CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Zabavni sadržaji preko Interneta kao izvor opasnosti od napadača

CCERT-PUBDOC-2008-08-236

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Internet je radikalno promijenio svakodnevnicu. Deseci milijuna ljudi ga redovito koriste diljem svijeta pregledavajući web stranice, čitajući i šaljući elektronsku poštu, kupujući, slušajući glazbu, gledajući televiziju ili koristeći razne društvene servise. Nažalost, među njima se nalaze i zlonamjerni korisnici koji tehnologiju koriste kako bi vrebali ostale korisnike, izvodili različite prijevare zbog vlastitog zadovoljstva, ali i osobne materijalne koristi. Unatoč činjenici da je Internet iznimno koristan kada treba pronaći neku informaciju, ima edukativnu vrijednost, a isto tako može poslužiti i za zabavu, neupitno je da je Internet i izvor opasnosti.

Nove tehnologije i širokopojasne veze pomogle su u populariziranju Internet igara (eng. *online games*) i ostalih oblika zabave, poput socijalnih mreža i klađenja. Dok igrači ulažu značajne količine vremena i novca u igre radi osobnog zadovoljstva, neki korisnici vide priliku za podvale i/ili (ilegalnu) zaradu. Igrači koji se upuštaju u takve aktivnosti trebali bi biti svjesni dvojakog rizika: tehnološkog i socijalnog. To uključuje:

- rizik od utjecaja nepoznatih igrača koji bi mogli navesti korisnika na otkrivanje povjerljivih osobnih ili financijskih informacija,
- rizik od nedozvoljenog pristupa napadača korisniku računala i
- rizik od virusa, trojanskih konja, računarskih crva i *spyware* programa.

Iako se u igrama iskorištavaju najnovija tehnološka dostignuća na području umjetne inteligencije, računalne grafike, interakcije s korisnikom, tehnike programiranja, tehnike distribuiranog i mrežnog računarstva itd., često se nedovoljno pažnje posvećuje sigurnosnim pitanjima, posebice kada se radi o igrama namijenjenim igranju preko Interneta.

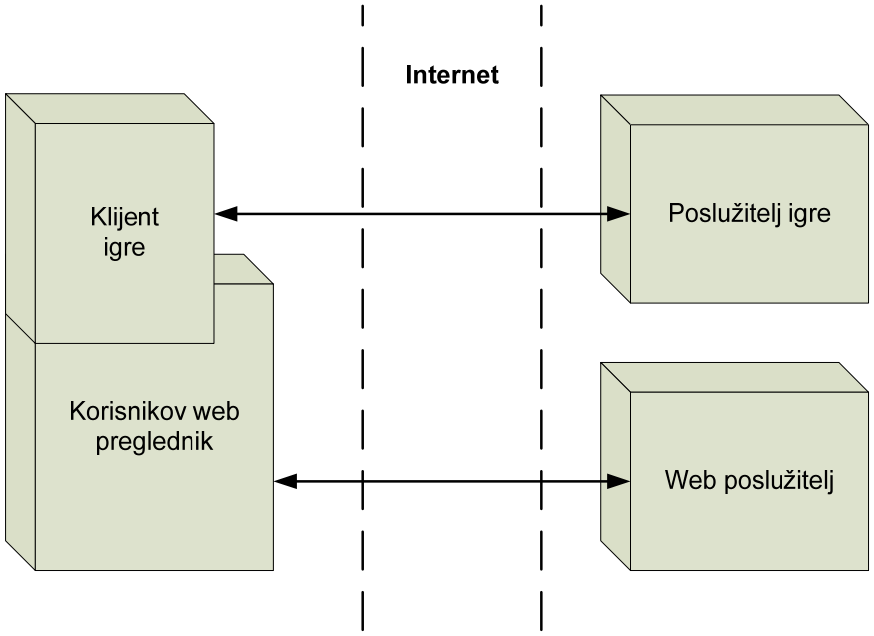
U dokumentu je opisan koncept igranja preko Interneta, naznačeni su najznačajniji propisi i zakoni o zaštiti podataka te pravila sigurnosti, tehnološki i socijalni rizici kao i mjere zaštite do napada. Također, dani su i konkretni primjeri ranjivosti nekoliko popularnih igara. Zadatak dokumenta je približiti korisniku, pojasniti i omogućiti razumijevanje problematike vezane uz sigurnost igranja preko Interneta, ali i korištenja ostalih *online* servisa namijenjenih zabavi.

2. Zabavni sadržaji na Internetu

Zabavnih sadržaji na Internetu uključuju, pored drugih sadržaja, i *online* igre. One pripadaju skupini igara namijenjenih igranju preko kompjuterskih mreža. Ekspanzija računalnih igara pratila je napredak računalnih mreža: počevši od lokalnih sve do Interneta.

Online igre kreću od jednostavnih kojima se upravlja putem tekstualnog sučelja, a raspon im seže sve do grafički orijentiranih, vrlo zahtjevnih i složenih igara koje uključuju čitav virtualni svijet u kojemu se nalazi velik broj igrača istovremeno. Mnoge Internet igre današnjice razvijaju vlastite *online* zajednice (eng. *community*) koje ih odmiču daleko od igara za jednog ili manji broj igrača, kakve su, uglavnom, bile u začecima. Povećanje popularnosti Flash i Java tehnologija rezultiralo je web stranicama koje implementiraju zvuk, video i niz novih funkcionalnosti za korisnika. Nova mogućnost, ugradnja modula za reprodukciju Flash sadržaja u Microsoft Internet Explorer (i ostale web preglenike), smatra se prekretnicom u razvoju Interneta, koji nakon toga počinje u sve većoj mjeri nuditi i tzv. zabavu na zahtjev (eng. *entertainment on demand*). Arhitektura takvog sustava za *online* igranje prikazana je slikom *Slika 1*.

Na taj se način nekoliko igara uvrstilo u sam vrh Internet zabave, a najpoznatije među njima su Second Life, World of Warcraft, Final Fantasy te Guild Wars. Posljednje navedena igra dostupna je igračima bez ikakve novčane naknade, dok se za igranje preostalih igara plaća mjesečni iznos. Postoje i inačice koje se nalaze između dviju opisanih vrsta: besplatno igranje, ali se uz dodatna plaćanja dobiva i dodatan sadržaj.



Slika 1: Odnos klijenata i poslužitelja u arhitekturi većine *online* igara

Od svih vrsta *online* igara, valja izdvojiti sljedeće dvije vrste:

- igre za web preglednik (eng. *browser games*) koje koriste preglednik kao klijent aplikaciju i
- *online* igre za više (stotina pa i tisuća) igrača (eng. *MMOG – Massively multiplayer online games*) koje se dijele na:
    - MMORPG (eng. *Massively multiplayer online role-playing game*) – u kojoj igrač preuzima ulogu virtualnog lika iz igre,
    - MMORTS (eng. *Massively multiplayer online real-time strategy*) – strategija u realnom vremenu,
    - MMOFPS (eng. *Massively multiplayer online first-person shooter)* – „pucačina“ iz prvog lica,
    - MMOSG (eng. *Massively multiplayer online social game*) – igra namijenjena druženju odnosno socijalnim aktivnostima.

Treba napomenuti da i MMOG igre mogu kao klijent aplikaciju koristiti web preglednik što olakšava distribuciju klijentskih aplikacija, ali i djelomično ograničava mogućnosti igre.

Većina igara temelji se na *online* likovima koji sudjeluju u različitim avanturama. Unatoč svoj toj virtualnosti, doticaj sa stvarnim svijetom postoji. Igrači, primjerice, prodaju virtualnu robu za pravi, realan novac na Internet mjestima namijenjenima razmjeni realnih dobara, poput eBay aukcija. U nekim igrama igrači pak u virtualnom svijetu koriste stvarni novac kako bi načinili ili kupili virtualnu robu u *online* svijetu. Ovakav pristup je stvorio mogućnosti za nove tipove kriminalnih aktivnosti. Takve se aktivnosti jednim imenom nazivaju virtualnim zločinom (eng. *virtual crime, in-game crime*).

Pored opisanih, vrlo se često igraju i kartaške igre, *casino* igre i različite druge igre na sreću kao i *online* kladionica. Primjeri sučelja takvih igara dani su na slici *Slika 2*. I ove igre su također na meti napadača koji u većini slučajeva pokušavaju ostvariti materijalnu korist na nekorektne ili čak zakonom zabranjene načine.

