SIM Card Cloning Guide*. Dublin, Irska: Gsm Solutions, 2004.

[69] P. Jungck, *VoIP Fraud: Scenarios and Solutions*. Norwalk, Connecticut: Technology Marketing Corporation, 2004.

[70] U. Meyer and S. Wetzel, *A Man-in-the-Middle Attack on UMTS*. Philadelphia, Pennsylvania: ACM Workshop on Wireless Security (WiSe 2004), 2004.

[71] M. Tory and T. Möller, *Human Factors In Visualization Research*. Washington, District of Columbia: IEEE Transactions on Visualization and Computer Graphics, Vol. 10, 2004.

[72] M. Friendly, *Re-Visions of Minard*. Toronto, Ontario: York University, 1999.