Проф. др *Драган РАНЂЕЛОВИЋ*[1]
Криминалистичко-полицијска академија, Београд
Милош РАНЂЕЛОВИЋ
Хелп Ниш

UDK – 004.4 : 351.741
Примљено: 25.09.2014.

Специфичност и безбедност софтверског алата као дела сервиса за одговор на хитан позив у полицији

Апстракт: *Сервис сталног дежурства је једна од најважнијих услуга на којима се заснива рад полиције, а одговор на хитан позив у том сервису је један од најважнијих послова. Овај рад покушава да пружи увид у организацију, послове и рад безбедносних служби које се баве одговором на хитан позив, како би указао на неопходност имплементирања савремених сервиса који би подигли ниво предвиђања ситуације на терену у реалном времену и тако омогућили адекватније ангажовање и одлучнију − бржу реакцију. Специфичност алата који треба да обезбеди информације командном кадру полиције, одговорном за деловање у случају хитног позива полицији, огледа се у степену тачности, брзини приспећа и брзини обраде података у информацију корисну за грађење слике о хитним позивом пријављеној инцидентној или кризној ситуацији. Циљ рада је утврђивање неопходних метода и принципа при реализацији алата за одговор на хитан позив. То се чини, с једне стране, анализом резултата претходно реализованих алата, како са аспекта пројектовања и имплементирања, тако и експлоатисања као најбитније оцене реалне учинковитости сваког алата, и, с друге стране, проналажењем одговарајуће методологије решења. У раду је приказана функција једног од могућих сценарија имплементирања информационо-комуникационих система, која посебно скреће пажњу на безбедносне аспекте.*

Кључне речи: *хитан позив за помоћ, алати за одговор на хитан позив, сигурност система за хитне позиве, аутентификација, енкрипција.*

[1] E-mail: dragan.randjelovic@kpa.edu.rs

Увод

Одговор на хитан позив полицији за помоћ грађанима је један од основних послова полиције који спроводи начело константне присутности, а одвија се по аутоматизму, коришћењем предефинисаних оперативних процедура. Као један од основних задатака, који не трпи толеранцију у времену реакције на инцидентну или кризну ситуацију, мора да има довољну количину прикупљених информација како би се изградио адекватан одговор. Специфичност алата за помоћ при одговору на хитан позив огледа се у задовољавању потреба службе сталног дежурства у чијој је надлежности прихватање позива, које обавезно прати прикупљање података и њихово процесуирање у квалитетне информације на основу којих руководећи кадар може да гради јасну слику о ситуацији на терену. Тиме се обезбеђује брза, квалитетна и одлучна реакција са високим степеном поузданости, која води ка адекватном и ефикасном руковођењу тимовима за реакцију.

Може се рећи да су информације почетни чинилац полицијског деловања. Од количине и квалитета прикупљених и прослеђених података зависи и деловање под условима извесности[2] , на коју треба утицати и подићи њен степен при деловању ради довођења инцидентне или кризне ситуације у контролисано стање.

Стицај несрећних околности у којем је била наша земља крајем 20. века је успорио праћење савремених тенденција развоја информационих и телекомуникационих технологија, као и њихово имплементирање у постојеће информационо-комуникационе системе (ИКС), а примери за то су: обезбеђивање информација о локацији по-зиваоца у реалном времену, обезбеђивање информација о локацији и статусу полицијских службеника који су на терену у реалном времену, приказ дигиталних мапа, израда база података и њихово повезивање са дигиталним мапама (Ранђеловић, Јаћимовски, 2011). Истовремено, у МУП-у имамо примере успешне имплементације савремених сервиса лоцирања системом ТЕТРЕ и ГСМ мреже.

Рад, пружајући увид у организацију, послове и рад безбедносних служби које се баве одговором на хитан позив, приказује функције једног од могућих сценарија имплементирања ИКС-а, које посебно скрећу пажњу на безбедносне аспекте чија се неопходност имплементирања у ИКС превасходно односи на заштиту осетљивих информација (Ранђеловић, Петровић, Радовановић, Поповић, 2009;

[2] Све чешће се у страној литератури помиње појам „свест о ситуацији“ (енг. Situation awareness), као синоним за перцепцију променљивих у времену и простору, а које су од важности за даљи развој ситуације на терену на коме се дешавају појаве од интереса за безбедносне службе.

Ранђеловић, Ранђеловић, Кузмановић, 2014) и онемогућавање њихове злоупотребе (Van Tilborg, 2005; Stamp, 2006; Ранђеловић, Делија, Поповић, 2009; Ранђеловић, Богдановић 2010; Ранђеловић, Ђорђевић, 2011; Ранђеловић, Стојковић, 2012; Ранђеловић, 2013).