Slika 2: Grafička korisnička sučelja za *online* kockanje

Zabavni sadržaji uključuju i servise za *online* druženje (društvene mreže, eng. *social network service*) pomoću kojih nastaju virtualne zajednice (eng. *virtual community, e-community or online community*). Zadatak im je omogućiti korisnicima različite načine komunikacija i osobne prezentacije, a u posljednje vrijeme ovakve usluge bilježe značajan rast broja korisnika. Najpoznatiji među njima na svjetskoj razini su Facebook, LinkedIn, MySpace i Bebo. Postoje i domaće usluge ovog tipa u koje se ubrajaju Iskrica, Trosjed i Tulumarka. Ilustracije radi, web stranice nekih servisa dane su sljedećom slikom.

Slika 3: Početne stranice Facebook, MySpace i Iskrica servisa

2.1. Varanje u online igrama

Pojam varanja star je koliko i pojam igranja. Varanje bi se moglo opisati kao ponašanje igrača koje ima za svrhu stjecanje nedozvoljene prednosti ili neke druge koristi. Prema radu, „How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It" (Matt Pritchard, 2000.g.), *online* varanje moguće je podijeliti u šest kategorija:

- lažni refleksi (eng. *reflex augmentation*) – nedozvoljena modifikacija igre (aplikacije) u svrhu zamjene odnosno poboljšanja reakcija igrača, a time i postizanja boljih rezultata;
- autoritativni klijenti (eng. *authoritative clients*) – iskorištavanje modificiranih klijentskih aplikacija koje su programski preoblikovane (reverznim inženjeringom) kako bi omogućile slanje zlonamjerno oblikovanih poruka koje odredišni klijenti uvažavaju;
- nedozvoljen pristup informacijama (eng. *information exposure*) – pristupanje potencijalno osjetljivim informacijama kompromitiranjem klijentskih aplikacija;
- kompromitiranje poslužitelja (eng. *compromised servers*) – promjena konfiguracije poslužitelja na način koji zlonamjernom korisniku omogućava nedozvoljenu prednost u igri;
- propusti programske podrške (eng. *bugs and design loopholes*) – iskorištavanjem propusta u oblikovanju programske podrške moguće je steći nedozvoljenu prednost poput pristupa računalu korisnika ranjive klijentske aplikacije;
- slabosti okoline (eng. *environmental weaknesses*) – iskorištavanje sklopovlja i uvjeta izvođenja programa u svrhu izvođenja različitih malverzacija.

3. Rizici Internet zabave

Rizik kojim se izlažu igrači računalnih igara sličan je onome kojemu su izloženi ostali korisnici računala, ali treba biti svjestan da *online* igre donose i novi, drugačiji, u nekim segmentima neuobičajeni rizik – virtualni kriminal. Zanimljivost koja ide u prilog činjenici da je virtualni kriminal vrlo ozbiljno shvaćen jest ta da su neke zemlje oformile posebne policijske odrede koji se bave sprječavanjem isključivo ovakvog oblika kriminala. Južna Koreja jedna je od takvih zemalja. U prvoj polovici 2003. godine kod njih je zabilježeno 22 000 virtualnih prekršaja.

Sigurnosni nedostaci pokazali su se čestima kod MMORPG igara. Naime, MMORPG igre temeljene su na arhitekturi klijent-poslužitelj. Poslužitelji moraju u stvarnom vremenu omogućiti interakciju stotina, a nerijetko i tisuća korisnika, što predstavlja iznimno velik broj klijentskih aplikacija spojenih na poslužitelje. Zbog toga se smatra da je upravo ova vrsta igara najpogodnija za pronalazak postojećih, ali i nastanak novih sigurnosnih nedostataka.

Važnost rješavanja sigurnosnih problema pojačava činjenica da su *online* igre postale velik izvor zarade. Najpopularnija MMORPG igra na svijetu, World of Warcraft (ili kraće WoW), ima više od osam milijuna korisnika od kojih svaki plaća nešto više od deset dolara mjesečno, ovisno o načinu plaćanja cijena iznosi 13 do 15 USD, za održavanje svog korisničkog računa. Očekuje se da će već do 2009. ovo tržište doseći 12 milijardi dolara. Mnoge igre, budući da se zasnivaju na prikupljanju i trgovanju virtualnim dobrima, imaju BDP (bruto domaći proizvod, eng. *GDP - gross domestic product*) nerijetko veći od prihoda manjih država. Primjerice, igra Everquest 2003. godine zabilježila je BDP po glavi (virtualnog) stanovnika veći od 2000 dolara, izjednačavajući se tako s Hrvatskom, Tunisom i Vijetnamom. Navedena činjenica dovodi do stvaranja jedne skupine igrača koja je koncentrirana na prihode, a ne na zadovoljstvo, što je inicijalna svrha same igre. Poznato je da, gdje god je novac prisutan, pojavljuje se i kriminal. Upravo zato nije rijetkost niti postojanje korisnika koji se igranjem, a neki i varanjem u igrama, bave i žive od toga. Američka Služba Sigurnosti (eng. *Secret Service*) objavila je kako se *online* igre poput Second Life i World of Warcraft koriste i za 'pranje' novca.

Općenito, što se tiče kriminala u *online* igrama, očekuje se porast broja virtualnih bandi i kriminalaca. Na primjer, 2005. godine je 56 milijuna dolara potrošeno samo na reklame u igrama, a predviđa se rast od 70% godišnje, što dovodi do brojke od jednu milijardu dolara do 2010. godine.

Ilustracije radi, sljedeća tablica prikazuje popularne Internet igre u Americi početkom 2007. godine (prema podacima tvrtke Hitwise).

Broj	Prema tržišnom udjelu	Prema vremenu provedenom u igranju
1.	Pogo.com	IamGame.com
2.	Yahoo! Games	BrainKing.com
3.	RuneScape	Hogwarts Live
4.	Yahoo! Games Downloads	Eternal Kingdoms
5.	MSN Games	Hogwarts Extreme
6.	Neopets.com	Cyber Arcade World
7.	Gamefaqs.com	Gothador
8.	Miniclip Games	Gang-Wars
9.	Addicting Games	Game Bonus
10.	Yahoo! Fantasy Sports	The Pokemon Crater

Tablica 1: Poredak *online* igara u Americi

Kod društvenih servisa javlja se rizik od preuzimanja i kompromitiranja identiteta. Razvojem aplikacija za pojedine servise i navođenjem korisnika na dodavanje takvih aplikacija u svoj korisnički račun, napadači najčešće izvode spomenute zlonamjerne aktivnosti.

Bez obzira na vrstu *online* zabave, svi korisnici podložni su tehnološkim i socijalnim rizicima, pojašnjenima u nastavku.

3.1. Tehnološki rizik

Igre preko Interneta mogu uključivati tehnološke rizike koji pak mogu imati utjecaja na korisnika ponekad i u značajnoj mjeri s ozbiljnijim posljedicama. Upravo je zato vrlo korisno poznavati te rizike.

3.1.1. Virusi i crvi

Računalni virusi i crvi do korisnikovog računala mogu dospjeti putem privitaka elektroničke pošte ili prijenosom nepoznatih datoteka alatima za razmjenu poruka u stvarnom vremenu (eng. *IM – Instant messaging*). Također, ovakve aplikacije mogu biti sakrivene u datotekama igara koje korisnik preuzme s Interneta ili u nekoj drugoj programskoj podršci koju korisnik preuzme na svoje računalo i pokrene bez prethodne provjere odgovarajućim antivirusnim alatom.

3.1.2. Zlonamjerna programska podrška

Virusi i crvi se mogu iskoristiti za instaliranje drugih zlonamjernih programa na korisnikovo računalo. Napadači mogu, korištenjem društvenih mreža, elektroničke pošte ili čak glasovnom komunikacijom, uvjeriti žrtvu na otvaranje posebno oblikovanih web stranica ili priloga elektroničke pošte koji sadržavaju zlonamjerne programe. Na taj način napadač može stvoriti pogodne okolnosti za izvođenje protuzakonitih aktivnosti na žrtvinom računalu.

3.1.3. Nesigurni poslužitelji igara

Promatrano sa strane igrača, ukoliko je programska podrška poslužitelja u sigurnosnom kontekstu kompromitirana, računala koja su mrežom spojena na poslužitelj također su u opasnosti od kompromitiranja. Općenito vrijedi da bilo koja igra temeljena na mrežnim uslugama donosi sa

sobom stanoviti količinu rizika, osobito u usporedbi s igrama koje ne zahtijevaju povezivanje s drugim računalom ili Internetom. Iskorištavanjem ranjivosti zlonamjerni korisnici stječu mogućnosti za udaljenu kontrolu žrtvinog računala, a mogu iskoristiti isto računalo kako bi zarazili neko treće računalo ili instalirali zlonamjeran program poput trojanskog konja, *adware* i *spyware* aplikacija. Također, ovakve propuste može se iskoristiti i za neovlašten pristup osobnim i potencijalno osjetljivim informacijama na računalu žrtve.

S druge strane, poslužitelji igara susreću se s istim potencijalnim problemima kao i poslužitelji bilo koje druge namjene. Napadač može ostvariti nedozvoljen pristup, onemogućit njegov ispravan rad i sl. ukoliko poslužitelj nije ispravan u sigurnosnom kontekstu.

3.1.4. Propusti u razvoju igara

Neki protokoli namijenjeni komunikaciji između pojedinih podsustava igre mogu biti razvijeni na ne potpuno ispravan način što omogućava napadaču različite malverzacije. Također, podsustavi igara mogu sadržavati različite propuste, počevši od neispravnog dizajna do logičkih pogrešaka i pogrešaka u kodiranju. Kao posljedica toga, na korisnikovom računalu mogu se pojaviti sigurnosne rupe. One su pogodne za zlonamjerne korisnike koji na taj način stječu mogućnosti neovlaštenog pristupa žrtvinom računalu što za sobom, između ostalog, povlači i mogućnost pristupa potencijalno osjetljivim informacijama.

3.2. Socijalni rizik

Napadači mogu iskoristiti danas uobičajene načine komunikacije tijekom igranja igre za neovlašten pristup žrtvinom računalu, odnosno za iskorištavanje sigurnosnih nedostataka. Uobičajen cilj svih napadača obuhvaća:

- prikupljanje osobnih podataka žrtve,
- krađu identiteta,
- krađu podataka o kreditnoj kartici i
- pristup djeci od koje je najlakše 'izvući' korisne podatke (naivnost i neiskustvo djece mogu napadaču biti od koristi kod prikupljanja informacija o članu obitelji ili nekoj drugoj osobi o kojoj dijete posjeduje informacije).

3.2.1. Socijalni inženjering

Napadači imaju cilj navesti žrtvu na instaliranje zlonamjerne programske podrške pomoću koje oni stječu ovlasti nad žrtvinim računalom. Stjecanjem naklonosti žrtve, moguće je izvoditi različite aktivnosti s područja socijalnog inženjeringa, primjerice usmjeriti žrtvu na preuzimanje zlonamjerne inačice neke igre i sl.

3.2.2. Krađa identiteta

Ukoliko zlonamjeran korisnik skupi dovoljno podataka o žrtvi koristeći informacije iz profila igara i drugih izvora, može ih iskoristiti za stvaranje lažnih korisničkih računa ili za pristup postojećim računima korisnika. Jedan takav slučaj zabilježen je u Južnoj Koreji kada su preuzeti identiteti tisuća igrača. Pretpostavlja se da je glavni razlog bio pokušaj zarade prodavanjem virtualnih oružja i druge robe iz nekih igara.

3.2.3. Sheme zaštite

Unutar Internet igara uočena je i pojava 'reketarenja'. Uobičajen pristup napadača, kao što je slučaj i u stvarnom svijetu, je zastrašivanje slabijih igrača ili prijetnja negativnim posljedicama po njih ukoliko ne plate virtualnim ili stvarnim novcem za 'zaštitu'.

3.2.4. Internet prostitucija

Iako djeluje neizvedivo, ipak je zabilježen slučaj kada je sedamnaestogodišnjak zarađivao na tzv. *cybersex* uslugama unutar igre The Sims Online. Njegov korisnički račun je izbrisan, ali nije snosio pravne posljedice.

3.2.5. Virtualni prepadi

Termin tzv. virtualnih prepada je stvoren kada su igrači igre Lineage II koristili tzv. botove (eng. *bots*). Botovi su aplikacije razvijene sa specifičnim zadatkom prikupljanja informacija, napada na likove drugih korisnika i sl. Japanska policija 2005. godine uhitila je studenta na razmjeni koji je na taj način preuzimao virtualne likove drugih korisnika i prodavao njihova stečena dobra u svrhu zarade u *online* svijetu.

4. Propisi i zakoni o zaštiti privatnosti

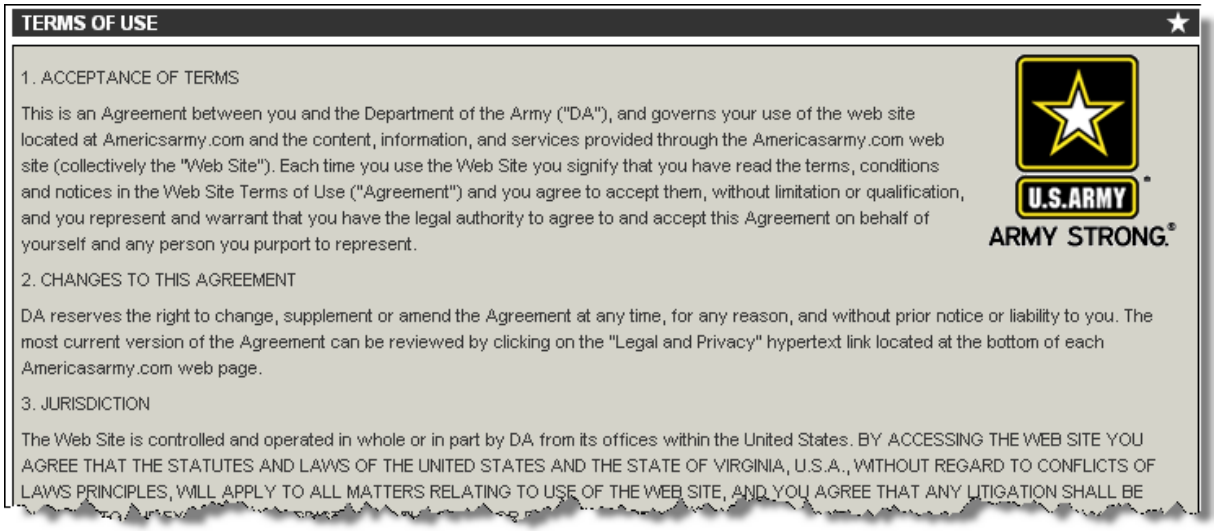
Tvrtke koje razvijaju računalne igre i drugi relevantni sudionici u razvoju i distribuciji igara stvorili su mnoštvo pravnih dokumenata vezanih uz licenciranje njihovih proizvoda. Ta su pravila razvijena u obliku dogovora s krajnjim korisnikom (eng. *EULA – End User License Agreement*) i uvjeta uporabe (eng. *TOU – Terms of Use*). Riječ je o dugim pravničkim tekstovima koje korisnici uglavnom ne čitaju.

Pravna zaštita *online* privatnosti u Republici Hrvatskoj uređena je većim brojem zakona. Naime, ne postoji jedan zakon ili kodeks u kojemu se mogu naći sve odredbe koje reguliraju to područje. Ustav RH štiti pravnu zaštitu osobnog i obiteljskog života, slobodu i tajnost dopisivanja te sigurnost i tajnost osobnih podataka. Nadalje, svakome se jamči štovanje i pravna zaštita njegova osobnog i obiteljskog života, dostojanstvo ugleda i časti, a sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Zakon o zaštiti osobnih podataka uređuje zaštitu osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u RH. Njegova svrha je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Osobni podatak se definira kao svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati, a obrada osobnih podataka je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim ili drugim sredstvima.