Службе сталног дежурства

Хитан позив у помоћ се упућује на број дежурног телефона нумерације 112 или 192. На позив одговара помоћник шефа смене који прима и води разговор са позиваоцем, и бележи податке о догађају који се пријављује како би прикупио довољно информација за стварање јасне слике о ситуацији на терену. Одговорно руководеће лице је шеф смене. Те две функције представљају тим за прву реакцију. Они су одговорни за пријем информације и њену обраду, као и за упућивање и информисање адекватне јединице која ће деловати на терену.

На интервенцију се најчешће упућује интервентна јединица која се, углавном, налази у свом моторном возилу вршећи патролну делатност на терену (код тога је потребно скренути пажњу на разлике у начину функционисања хитних ватрогасних и медицинских служби и функционисања полицијске службе). Ватрогасне и медицинске јединице за хитне интервенције су лоциране унутар базе и на позив реагују напуштањем базе и кретањем ка месту инцидента. Код полицијских служби одређене патроле су увек на терену, чиме се указује на неоходност праћења њихове локације у реалном времену преко дигиталних карти – мапа, на почетку интервенције, што није неопходно код других служби сталног дежурства. Док се праћењем кретања у реалном времену ватрогасних и медицинских служби утврђује време стизања на место инцидента, омогућава навигација најближом путањом и избегавање препрека на путу, код полицијских служби за хитне интервенције је потребно имати и могућност лоцирања адекватне јединице најближе месту инцидента.

Информације се преносе комуникационим каналима који су за то предвиђени –професионалним аналогним и дигиталним радио системима[3] . Уколико је нека друга јединица (позорница, секторска патрола) ближа и може брже и адекватније да одговори на позив, информације се њој преусмеравају на обраду. Остале јединице које су у околини места инцидента могу да се преусмере на пружање подршке

[3] ПМР (енг. PMR − Profesional Mobile Radio) је скраћеница за радио уређаје предвиђене да их користе професионалне организације, безбедносне службе, службе за хитне медицинске интервенције, ватрогасне хитне службе и компаније са посебним потребама. Ови радио уређаји имају особине као што је могућност обраћања групи корисника ПТТ (енг. PTT − push to talk) и сигурност канала.

јединици која врши интервенцију или, уколико ситуација захтева, на блокирање путних праваца. Све јединице које одговарају на постављени задатак на терену представљају јединице за први одговор на инцидентну/кризну ситуацију (Субошић, 2010; Талијан, 2001).

У току пријема података од грађана диспечер кроз разговор, према тачно дефинисаном сету питања и у зависности од ситуације, наводи грађанина у жељеном правцу и потражује од њега одређене податке који су прописани оперативним процедурама, а предуслов су за креирања менталне слике о догађају који се пријављује, са свим неопходним информацијама помоћу којих се може извршити интервенција са што већим степеном извесности.

Израда ИКС-а који би успео да запамти хеуристику[4] рада способног и искусног дежурног полицијског службеника који одговора на хитан позив у кризној или инцидентној ситуацији може да доведе до израде савременијих оперативних процедура.

Комуникациони канали у полицији

Потреба за комуникацијом и разменом информација на свим нивоима организације подразумева постојање комункационих канала који пружају захтевани степен заштите информација које се тим каналима преносе. Полицијске и војне структуре су прве почеле са употребом комуникационих канала коришћењем професионалних радио уређаја ПМР-а као неопходних материјално-техничких средстава (у даљем тексту: МТС) за извршавање одређених задатака из делокруга својих послова. Брзина преноса релевантних информација кориснику је најчешће пресудан чинилац у вршењу полицијских послова са становишта у овом раду разматраног хитног позива.

Савремени поглед на ИС не може се замислити без синтезе функција телекомуникација и ИС-а. Као историјски наставак непрекидног процеса развоја комуникација појављује се као неопходно и електронско-информатичко комуницирање, које има своје предности и мане. Увођењем у рад полиције средстава за електронско комуницирање омогућава се преношење информација, поред комуници-рања гласом и комуницирање писаним текстом и мултимедијалним садржајима код којих раздаљина учесника у комуницирању не представља проблем и носи одређене предности. Савремени видови

[4] Рад службе сталног дежурства или хитне интервенције се базира првенствено по прописаним оперативним процедурама, али се ослања и на искуства кадра стеченог годинама рада у различитим ситуацијама које се не би могле ни предвидети и за њих израдити оперативне процедуре. Уколико би се анализирале архиниране ситуације и деловање људи у тим ситуацијама, могло би се доћи до хеуристике рада службеника у кризним или инцидентним ситуацијама.