Kod prikupljanja osobnih podataka o korisnicima, zakon nalaže da ih se mora informirati o razlozima prikupljanja tih podataka, vremenskom ograničenju pohrane podataka, vrstama obradbe i sličnome. Svi podaci moraju imati dobro obrazložene razloge prikupljanja, a zakoni uglavnom inzistiraju na minimalnoj količini podataka potrebnoj za uspješno obavljanje obrade. Također, korisniku se mora omogućiti naknadna promjena i uvid u dane informacije. Trajnost podataka ograničena je svrhom njihova prikupljanja; nakon što je ona ispunjena, podatke treba obrisati. Ukoliko su oni i dalje potrebni radi statističke ili neke druge obrade, nad tim podacima mora se ukloniti svaka mogućnost povezivanja s identitetom ispitanika. Čuvanje podataka mora biti strogo kontrolirano kako ne bi došlo do krađe, a time i mogućnosti njihova neovlaštenog iskorištavanja.

Vezano uz krajnjeg korisnika, zakon je vrlo jasan i omogućava mu sve ovlasti kojima se onemogućava korištenje privatnih informacija bez znanja samog korisnika. Korisnik, svaki puta kada se zatraže njegovi podaci, ima pravo zatražiti i dobiti informacije vezane uz razloge prikupljanja njegovih podatka, način njihova korištenja, osobe koje će imati pristup podacima i duljinu pohrane tih podataka.

Za nepoštivanje takvih zakona najčešće su predviđene novčane kazne reda veličine tisuća ili desetaka tisuća kuna.



TERMS OF USE

1. ACCEPTANCE OF TERMS

This is an Agreement between you and the Department of the Army ("DA"), and governs your use of the web site located at Americsarmy.com and the content, information, and services provided through the Americasarmy.com web site (collectively the "Web Site"). Each time you use the Web Site you signify that you have read the terms, conditions and notices in the Web Site Terms of Use ("Agreement") and you agree to accept them, without limitation or qualification, and you represent and warrant that you have the legal authority to agree to and accept this Agreement on behalf of yourself and any person you purport to represent.

U.S.ARMY
ARMY STRONG.®

2. CHANGES TO THIS AGREEMENT

DA reserves the right to change, supplement or amend the Agreement at any time, for any reason, and without prior notice or liability to you. The most current version of the Agreement can be reviewed by clicking on the "Legal and Privacy" hypertext link located at the bottom of each Americasarmy.com web page.

3. JURISDICTION

The Web Site is controlled and operated in whole or in part by DA from its offices within the United States. BY ACCESSING THE WEB SITE YOU AGREE THAT THE STATUTES AND LAWS OF THE UNITED STATES AND THE STATE OF VIRGINIA, U.S.A., WITHOUT REGARD TO CONFLICTS OF LAWS PRINCIPLES, WILL APPLY TO ALL MATTERS RELATING TO USE OF THE WEB SITE, AND YOU AGREE THAT ANY LITIGATION SHALL BE

Slika 4: Isječak iz uvjeta korištenja vezanih uz igru America's Army (dostupno na http://www.americasarmy.com/army/privacy.php)

4.1. Zakoni u online igrama

Federalni zakon u Americi (eng. *CFAA - Computer Fraud and Abuse Act*) donesen 1986. godine predviđa šest vrsta računalnog kriminala od kojih svaki uključuje i nedozvoljen pristup računalima drugih korisnika. Zakon je vrlo jasan glede neovlaštenog pristupa računalima preko računalne mreže: neovlašten pristup nije dopušten.

Iste godine Kongres Sjedinjenih Država (eng. *ECPA - Electronic Communications Privacy Act*) izglasao je zakon koji uvodi mogućnost kažnjavanja neovlaštenog prikupljanja mrežnog prometa (eng. *network sniffing*) i drugih oblika 'presretanja' podataka. I ovaj zakon vrlo je jasan u svojim odrednicama o zabrani opisanih aktivnosti.

Nasuprot spomenutima, američki zakon vezan uz sigurnost u *online* igrama nije potpuno jasan. Često nije moguće odrediti što je legitimno, ili važnije, što nije legitimno. Zakonske odrednice vrlo je teško precizno definirati iako se 'hakerske' sposobnosti gotovo izravno pretaču u novac nedozvoljenim prikupljanjem virtualnih dobara, uočavanjem sigurnosnog propusta igre ili stvaranjem bot aplikacije namijenjene preuzimanju virtualnih likova. Postavlja se pitanje na koji način odrediti i povući jasnu crtu koja će dijeliti legitimne od nelegitimnih aktivnosti. Primjerice, promijeniti datoteku s popisom igrača s najvećim ostvarenim brojem bodova (eng. *high score*) u igri smije svatko na svom računalu i to se ne smatra nelegitimnim djelom. Ukoliko su dijelovi neke mrežne igre na korisnikovom računalu, postavlja se pitanje smije li ih on slobodno mijenjati, pogotovu ako se radi o virtualnim dobrima koja je moguće pretočiti u novac. Usko vezano s tim pitanjem postavlja se i pitanje narušavanja privatnosti drugih osoba tj. otuđivanja njihovih korisničkih računa i sl. Opisana EULA pravila pokazala su se nedovoljno čvrstima za održavanje na sudu. Razlog tomu je mogućnost prigovora na brojne klauzule sadržane u ugovoru, ali ipak ne na sve. To ponajviše ovisi o konkretnom slučaju. Nejasni i nedorečeni zakoni i propisi, s obzirom na sve veće količine novca koje kruže virtualnim svijetom, stvaraju i stvarati će vrlo teške probleme sve dok ne postanu otporni na mogućnosti dvojakih tumačenja, nejasnoće i dr.

Kazneni zakon Republike Hrvatske inkriminira povredu *online* privatnosti u nekoliko kaznenih djela, a to su: povreda tajnosti pisama i drugih pošiljaka; nedozvoljena uporaba osobnih podataka; povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava; računalno krivotvorenje i računalna prijevara. Privatnost u *online* zabavi u potpunosti podliježe prethodno navedenim regulativama.

5. Mjere zaštite

Igranje igara preko Interneta (kao i korištenje ostalih zabavnih sadržaja dostupnih na Internetu) može biti sigurno i ugodno ukoliko se korisnici educiraju o osnovnim principima računalne sigurnosti te ukoliko ih se pridržavaju. Zbog ekspanzije zlonamjernih korisnika na Internetu, nepažnja i naivnost mogu i značajnije utjecati na materijalne troškove korisnika.

5.1. Uobičajena sigurnosna praksa

Načela računalne sigurnosti vezana uz *online* igre u velikoj su mjeri slična načelima sigurnosti prisutnima kod drugih računalnih aplikacija. Ključne značajke kojih bi se pojedinac trebao pridržavati uključuju:

- korištenje antivirusnih i *antispyware* programa;
- oprez kod otvaranja datoteka prispjelih putem priloga elektroničke pošte ili instant poruka;
- provjeravanje autentičnosti i ispravnosti datoteka odnosno aplikacija preuzetih s Interneta;
- u sigurnosnom smislu ispravno podešen web preglednik;
- korištenje vatrozida;
- identificiranje i izradu sigurnosnih kopija osobnih i poslovnih podataka;
- stvaranje i korištenje lozinki koje je teško pogoditi;
- korištenje zakrpa i redovnu nadogradnju korištene programske podrške.

Sa druge strane, poslužitelj igara treba obratiti pažnju na:

- autentikaciju – provjeru da je igrač zaista onaj za koga se izdaje;
- kontrolu pristupa – dodjeljivanjem određenih ovlasti korisniku se određuje kojim resursima ima pristup, a kojima ne;
- digitalne certifikate – s obzirom da su certifikati datoteke koje sadrže privatne informacije korisnika, moguće ih je koristiti i za autentikaciju i za sigurnosno kodiranje prometa koji putuje po javnoj infrastrukturi;
- digitalne potpise – određuju da li je transformirani tekst nastao korištenjem ispravnog privatnog ključa i je li poruka tijekom prijenosa modificirana od strane treće osobe.

5.2. Sigurnosna praksa kod igranja preko Interneta

5.2.1. Opasnosti administratorskog korisničkog računa

Neke igre zahtijevaju izvođenje s pravima administratora računala. U tom je slučaju vrlo važna reputacija tvrtke koja je igru razvila kao i izvora s kojeg se preuzima. Besplatne igre nerijetko sadržavaju skrivenu zlonamjernu programsku podršku, često u obliku programskih priključaka za koje se tvrdi da su neophodni za igranje. Međutim, nerijetko je zlonamjerna podrška i potpuno neuočljiva za korisnika. Pokretanje aplikacija s administratorskim ovlastima povlači za sobom i rizik da zlonamjerni korisnik stekne potpunu ovlast nad žrtvinim računalom. Surfanje webom korištenjem korisničkog računa bez povećanih ovlasti daleko je sigurnije i preporuča se kada god je to moguće.

5.2.2. Opasnost od ActiveX i JavaScript kontrola

Online igre koje kao klijentsku aplikaciju koriste web preglednik, najčešće zahtijevaju pokretanje i izvođenje ActiveX kontrola ili JavaScript koda za uspješno izvođenje dinamičkog sadržaja u

kontekstu web preglednika. Kod ovakvih situacija korisnik mora biti svjestan da omogućavanjem izvođenja nepoznatog koda (koji može biti i zlonamjerno oblikovan) u okviru web preglednika, napadaču omogućava preuzimanje ovlasti nad svojim računalom. Zaštita od ovih opasnosti prvenstveno leži u korištenju provjerenih i certificiranih kontrola i programskog koda.

5.2.3. Igranje i pregledavanje ostalih web sadržaja

Igranje igre koja zahtijeva povišene korisničke ovlasti najbolje je izvesti tako da se tijekom igranja ne pregledava drugi sadržaj na webu. Preporuča se tek po završetku igre prijeći u korisnički račun bez posebnih ovlasti i nastaviti pregledavanje weba. Na opisani način izbjegava se mogućnost pokretanja zlonamjernog koda s posebno oblikovanih web stranica, budući da u preporučenom korisničkom modu takve aplikacije imaju daleko manje ovlasti, a time i smanjene mogućnosti nanošenja štete korisniku.

5.2.4. Podešavanje vatrozida

Korisnici koji se priključuju na Internet osobnim računalom često koriste vatrozid kako bi zaštitili vlastito računalo od nedozvoljenih pristupa zlonamjernih osoba ili aplikacija. Igranje igara preko Interneta ponekad zahtijeva uvođenje iznimke (eng. *exception*) u pravila vatrozida te se na taj način omogućava dopuštanje razmjene informacija vezanih uz igru. Svako dodavanje iznimke ostaje trajno pohranjeno i postaje potencijalan otvor za pristup računalu žrtve. Vatrozidi također dopuštaju postavljanje IP adresa od povjerenja s kojima se komunikacija ne podvrgava sigurnosnoj provjeri. Tu također postoji mogućnost za izvođenje različitih malverzacija ukoliko se nepažljivog igrača navede na dodavanje nepoznatih IP adresa u taj popis. Preporuka je svim igračima da pažljivo provjere koje iznimke dodaju vatrozidu, po mogućnosti da istraže sigurnost protokola kojeg se time omogućava te koje IP adrese postavljaju kao vjerodostojne.

6. Primjeri ranjivosti poznatih *online* igara i servisa

6.1. Second Life

6.1.1. Općenito o igri

Second Life je socijalna igra sačinjena od virtualnog svijeta i pripadnih likova koje predstavljaju igrači. Igru je razvila tvrtka Linden Lab, a službena stranica igre je http://secondlife.com/. Krajem ožujka 2008. godine zabilježeno je više od 13 milijuna registriranih korisničkih računa. Second Life postao je jedan od najvećih servisa za zabavu na svijetu. Riječ je o virtualnom prostoru za razmjenjivanje poruka koji umjesto sličica ima 3D likove (avatare) koji hodaju, skaču, prave grimase, vode ljubav, plešu pa čak i lete. No, Second Life se s vremenom razvio u vrlo složenu društvenu mrežu koja ima vlastite zakone, moralne vrijednosti pa čak i vlastitu ekonomiju. Na taj način je, uz socijaliziranje, glavni cilj stjecanje privatnog vlasništva što povlači i bavljenje virtualnim poslom kako bi se zaradilo što više Linden dolara (L$). Second Life svoju popularnost može zahvaliti i činjenici da je dostupan širokom broju korisnika zbog relativno skromnih zahtjeva na resurse. Dakle, korisnikom, odnosno igračem igre Secod Life može postati bilo koji korisnik računala sa širokopojasnom vezom prema Internetu.

Postoje dva tipa korisničkog računa, jedan koji ne zahtijeva novčanu naknadu, dok je drugi tzv. „*premium*“, a plaća se pri otvaranju i zahtjeva mjesečno nadoplaćivanje. Premium račun, u odnosu na besplatan, obuhvaća mogućnosti otvaranja vlastitog virtualnog poduzeća, zakupljivanja i prodaje zemljišta i dr.

No, plaćanje korisničkih računa nije ono zbog čega se proziva tvrtka Linden Lab. Sporna je činjenica da se Linden dolari mogu zamijeniti za US dolare po posebnom tečaju (1 USD - 250 L$, ali može varirati) kojeg diktira sam Linden Lab. Zabilježeni su slučajevi bogaćenja korisnika prodavanjem virtualnih zemljišta, automobila, filmova ili odjeće. Sociolozi imaju jednake prigovore kao i na ostale igre sličnog žanra, poput igre World of Warcraft, a glavni argument je otuđenje igrača, njihova pretjerana orijentacija virtualnoj stvarnosti i zanemarivanje stvarnog života i ljudi koji ih okružuju.

Slika 5: Izgled jednog od posjećenijih virtualnih mjesta u igri Second Life

6.1.2. Zlouporaba

Iako ga proizvođač pokušava predstaviti kao savršeno mjesto za ostvarivanje snova i želja, Second Life je itekako podložan zlouporabi. Najozbiljnija optužba odnosi se na stvaranje i distribuciju dječje pornografije. Gotovo je nemoguće uspješno kontrolirati toliki broj aktivnih korisnika, a i samo sprečavanje je isto tako vrlo teško zbog toga što niti jedan od korištenih sigurnosnih protokola ne može zabraniti interakciju između dva ili više avatara bez obzira na njihovu virtualnu starost.

Jedna od uočenih ranjivost, a time i mogućih zlouporaba, vezana je uz određenu inačicu Apple QuickTime preglednika. Dakle, nije izravno vezana uz igru Second Life nego se preglednik koristi kao tzv. *3rd party* aplikacija. Igra dopušta igračima da postavljaju datoteke zabavnih sadržaja u objekte iz igre te koriste QuickTime preglednik za prikazivanje tih video sadržaja. Ukoliko igrač ranjivim preglednikom otvori zlonamjerno oblikovan video sadržaj, privatnost njegovih podataka može biti ugrožena. Potencijalne opasnosti uključuju i otuđenje korisnikova virtualnog novca. Ranjivost je uklonjena iz preglednika krajem 2007. godine u cijelosti.

Druga uočena opasnost unutar igre Second Life vezana je uz spremanje podataka o korisnicima bez sigurnosnog kodiranja. To je omogućavalo napadaču dohvaćanje korisničkih imena, imena ljudi iz stvarnoga svijeta i njihove kontakt informacije zajedno s kodiranim zaporkama i financijskim informacijama. Kao mjeru zaštite, vlasnik igre ispravio je nedostatak, poništio sve zaporke te od igrača tražio unos nove zaporke.

6.2. World of Warcraft

6.2.1. Općenito o igri

World of Warcraft jedna je od najčešće igranih *online* igara na svijetu. Tematski se nadovezuje na prethodne nastavke istoimenih igara (Warcraft I, II i III). Proizvođač igre je Blizzard Entertainment, a učestvovanje u igri se temelji na mjesečnoj pretplati. Samim time što ova igra nosi atribut najpopularnije igre, to donosi i povećanu vjerojatnost bivanja metom napada zlonamjernih igrača.

WoW pripada skupini MMORPG igara. Poput drugih igara istoga žanra, i ovdje igrač kontrolira svoj virtualan lik unutar *online* svijeta, istražuje okolinu, bori se protiv različitih likova, a omogućena je i interakcija s drugim igračima.