комуникације омогућавају превазилажење раздаљине, за разлику од претходних облика комуникације где то није могло да се искључи или је изискивало временски интервал који је савременим средствима комуникације скраћен. Нове могућности дигиталне комуникације су преношење модела ситуација или преношење симулације ситуација са елементима предвиђања одређених појава и њихових исхода[5] .

Подаци прикупљени комуникацијом полицијских службеника, које полиција користи у раду, односе се на бројне појаве, процесе и догађаје.

Све појаве, процеси и догађаји од интереса за рад полиције дешавају се у одређеном простору. Такође у простору поједине организационе јединице полиције обављају сопствену активност. У том најмање двосмерном односу, на пример на релацији делинквенти – полиција, ствара се повезаност чији су основни елементи: врста деликта, време и место његовог дешавања, извршиоци, њихово кретање, с једне, и распоред позорника и патрола у одређеном времену и простору, с друге стране.

Полиција за овакве случајеве најчешће сазнаје дојавом оштећених преко телефонске линије јединственог броја 112, 192. Када дежурна служба (у даљем тексту: ДС) сазна за извршење и прикупи податке о локацији извршења, нпр., разбојништва, она затвореним системом радио веза упућује најближу патролу на место догађаја да изврши интервенцију, коришћењем система за помоћ у одговору на хитан позив према шеми на слици 1, уз архивирање комплетне аудио комуникације (шема на слици 2).

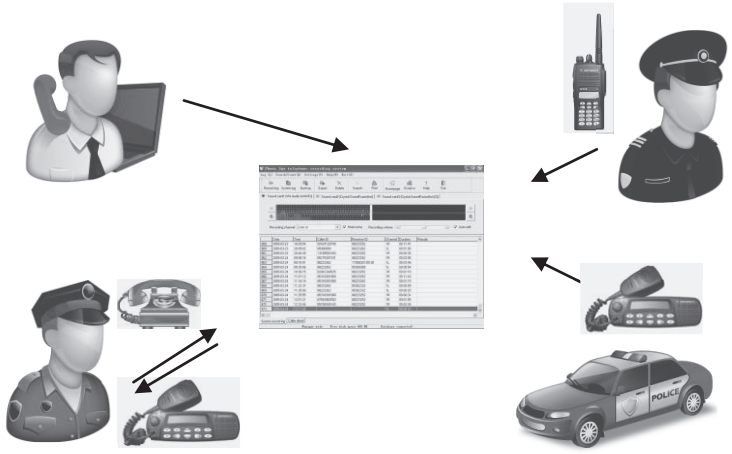
[5] Један од примера је праћење и предвиђање штете услед несреће при превозу опасних материја у саобраћају, праћење стања елементарних непогода и предвиђање могуће штете и угрожености одређених подручја.

Слика 1 – *Илустрација система за помоћ при одговору на хитан позив*

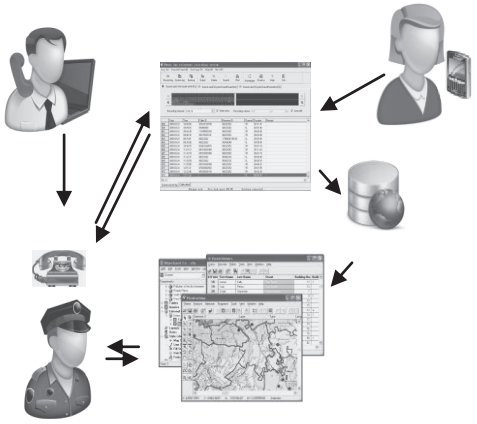
Одређивање позиције у простору позорника или патролне јединице врши се њиховим прозивањем преко затвореног система радио везе у реалном времену. Савремени радио систем лоцира полицијске службенике на дигиталним мапама географско-информационог система (у даљем тексту: ГИС) употребом ТЕТРА[6] терминала коришћењем интегрисаног ЛИП[7] протокола, који се користи за лоцирање тетра радио терминала, према блок шеми на слици 3.

[6] ТЕТРА – (енг. Terrestrial Trunked Radio) је савремени стандардизовани професионални радио систем који помоћу ТДМА (енг. Time Division Multiple Access), мултиплексирањем преносног сигнала, омогућава укупно четири канала на једној фрекфенцији ширине 25 kHZ, док се код аналогних радио станица једна фрекфенција користила за један комуникациони канал.

[7] ЛИП – (енг. Location Indetification Protocol) дефинисан од стране ЕТСИ (eng. *European Telecommunications Standards Institute*) институције, је саставни део савременог телекомуникационог система ТЕТРА, и служи за лоцирање тетра терминала који користе полицијски службеници, чиме се омогућава утврђивање њихове локације у реалном времену.



Слика 2 – *Илустровани приказ архивирања комплетне аудио комуникације*



Слика 3 – *Илустровани приказ лоцирања позиваоца на ГИС мапи*

Такав алат треба да поседује особине редундантности, сигурности, стабилности и пре свега немогућности злоупотребе на неприхватљив или незаконит начин прикупљених информација. Да би ИКС поседовао поменуте особине, неопходно је предузети низ мера и метода као што је софтверско инжењерство, уз незаобилазно учешће кибернетичке теорије при пројектовању ИКС-а.

Један од кључних захтева је реална употребљивост алата. Таква врста употребљивости не може се постићи занемаривањем захтева

крајњих корисника. Полицијски службеници и техничко особље морају да нађу начин да превазиђу проблеме у комуникацији и артикулишу потребе и проблеме полицијског посла, који треба да буду адекватно атикулисани и представљени, а затим превазиђени имплементирањем решења савремене технологије. На ту врсту проблема указује и *State of the Art Report: Crisis Management Tools. – INDIGO*,[8] извештај који јасно указује на неразумевање између произвођача и корисника информационих система. Поменути проблеми нису критични у свакодневним ситуацијама, али могу бити итекако озбиљни у кризним ситуацијама.

Безбедносни аспекти информационог система

ИКС је подлога на коју се стављају функционалности за којима имају потребу корисници креираних софтверских алата посебне намене. ИКС управљање представља скуп органа и појединаца (конкретног организационог система) и техничких средстава информатике и везе, организационо и функционално повезаних, помоћу којих се, на основу унапред дефинисаних и разрађених метода и поступака, реализују задаци стварања, прикупљања, обраде, чувања и дистрибуције података и информација у датим условима.[9] Основна улога информационог система јесте остварење динамичке повезаности између управних и извршних органа управљања у оквиру једне организационе целине или једног система у целини, али и система са окружењем, у процесу извршавања задатка, кроз читав животни циклус система и у различитим амбијенталним условима, при остваривању жељене мисије.

Када се у циљу остваривања безбедности грађана употребљава ИКС, он треба да делује по принципу приказивања могућих сценарија (пракса показује да треба кренути од сценарија са најлошијим факторима по безбедност и елиминисати негативне елементе прикупљањем реалних информација, њиховом обрадом и пласирањем јасне слике о безбедносној ситуацији). ИС треба да пруже све релевантне информације за све сценарије које је могуће предвидети, а каснијим филтрирањем могу се приказати само релевантне информације о сценарију који је најприближнији реалној ситуацији затеченој на терену.

[8] Овај извештај даје преглед главних технологија израђених и доступних за кризне менаџере. Даје преглед доступног софтвера и преглед актуелне литературе из те области, и указује на проблем између корисника информационих технологија и произвођача, који се манифестује у неразумевању међусобних потреба.

[9] Андрејић Марко Д., Миленков Марјан А., Соколовић Влада С, *Логистички информациони системи*, Војнотехнички гласник, бр. 1/10, стр. 34.

Лакше је прихватити тежи сценарио ситуације на терену и обавити све предвиђене радње у складу са оперативним процедурама, него бити изненађен лошијим сценаријом од оног који је претходно саопштен.

Такође, уз друге сервисе ИКС омогућава вођење акције у реалном времену и стварање јасније слике о безбедносној ситуацији на терену, подизање степена информисаности и креирање свести о ситуацији у којој мора да се управља тимовима на терену.

Посматрање интранет мреже МУП-а (унутрашња рачунарска мрежа којој могу да приступе само припадници МУП-а) као потпуно безбедне мреже јесте помало утопијски поглед на реалност у којој се налазимо.

Неке грешке у систему или злоупотребе система за информисање од стране одређених група не морају да имају карактер намерног саботирања или злоупотребе зарад личне користи или користи трећег лица, али ипак постављају питање одговорности инжењера који су креирали систем и извршили имплементацију, затим одговорних лица који су то одобрили и оперативних радника који користе такав систем, утврђивањем да ли су испоштовали све предвиђене процедуре при руковању системом.