Slika 6: Isječak iz igre World of Warcraft

6.2.2. Slučajevi zlouporabe

Igrači igre WoW bili su metom zlonamjernih korisnika koji su se koristili propustom u načinu na koji operacijski sustav Microsoft Windows obrađuje animirane kursore. Iskorištavanje propusta od napadača traži posebno oblikovanje web stranice i navođenje žrtve na posjet istoj. Konačan ishod je preuzimanje korisničkog računa, a svaki od računa vrijedi stanovit iznos novca, ovisno o uspjehu korisnika koji ga posjeduje. Analiza je pokazala da se zlonamjeran programski kod stavlja u stanje mirovanja na žrtvinom računalu i tako ostaje sve do prijavljivanja na WoW sustav. U tom trenutku prikupljaju se podaci o žrtvinom korisničkom računu i šalju napadaču.

6.2.3. Rootkit u igri World of Warcraft

Hakeri usmjereni na igru World of Warcraft potvrdili su da je moguće iskoristiti dijelove Sony DRM *rootkit* aplikacije za skrivanje vlastitih zlonamjernih aplikacija koje su razvijene u svrhu varanja u *online* svijetu navedene igre. Tako skrivene aplikacije nemoguće je uočiti pa je kao odgovor na taj problem proizvođač igre, Blizzard Entertainment, izdao Warden, program koji je namijenjen uočavanju instaliranih *rootkit* alata namijenjenih varanju u igri WoW. Međutim, pokazalo se kako je ta aplikacija nepotpuna budući da je dodavanjem prefiksa 'sys' na proizvoljnu zlonamjernu datoteku moguće izbjeći njenu detekciju.

6.3. Facebook

6.3.1. Općenito o servisu

Riječ je o poznatoj društvenoj mreži koja je započela s radom u veljači 2004. godine. Servis je osmislio Mark Zuckerberg tijekom studiranja na Harvardu. Korisnici se mogu proizvoljno pridruživati pojedinim grupama (zvanim mrežama) prema mjestu u kojemu žive, radnom mjestu, školi, regiji, državi itd. Svaki korisnik posjeduje vlastiti popis prijatelja kojeg može proizvoljno modificirati. Servis omogućava razmjenu poruka u realnom vremenu, kao i poruka sličnih porukama elektroničke pošte, postavljanje informacija o korisniku. Također, omogućene su socijalne aktivnosti korištenjem brojnih web aplikacija razvijenih posebno za Facebook.

6.3.2. Uočeni propusti i zlouporaba

Ostali oblici online zabave poput društvenih mreža predstavljaju za korisnike različite potencijalne opasnosti. Jedan od poznatijih propusta Facebook servisa uočio je kanadski računalni tehničar Byron Ng. On je na taj način ostvario pristup zaštićenim fotografijama Paris Hilton i njenog brata Nicholasa i na taj način osigurao medijsko eksponiranje tog propusta.

Prvi propust Facebook servisa uočen u kolovozu 2008. omogućavao je pokretanje izvođenja proizvoljnog JavaScript koda zbog neispravne obrade prvog parametra funkcije setTimeout(). Drugi propust omogućavao je također pokretanje proizvoljnog programskog koda koristeći funkcijski konstruktor. Vrlo korektno, pronalazač ovih propusta, Neil Mix, najprije je obavijestio Facebook razvojni tim, a tek nakon ispravaka propusta javno objavio dane informacije.

7. Mehanizmi implementirani u operacijske sustave korisnika

Izdavači računalnih igara poduzeli su različite mjere kako bi unaprijedili sigurnost svojih korisnika. Neke od tih mjera, poput nametanja strogih uvjeta korištenja (uvjeta kojima se ograničavaju načini korištenja aplikacije, uključujući i zlonamjerne aktivnosti), potpuno su opravdane. Neke su pak trivijalne za 'probijanje', primjerice, korištenje sigurnosnog kodiranja (kriptiranja) uz uključivanje tajnog ključa u izvorni kod klijent aplikacije. Naime, reverznim inženjeringom moguće je na relativno jednostavan način doći do tako pohranjenog tajnog ključa. Posljednja skupina u najmanju ruku je kontroverzna, a ona obuhvaća nadzor igrača bez njegova znanja što nije u skladu sa zakonom većine zemalja.

Poznato je da neke tvrtke koriste tehnike prikrivanja kakve se najčešće nalaze u tzv. *rootkit* aplikacijama da bi nadgledali korisnike svojih klijentskih aplikacija. Takve tvrtke također su poznate i po vrlo strogim taktikama kojima uklanjaju i prve naznake mogućeg štetnog ponašanja u igri, čak i kada ti pokušaji nisu zlonamjerni.

7.1. Što je rootkit

Rootkit je kolekcija alata odnosno aplikacija koje omogućavaju pristup s povišenim ovlastima odredišnom računalu odnosno računalnoj mreži. Napadač uobičajeno instalira *rootkit* nakon ostvarivanja pristupa uobičajenom korisničkom računu bez povećanih ovlasti. Takav pristup moguće je ostvariti iskorištavanjem propusta u nekoj aplikaciji ili probijanjem lozinke potrebne za pristup. Jednom kada je zlonamjeran alat instaliran, napadač na jednostavan način ostvaruje pristup žrtvinom računalu s povećanim ili potpunim ovlastima.

Rootkit može sadržavati čitav niz drugih dodataka poput *spyware* aplikacija ili aplikacija za nadzor mrežnog prometa, nadzor ulaznih jedinica (tipkovnice i miša), stvoriti tzv. *backdoor* mogućnost kasnijeg ponovnog pristupa žrtvinom računalu, napadati druga računala na mreži i čitav niz ostalih zlonamjernih aktivnosti. Također može mijenjati sistemske alate i dnevničke zapise (eng. *log*) kako bi onemogućio detekciju vlastita neovlaštenog pristupa računalu.

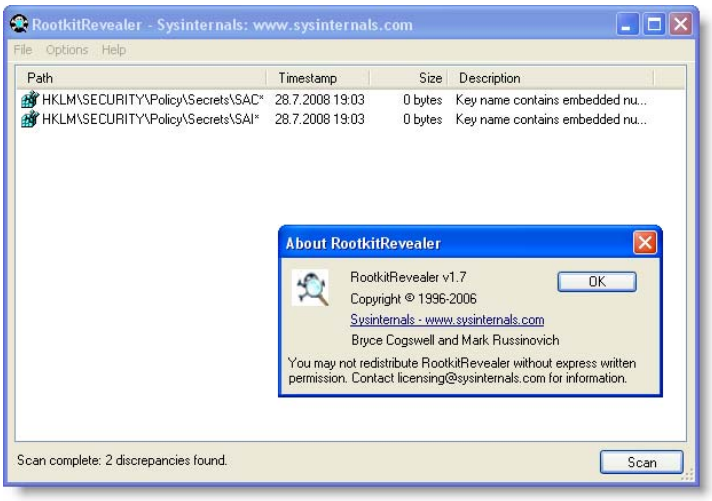
Prisutnost ovih zlonamjernih aplikacija započela je u ranim devedesetima kada su Sun i Linux operacijski sustavi bili metama napada. Danas su se napadi proširili na većinu operacijskih sustava uključujući i Microsoft Windows sustave.

Jedan od važnijih događaja kojima su *rootkit* alati postali znatnije eksponirani u javnosti, dogodio se krajem listopada 2005. godine kada je stručnjak za računalnu sigurnost Mark Russinovich iz tvrtke Sysinternals otkrio postojanje takvog alata na svom računalu. *Rootkit* je bio instaliran kao DRM (eng. *Digital Rights Management*) komponenta programske podrške tvrtke Sony. Bila je riječ o aplikaciji koja se transparentno za korisnika instalira u jezgri operacijskog sustava. Na taj način Sony je pokušao onemogućiti neke nedozvoljene aktivnosti poput neovlaštenog kopiranja CD medija. Stručnjaci strahuju da je ovakva praksa mnogo češća nego se misli i da bi napadači mogli iskorištavati takve *rootkit* alate. Mikko Hypponen iz tvrtke F-Secure izjavio je kako ovo stvara autorima virusa pogodnosti za razvoj novih zlonamjernih programa. Ukoliko se *rootkit* alati upotrijebe u zlonamjerne svrhe, sigurnosnim tvrtkama posao otkrivanja prijetnji uvelike je otežan. Razlog tome je integracija *rootkit* alata u jezgru operacijskog sustava.