Савремени сервиси, као што је позиционирање мобилних претплатника,[10] су изузетно осетљиво питање, посебно у нестабилним друштвеним системима или системима који пролазе кроз процес транзиције и мењања устаљених навика, правила понашања, као и правних норми.

Такође, питање коришћења позиционирања позиваоца службе за хитне интервенције тиче се *Закона о заштити података о личности*, у коме се помињу изузеци (члан 12 и 13), а према члану 80 *Закона о електронским комуникацијама*, софтверски систем за помоћ при одговору на хитан позив је изузетак у *Закону о заштити података о личности*. Злоупотреба таквог система је потпуно искључена као могућност, а постављено је као пројектни задатак да се изгради систем који адекватно испуњава постављене услове и захтеве. Оперативне линије рада које су под могућношћу социјалног инжењеринга као врсте напада на идентитет личности, ради злоупотребе идентитета личности које припадају безбедносном систему зарад прибављања поверљивих информација, излазе из поља овог рада, али јесу једно од питања о коме мора да се разговара и којим морају да се позабаве одговарајуће службе

[10] Према члану 80 *Закона о електронским комуникацијама*, мобилни оператери су у обавези да проследе информацију о локацији позиваоца службама сталног дежурства, али пројектовани систем не сме да остави могућност произвољног упита или системске грешке која би могла да се искористи у ту сврху.

унутар МУП-а и стручњаци надлежни и компетентни за ту проблематику. Од изузетне користи могу бити радови Kevina Mitnika,[11] који се баве темом социјалног инжењеринга[12] – Mitnik, Simon, 2003. и Mitnik, Simon, 2005.

У радовима (Митник, 2003; Митник, 2005) се првенствено обрађује тематика заштите информација на извориштy (заштитом рачунарских система, употребом уграђених сервиса заштите у опертивне системе, употребом криптолошких метода за заштиту података), заштитом транспортних путева (коришћењем протокола за сигурну комуникацију), заштитом информација на одредишту (које се складиште зарад касније анализе), и све то са циљем перманентног праћења могућих безбедносних претњи и нових начина напада, као наставак кружног процеса остваривања сигурности комуникационо-информационих система, јер сигурност није производ већ процес који траје (Ранђеловић, 2014) и јер је математика објективна и у недостатку бољег израза „савршена“ (Schneier, 2004), док је реалност у којој обитавају и делују сигурносни системи субјективна.

Да би се остварио такав циљ, неопходне су разне методе које користе криптозаштиту као основни алат за спровођење директне заштите информација, али и основ за многе друге методе који се користе у системима заштите, као што је заштита интегритета података, аутентификација, заштита од прислушкивања и слично. Такође је неопходно коришћење алата[13] за јачање отпорности на дисасемблирање и обрнути инжењеринг.

Потребан је стабилан оперативни систем са најновијим исправкама (енг. patch) које су уствари дорада кода оперативних система за пропусте и грешке које су откривене након пуштања система у рад (Brown, 2004).

Након тога, потребан је сигуран транспортни пут који ни прислушкивањем[14] не одаје корисне информације, а то подразумева употребу сигурносних протокола као што су сигурни начин повезивања SSL-а (енг. Secure Sockets Layer) или отворени ССЛ (енг. OpenSSL), који је отворен код (енг. open-source) имплементације SSL и TLS (енг.

[11] Кевин Митник је познати хакер који је три године успео да избегава хапшење, а за то време је правио упаде у ИС и телекомуникационе системе углавном служећи се социјалним инжењерингом, што је описао у књигама *Уметност обмане* и *Уметност упада*.

[12] Социјални инжењеринг користи утицај, убеђивање и манипулацију да би неко себе представио као другу особу и тако прибавио информације које не би био у могућности да прибави другим средствима у датом моменту.

[13] енг. Obfuscation – софтвер који у изворни креирани програмски код убацује додатне функције које немају намену, мења називе одређених делова програма тако да немају смисла када се дисасемблују или се покуша обрнути инжењеринг над софтвером.

Transport Layer Security) протокола, где се може изменити алгоритам за шифровање и тиме још више ојачати сигурност преносног пута.

Bruce Schneier у књизи *Тајне и лажи: Дигитална сигурност у умреженом свету* (енг. *Secrets and Lies: Digital Security in a Networked World*) говори о три типа мера, а то су заштита, детекција и реакција. Када се пишу програми, обично је у фокусу заштита коришћењем криптографије, а слабо се води рачуна или се уопште не води рачуна о детекцији и реакцији.

Детекција напада је, наравно, такође битна са становишта безбедности ИКС, при чему многи алати за детекцију напада у такозваном активном режиму рада имају уграђену и реакцију.

Програми Снорт[14] (енг. Snort), Трипвер[15] (енг. Trip Wire) и Своч[16] (енг. Swatch) могу да обезбеде детекцију упада у ИКС чувањем података у одговарајућим фајловима, сваки као типичан представник једне од три групе, респективно:

- датотеке које се праве на основу података пренетих са мреже на коју је рачунар прикључен – програмима који се зову њушкала;
- датотеке које се праве приликом настајања промена у најзначајнијим системским датотекама, такозвани мониторинг интегритета;
- датотеке које се формирају приликом приступа систему – логовања, отуд назив лог датотеке (енг. files)(праве се и за друге врсте приступа, нпр. другим датотекама).

Безбедност програмског кода

И поред познавања свих сигурносних процедура, претњи на различитим оперативним платформама, позива одговарајућих сигурносних програмерских приступних функција из сигурносних библиотека (енг. Application Programming Interface − API), ако се код не напише на безбедан начин, и поред употребе безбедносних функција програм ће бити отворен за различите врсте напада (Freeman, Jones, 2003).

[14] Снорт (енг. Snort) је детекционо превентивни систем отвореног кода, што значи да је бесплатан. Представља стандард и има 400.000 регистрованих корисника. ИПС (енг. Intrusion prevention system) и ИДС (енг. Intrusion detection system), превентивни и детекцијски систем упада, респективно.

[15] Трипвер (енг. Trip Wire) је компанија која има палету програма за смањивање ризика од упада у ИС, остваривање интегритета фајлова и других програма који омогућују сигурност ИС.

[16] Своч (енг. Swatch) је Unix-Linux алат дизајниран за праћење системских активности рачунарског система.

Моделовање претњи по Мајкрософту

Мајкрософт је развио свој систем моделовања претњи – STRIDE[17] :

- **S**poofing (лажирање),
- **T**ampering (преправљање доступних фајлова),
- **R**epudiation (порицање одређене радње),
- **I**nformation disclosure (прислушкивањем)
- **D**enial of Service (онемогућавање ауторизованог корисника да приступи систему),
- **E**levation of privileges (подизање степена права).

Лажирање је претварање да сте неко ко нисте, чиме стичете одређена права која вам не припадају. Један од корисника мреже може лажно да се пријави на систем како би добио приступ фајловима (информацијама) којима не би смео да приступи. Пример у рачунарском свету је пријем дигиталне поште која вас упућује на привидно познате светске сајтове (изгледом веома слична правом сајту, на пример, за електронску куповину), и онда од вас тражи да унесете осетљиве податке, као што је пин код (енг. Personal Identification Code – лични идентификациони код), број кредитне картице, корисничко име и лозинка.

У нашем случају, поред рачунарског лажирања, постоји и телефонско лажирање које се остварује увезивањем Астериск (енг. Asterisk), софтверска имплементација кућне телефонске централе (енг. Private Branch Exchange – PBX), и ВОИП (енг. Voice Over IP – VoIP), говор преко ИП-а провајдера. Након подешавања система могуће је у телефонској мрежи представити се као неки други број, тј. као друга особа.

Преправљање фајлова је нешто о чему програмери ретко размишљају, те се дешавају ситуације да се малом променом у конфигурационим фајловима или било којим фајловима који процесуирају податке не врши верификација унетих података на исправан унос, тако да долази до пада система или до његовог другачијег – непредвиђеног понашања, што за последицу може да има да се таквим нападом оствари добијање привилегије над ИКС-ом.

Порицање (одрицање) је метод којим треће лице, које није у систему, покушава да порекне да је урадило неку радњу. Такав метод захтева могућност скривања (брисања) трагова или извршавања напада преко четвртог лица у ланцу комуникације. Најчешћа одбрана од ове

[17] Brown, K., (2004). *The dot net developer's guide to windows security*, Addison Wesley.

врсте напада је креирање лог фајлова за осетљиве операције и прављење временског печата за креиране датотеке.

Гледање података је напад који се дешава и на статичким подацима (ускладиштеним на меморији рачунара) и на динамичким подацима (при транспортовању преко рачунарске мреже).

ДоС (енг. Denial of Service − немогућност употребе сервиса) је начин напада када се ауторизованим корисницима, који се сматрају делом система, онемогућава приступ и коришћење услуга система. На пример, ако неко „обори“ сервер, он је ауторизованим корисницима онемогућио приступ том серверу.

Подизање степена права омогућава кориснику или трећем лицу да одређени налог са одређеним степеном права компромитује тако да тај корисник добије већа овлашћења него што би требало да има и тиме омогући приступ подацима или неким осетљивим сервисима.