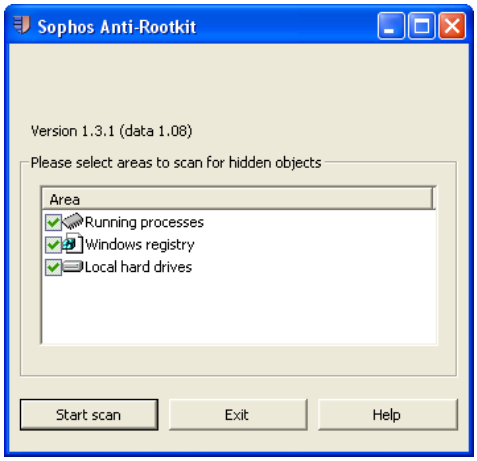
Proizvođači programske podrške poput tvrtki Microsoft, F-Secure i Sysinternals često korisnicima nude aplikacije kojima se može detektirati postojanje *rootkit* alata. Ukoliko korisnik na svom računalu to zaista i uoči, predlaže se instalacija operacijskog sustava uz prethodno brisanje svih podataka s diska što je najpraktičnije izvesti formatiranjem diska.

Dva besplatna alata čiji se prikazi mogu vidjeti na slikama ispod, moguće je dohvatiti s adresa:

- http://download.sysinternals.com/Files/RootkitRevealer.zip i
- http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html (zahtijeva prethodnu registraciju).



Slika 7: Aplikacija RootkitRevealer koju nudi tvrtka Microsoft u svrhu otkrivanja *rootkit* alata



Slika 8: Anti-Rootkit aplikacija tvrtke Sophos

8. Povijesni pregled razvoja *online* zabavnih sadržaja i osvrt na budućnost

Prvi početci igara sežu u daleku 1864. godinu kada je Charles Babbage postavio temelje za strojno igranje šaha. Digitalna računala započinju razvoj 1940-ih godina kada su John von Neumann i Oskar Morgenstern proučavajući teoriju igra primijenili „minimax" algoritam na program za igranje šaha.

Jedna od prvih poznatijih igara stvorena je 1962., a nosi naziv *Spacewar!*. Razvijena je na računalu PDP-1 na institutu MIT (eng. *Massachusetts Institute of Technology*), prvom komercijalnom računalu s 15" CRT (eng. *Cathode Ray Tube*) monitorom. Upravo je ta sličnost s današnjim računalima razlog zašto se spomenutu igru smatra pretečom današnjih računalnih igara. Valja napomenuti da su takva računala korištena kao tzv. *main-frame* računala na kojima su se odvijala većinom različita istraživanja, a igrači su bili uglavnom računalni stručnjaci i znanstvenici.

Prvo računalo namijenjeno isključivo izvođenju računalnih igara nazvano je *Computer Space*. Radi se o nešto jednostavnijoj inačici prethodno navedene igre *Spacewar!*. Igranje se temelji na ubacivanju kovanica u automat čime se određuje duljina trajanja pojedinog igranja, odnosno broj pokušaja igranja. Takav tip igara i pripadnih sklopovskih sustava naziva se arkadnim igrama (eng. *arcade games*).

Za razliku od arkadnih, konzolne igre razvijene su za kućne korisnike koji su se mogli igrati priključivanjem konzole na televizijski prijamnik. Prva ovakva konzola nosila je naziv Odyssey. Uskoro su razvijene i inačice konzola s dodatnim elektroničkim modulima (eng. *catridge*). Sredinom 1980-ih Nintendo je ostvario ogromnu zaradu razvojem svoje 8-bitne konzole naziva NES. 1995. godine Sony izdaje Playstation, revolucionaran proizvod u pogledu računalne grafike, zvuka i interakcije s korisnikom. Microsoft 2001. slijedi Sony i izdaje popularan X-Box. Današnje igraće konzole koje se smatraju vrhunskim dostignućima na području realističnosti su već spomenuti Microsoft X-Box, Nintendo Game Cube te Sony Playstation II i III.

Razvoj modernijih igara za digitalna računala započinje Sinclair Spectrum računalom iz 1981. godine. Nedugo zatim i vrlo popularan Commodore 64 postaje dostupan na tržištu. Oba proizvoda omogućavala su korisnicima razvoj vlastitih aplikacija, prema tome i igara.

Novi zaokret u razvoju računala donose osobna računala (eng. *PC - personal computer*). Pojavljuju se Quake, Wolfenstein, Tomb Raider i druge popularne igre. Igre su većinom bile namijenjene MS-DOS i MS-Windows operacijskim sustavima, a u manjoj mjeri Linux, odnosno sustavima temeljenim na Unixu. Ove igre donose novi način interakcije s korisnikom, ali i uvode novi koncept igara – mrežne igre. Prethodno su igre bile razvijane za jednog igrača. Nadogradnju predstavljaju inačice koje su koristile virtualne igrače kao suigrače korisniku.

Sljedeći korak u razvoju računalnih igara obilježava pojava igara za više igrača (eng. *multiplayer games*). Ovdje se razlikuju dvije vrste igara:

- igre namijenjene igranju više igrača na istom računalu i
- igre namijenjene igranju više igrača od kojih je svaki na zasebnom računalu, a komunikacija se odvija putem računalne mreže.

Druga vrsta igara doživjela je procvat razvojem Interneta koji je omogućio vrlo jednostavno povezivanje računala. Virtualne likove, do sada simulirane, sada predstavljaju ljudi koji se nalaze na bilo kojem mjestu na Zemlji što uvelike povećava zadovoljstvo igranja. Uz Internet igre pojavljivale su se i virtualne zajednice koje su omogućavale i komunikaciju među igračima, jedan oblik druženja. Prvom *online* igrom smatra se MUD1 (eng. *multi-user dungeon*), razvijena 1979. godine.

Današnje *online* igre postaju vrlo unosne zbog činjenice da su ljudi voljni platiti za ovakav način zabave.

Sigurnost u počecima razvoja igara uglavnom se zanemarivala, iako je bila predmetom proučavanja računalnih eksperata još od 1960-ih godina. Sigurnosna pitanja arkadnih igra vezana su uglavnom uz fizičke karakteristike mehanizma za prihvat novca. Od samog početka, igre namijenjene igranju na osobnim računalima bile su podložne neovlaštenom umnožavanju zbog načina distribucije koji je uglavnom podrazumijevao diskete, a kasnije i CD/DVD medije.

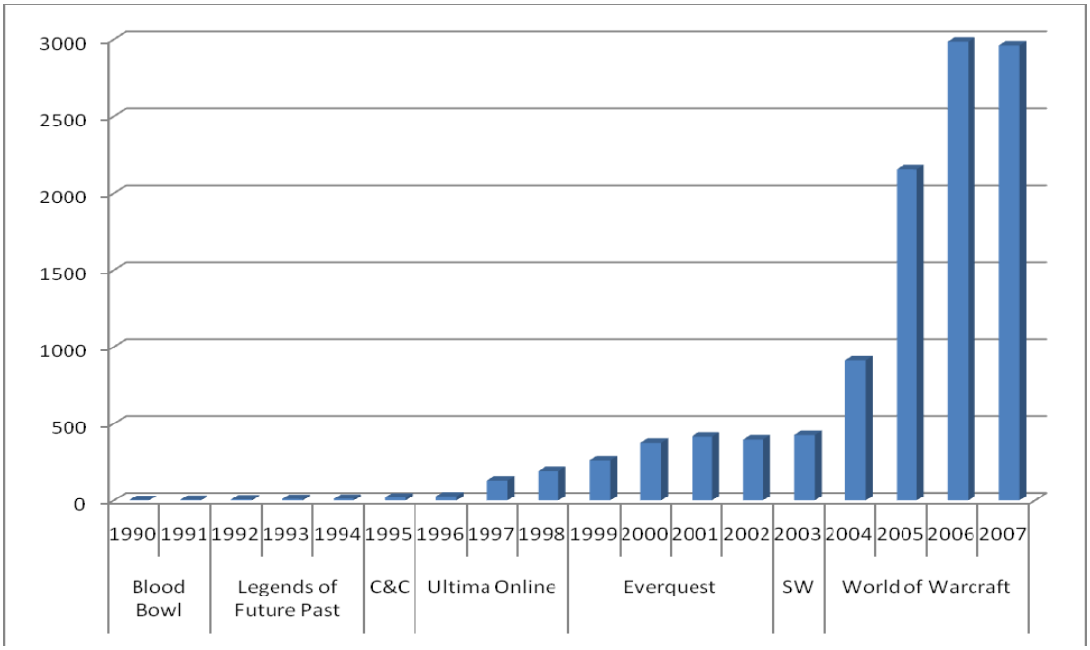
Na području igraćih konzola, Nintendo je prvi uveo zaštitne mehanizme čiji su temelji ostali prisutni sve do danas. Riječ je o tzv. *lock-and-key* konceptu, sigurnosnom čipu na temelju kojega se osigurava korištenje isključivo izvornih *catridge* medija. Po jedan čip se nalazio i na konzoli i na mediju, a sustav je radio jedino ako

su ta dva čipa ispravno međusobno komunicirala. Slična se tehnologija koristi danas i u konzolama ostalih proizvođača.