Други приступ је у грађењу стабла сигурности, и спроводи се на основу размишљања како би нападач кренуо у компромитовање система и на ком делу система би то урадио. Криптографија је најјача карика у ланцу одбране и мала је вероватноћа да се ту нападне, али постоје делови система који су много мање отпорни на нападе. Откривањем тих тачака и повећањем заштите нападач је заустављен и пре покушаја напада.

Може се чак направити листа приоритета узимајући променљиве и рачунајући ризик:

РИЗИК = ШТЕТА x ВЕРОВАТНОЋА.

Након креирања стабла и развијања сценарија разних начина напада,[18] долазимо до питања шта урадити са штетом ако се догоди.

Штета или компромитација система се може посматрати као руковођење ризиком.

Постоје четири начина како се ризик регулише, а то су:

1. прихватање ризика,
2. пребацивање ризика,
3. отклањање ризика, и
4. ублажавање последица.

Прихватање ризика је део свакодневице, и сама цена спречавања одређеног ризика може да буде скупља од последица које тај ризик може да изазове. Па је исплативије прихватање ризика и цене коштања за опоравак система.

Пребацивање одговорности је такође ваома чест начин ношења са ризиком. У рачунарским системима се то ради тако што се осигура

[18] Пожељно је у што већој мери и заједно са што већим тимом урадити креирање могућих начина напада и њихових стабала гранања.

систем преко осигуравајућих компанија од штете нанете нападом на ИС.

Отклањање ризика је ређи али често веома пожељан начин погледа на проблем решавања ризика. Откривањем потенцијалног ризика у појединим функцијама система и избацивањем те функције на основу процене њене употребљивости и могуће штете коју може проузроковати, смањује се функционалност система али и степен ризика. Ако избачена функција није од виталног значаја, ризик је сведен на минимум а функционалност задржана.

Ублажавање последица ризика као начин суочавања са ризиком јесте начин који се употребљава када дође до злоупотребе система и начињене штете.

Принцип најниже привилегије

Принцип најниже привилегије је први дефинисао Satzel[19] : „Сваки програм и сваки корисник система требало би да може да ради користећи се најнижим сетом привилегија које му омогућавају да обави посао на систему, овај принцип такође смањује ризике од могућих грешака које су настале извршавањем програма.“

Тако се систем чува и од нападача, али и од лоше написаних програма.

Једно од првих правила-принципа треба да буде да се програми пишу под корисничким налозима са смањеним привилегијама.

Аутентификација

Аутентификација одговара на питање ко сте ви.

Када се неко логује на рачунар, он проверава његов идентитет тражењем уноса одређене лозинке за одређени налог.

Аутентификација се може вршити нечим:

1. шта имаш?
2. шта знаш?
3. какве јединствене особине имаш?

Прва могућност се односи на нешто што сам корисник поседује као, на пример, шифру корисничког налога.

Други поменути начин је бољи, снажнији систем поседовања картице, које се често посматра као вишефакторска аутентификација, која је јединствена, и када се аплицира на систем, он додатно тражи ПИН код картице − лични идентификациони код (енг. Personal Identification Code) чиме се увећава сигурност система. Корисник сада,

[19] http://web.mit.edu/Saltzer/

поред знања пин кода, мора да поседује и идентификациону картицу, која је најчешће смарт картица са микроконтролерима који обезбеђују додатне заштите од хаковања саме картице и комуникације са ИКС-ом.

Последња опција се односи на биометрију, која је јединствена за сваку особу. Сматрала се новим напретком у систему заштите, али су истраживања на реалним системима показала да је често лако преварити биометрију особе, а посебно отисака прстију.

Свакако да је комбинација ма која два, и наравно сва три наведена начина сигурнији и јачи систем, јер се повећањем броја начина којима се врши аутентификација повећава квалитет и смањује могућност грешке.

Аутентификација преко мреже може да се одвија на један од три начина:

1. сервер тражи од клијента да докаже свој идентитет (основно подешавање у Керберос[20] систему);
2. клијент може да тражи од сервера да се представи и докаже свој идентитет (основно стање код ССЛ конекције), и
3. обострана аутентификација (трећи систем подржавају и Керберос и ССЛ системи).