Razvoj *online* igara nije promijenio samo način igranja, nego je uzrokovao i radikalne promjene u odnosu prema sigurnosti igranja. Zbog novog načina plaćanja (prilikom prijavljivanja na poslužitelj igre, mjesečne pretplate i dr.), zaštita od neovlaštenog kopiranja medija više ne predstavlja značajan problem. Svojstvo raspodijeljenosti (izvođenje programskog koda igre na više povezanih računala) u *online* igre uključuje problematiku vezanu uz sigurnost mrežne komunikacije. Time nastaje potreba za mehanizmima koji omogućuju privatnost podataka i nadzor (ograničenje) pristupa zajedničkim resursima. Također, kod komercijalnih igara u kontekstu sigurnosti obuhvaćeni su i mehanizmi *online* plaćanja. Istraživanja su pokazala da je varanje u *online* igrama postalo značajan sigurnosni problem.

53% igrača očekuje da će nastaviti igrati igre i sljedećih 10 godina. 31% od svih igrača 2002. godine igralo je *online* igre dok se 2008. ta brojka popela na 44%. Prema tim statistikama za očekivati je rast korisnika ovakve vrste zabave. Sve veći broj korisnika sa sobom nosi i porast broja zlonamjernih korisnika. Zbog povećanja složenosti *online* igara, ali i drugih servisa za zabavu, očekuje se povećanje broja sigurnosnih nedostataka kao i njihova iskorištavanja. Ulaganja u *online* servise usmjerene na zaradu su velika, a to za sobom povlači i povećanje pažnje usmjerene na sigurnost i u okviru Internet zabave.

Sljedeća slika prikazuje najpopularnije igre u razdoblju od 1990. do 2007. godine – komercijalna igra World of Warcrafr zauzima čvrsto prvo mjesto u posljednjih nekoliko godina.



Slika 9: Pregled najpopularnijih igara u periodu od 1990 do 2007. godine prema broju glasova na portalu gamerDNA.com (SW – Star Wars Galaxies, C&C – Command and Conquer)

Idealan slučaj što se tiče budućnosti računalne sigurnosti bio bi onaj u kojemu računala posjeduju inteligenciju čovjeka. Tada bi se ona mogla samostalno braniti od virusa i drugih zlonamjernih aplikacija, bez potrebe za nadogradnjama antivirusne programske podrške, analizama ranjivosti sustava, iskusnim administratorima i sigurnosnim ekspertima itd. Usprkos 50 godina istraživanja s područja umjetne inteligencije, vjeruje se kako su sva dosadašnja saznanja vezana uz umjetnu inteligenciju tek vrlo mali djelić toga velikog područja. Napredak računarskih znanosti iznimno je brz pa se može očekivati da će nekada u budućnosti računala ipak biti u stanju voditi računa o sigurnosti bez intervencije čovjeka.

Sve do tada valja se osloniti na vlastitu inteligenciju kako bi se zaštitilo računalne sustave od zlonamjernih korisnika.

9. Zaključak

Igranje preko Interneta je područje čiji razvojni eksperti nisu nužno i eksperti za sigurnost. S druge strane pak, eksperti s područja računalne sigurnosti nisu ujedno i eksperti za široku domenu znanja s područja *online* zabave. Do prije nekoliko godina nisu postojala ozbiljnija proučavanja potencijalnih sigurnosnih opasnosti koje prijete takvim načinom zabave. Ipak, u posljednje vrijeme, povećanjem broja aktivnih sudionika *online* zabave, samosvjesnost proizvođača, a i sigurnosnih stručnjaka, osjetno je porasla. Pojavljuju se i specijalizirane knjige koje na vrlo precizan i detaljan način pojašnjavaju načine iskorištavanja propusta kod Internet igara koje napadači većinom iskorištavaju da bi načinili štetu drugima. Ipak, u posljednje vrijeme sve češća je namjera napadača stjecanje materijalne dobiti.

Industrija računalne zabave s vremenom raste i razvija se, igre kao i samo igranje postaju sve složenijima, a povećanjem složenosti raste i vjerojatnost za pojavom sigurnosnih propusta. Svi aktivni i strastveni igrači morali bi biti svjesni navedene činjenice i morali bi si dati truda za upoznavanjem barem najvažnijih opasnosti koje prijete igranjem preko Interneta. To je jedini i najbolji način za izbjegavanje rizika povezanih s ovim načinom zabave.

10. Reference

[1] Playing it safe: Avoiding Online Gaming Risks, http://www.us-cert.gov/reading_room/gaming.pdf, 2006.

[2] Zaštita podataka, skripta, http://mudrac.ffzg.hr/~ltatomir/skripte/skripte/zastita%20podataka.rtf, svibanj 2005.

[3] Cursor hackers target WoW players, http://news.bbc.co.uk/2/hi/technology/6526851.stm, travanj 2007.

[4] Exploiting Online Games, preface, http://www.cigital.com/justiceleague/2007/07/12/preface-from-exploiting-online-games/, srpanj 2007.

[5] World of Warcraft, Blizzard Entertainment, http://us.blizzard.com/support/index.xml?gameId=11, 2008.

[6] W. Chen i M. Chen, Internet Game Security, http://islab.oregonstate.edu/koc/ece478/03Report/wtchen_mtchen.pdf.pdf, lipanj 2002.

[7] J. Yan i B. Randell, Security in Computer Games: from Pong to Online Poker, veljača 2005.

[8] Online Game, http://en.wikipedia.org/wiki/Online_game, kolovoz 2008.

[9] New Scientist, Computer characters mugged in virtual crime spree, http://www.newscientist.com/article.ns?id=dn7865, kolovoz 2005.

[10] Online Games & the Law, http://www.darkreading.com/document.asp?doc_id=136128, listopad 2007.

[11] Zakon o zaštiti osobnih podataka, http://www.cert.hr/filehandler.php?did=337, srpanj 2008.

[12] Elektronička pošta i privatnosti, http://www.ericsson.com/hr/etk/novine/kom0405/e_mail.shtml, travanj 2005.

[13] Rootkit, http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci547279,00.html, siječanj 2008.

[14] RootkitRevealer, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, studeni 2006.

[15] World of Warcraft hackers using Sony BMG rootkit, http://www.securityfocus.com/brief/34, studeni 2005.

[16] Matt Pritchard, How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It, http://www.gamasutra.com/features/20000724/pritchard_01.htm, srpanj 2000.

[17] America's Army, http://www.americasarmy.com/army/privacy.php, 2008.

[18] 2007, The Year of the Online Game?, http://www.webpronews.com/topnews/2007/01/12/the-year-of-the-online-game, siječanj 2007.

[19] Second Life, http://en.wikipedia.org/wiki/Second_Life, kolovoz 2008.

[20] Security lapse exposes Facebook photos, http://www.msnbc.msn.com/id/23785561/, ožujak 2008.

[21] FBI PRESS RELEASE: Parents reminded to keep their kids safe on increasingly popular social networking sites, http://www.fastandloud.com/uncategorized/the-fbi-gets-dibs-on-the-myspace-facebook-friendster-frenzy/, ožujak 2006.

[22] Online Games Statistics, http://www.onlinegolf.info/blog/index.php?blog=1&title=online-game-statistics&more=1&c=1&tb=1&pb=1, siječan 2008.

[23] gamerDNA: Game History, http://www.gamerdna.com/GameHistory.php, kolovoz 2008.

[24] Identity 'at risk' on Facebook, http://news.bbc.co.uk/1/hi/programmes/click_online/7375772.stm, svibanj 2008.