Литература

1. Андрејић, М., Миленков М., Соколовић В., (2010). *Логистички информациони системи*, Војнотехнички гласник, год. 58, бр. 1, стр. 33-61.
2. Brown, K., (2004). *The dot net developer's guide to windows security*, Addison Wesley.
3. Freeman, A., Jones, A., (2003). *Programming .NET Security*, O'Reilly Media.
4. Mitnik, K., Simon,W., (2003). *The art of deception, controlling the human element of security*, Wiley Pub. Inc., Indianapolis.
5. Mitnik, K., Simon, W., (2005). *The art of intrusion: The Real Stories Behind The Exploits Of Hackers*, Intruders And Decivers, Wiley Pub. Inc., Indianapolis.

[20] Енг. Kerberos, грч. kɛərbərəs је протокол за аутентификацију преко РМ који ради по принципу „картице улазнице", како би омогућио корисницима да сигурно комуницирају преко небезбедне РМ утврђивањем идентитета и једног и другог учесника у комуникацији на сигуран начин. Првенствено је креиран за аутентификацију клијента ка серверу, али може да се конфигурише да ради и на начин обостране аутентификације. Керберос протокол је заштићен од недозвољеног прегледа порука-пакета и напада понављањем поруке. Керберос је креиран са симетричним начином шифровања и неопходна му је поверљива трећа страна. Он такође може опционо да се подеси за пренос симетричног круча користећи асиметрични алгоритам за шифровање.

6. Ranđelović, D., Delija, D., Popović, B., (2009). *EnCase forenzički alat*, Bezbednost, Vol. 50, br. 1-2, pp. 286-312.
7. Ranđelović, D., Petrović, L., Radovanović, R., Popović, B., (2009). *Security protocols*,
NBP – Žurnal za kriminalistiku i pravo, Vol. 14, No. 1, pp. 89-116.
8. Ранђеловић, Д., Јаћимовски, С., (2011). *Полицијска информатика*, КПА, Београд.
9. Ranđelović, D., Bogdanović, T., (2010). *Application of some tools of digital forensics*, NBP – Žurnal za kriminalistiku i pravo, Vol. 15, No. 2, pp. 25-47.
10. Ranđelović, D., Đorđević, V., (2011). A *test sample application ids open source and commercial source*, NBP – Žurnal za kriminalistiku i pravo , Vol. 19, No. 3, pp. 45-65.
11. Ranđelović, D., Stojković, D., (2012). *Possibilities of use the autopsy tool in forensic purpose*, NBP – Žurnal za kriminalistiku i pravo, Vol. 17, br. 3, pp. 19-35.
12. Ранђеловић, Д., (2013). *Високотехнолошки криминал*, КПА, Београд.
13. Ранђеловић, Д., (2014). *Управљање и заштита информационих система*, КПА, Београд.
14. Ranđelović, D., Ranđelović, M., Kuzmanović, Z., (2014). *Praktična primena softverskih alata u kriptografiji*, NBP, br. 2, pp. 115-136.
15. Schneier, B., (2004). *Secrets and Lies: Digital Security in a Networked World*, John Wiley& Sons, Indianapolis.
16. Stamp, M., (2006). *Information Security, priciples and practice*, John Wiley&Sons, NJ.
17. Субошић, Д., (2010). *Организација и послови полиције*, КПА, Београд.
18. Талијан, М., (2001). *Руковођење унутрашњим пословима*, ВШУП, Београд.
19. Van Tilborg, H., (2005). *Encyclopedia of Cryptography and Security*, University of Technology Eindhoven, New York.

.

The specificity of tools for responding to an emergency call's in the police

Abstract: *Service of permanent duty is one of the most important services on which work is performed and the to the police response to an emergency call that service is one of the most important tasks.*
This paper attempts to provide insight into the organization, activities and work of security services that deal with response to an emergency call, in order to point the necessity of implementing modern services which increase

the level of prediction of the situation on the ground in real time and allow adequate time engagement and a more determined - faster reaction.
The specificity of tools that should provide the information to the police command staff, which is responsible for the operation in case of an emergency call to the police, is reflected in the degree of accuracy, speed of incoming and the speed of data processing into information useful for constructing images of emergency declared by calling incidental or crisis situation.
The aim is to determine the necessary methods and principles required in the implementation of tools for responding to an emergency call. It seems, on the one hand, the analysis of the results of previously implemented tools, both from the aspect of design and implementation, and exploitation as the most important assessment of the real effectiveness of each tool, and, on the other hand, to find the appropriate methodology solutions.
Also, the paper presents function of one of the possible scenarios for implementing IKS, which especially divers attention to the security aspects which the necessity of implementation of the IKS is primarily related to the protection of sensitive information and prevent their abuse.

***Key words**: urgent call for help; tools for responding to an emergency call, the security system for emergency calls, authentication, encryption*